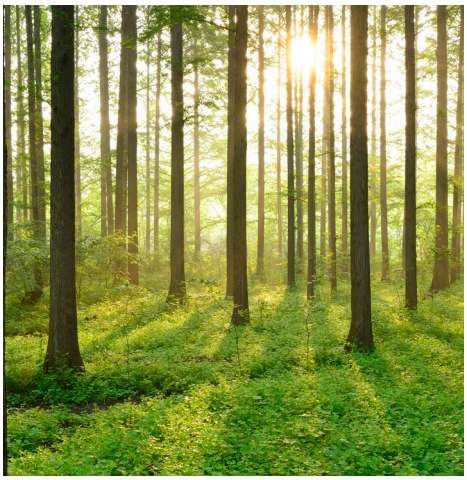
COTS DIGITAL DEVICES IN SAFETY CRITICAL INDUSTRIES

REPORT 2019:627



NUCLEAR

ENERGIFORSK NUCLEAR SAFETY RELATED I&C – ENSRIC

Energiforsk

COTS Digital Devices in Safety Critical Industries

Use and Licensing

EOIN BUTLER, GARETH FLETCHER, SAMUEL GEORGE, SOFIA GUERRA AND HEIDY KHLAAF

ISBN 978-91-7673-627-2 | © Energiforsk November 2019 | Cover photo Moore Industries
Energiforsk AB | Phone: 08-677 25 30 | E-mail: kontakt@energiforsk.se | www.energiforsk.se

Foreword

In the nuclear industry, nuclear grade products and components are 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. To ensure the performance of the equipment they are extensively tested. However, given that the number of nuclear grade equipment sold is lower, they are less well tried in real applications compared to industry standard components. This might actually increase the risk of unforeseen problems not included in the extensive test schemes.

In this report, senior consultant Sofia Guerra at Adelard in the UK has led the work to investigate if/how industry standard products are used in safety classed applications in other industries, and if it would be feasible to use it also in nuclear applications in the Nordic context. Adelard co-workers Eoin Butler, Gareth Fletcher, Samuel George and Heidy Khlaaf were also involved in the project. The activity is included in the Energiforsk Nuclear Safety Related Instrumentation and Control program – ENSRIC. The program is financed by Vattenfall, Sydkraft Nuclear/Uniper, Teollisuuden Voima Oy (TVO), Fortum, Skellefteå Kraft, Karlstads Energi and the Swedish Radiation Safety Authority.

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.

Sammanfattning

Commercial-Off-The-Shelf (COTS) -komponenter eller industristandardkomponenter används alltmer i styr- och reglersystem i kärnkraftstillämpningar. De har flera ekonomiska fördelar, eftersom kärnkraftspecifika produkter i vissa fall inte längre är tillgängliga och kostnaden för att utveckla skräddarsydda komponenter kan vara mycket höga. Dessutom tillverkas industristandardkomponenter vanligtvis i större serier, och det finns därmed mer drifterfarenhet och därmed större möjligheter att upptäcka fel som inte identifierats i de omfattande tester som görs av produkter som håller kärnkraftstandard.

Det finns också flera utmaningar när det gäller användning av industristandardkomponenter i kärnkraftstillämpningar, särskilt vad gäller säkerhetsdemonstration och licensiering. Traditionellt har COTS-komponenter motiverats genom att visa att de uppfyller relevanta standarder. Detta ger utmaningar för högkvalitativa komponenter som utvecklats i enlighet med äldre- eller olika standarder, eller bara uppfyller industriell god praxis och därför inte utvecklats specifikt för kärnkraftsindustrin. Nyligen har det gjorts en hel del forskning inom säkerhetsdemonstration för digitala processer.

I detta projekt granskades användningen av COTS-komponenter i säkerhets- och säkerhetsrelaterade applikationer i både kärnkraftsindustrin och i andra säkerhetskritiska industrier. Utifrån vår kartläggning har vi analyserat flera gemensamma teman. Fokus för arbetet har varit specifikt aspekter relaterade till säkerhetsdemonstration av programvara för smarta enheter, och inte faktorer som är gemensamma med analoga enheter, t.ex. miljökvalificering och typtestning. Projektet presenterades vid ett seminarium som ägde rum i Stockholm den 22 oktober 2019.

Summary

Commercial-Off-The-Shelf (COTS) components are increasingly used in nuclear Instrumentation and Control (I&C) applications. They have several commercial advantages, as nuclear specific products may not be available and the cost of developing bespoke components may be prohibitive. In addition, commercial components typically benefit from a wider user base, and therefore, greater amounts of operating data that increase the changes of detecting (and fixing) systematic faults.

While there are several commercial benefits in the use of COTS components, there are also several challenges and concerns with regard to their safety demonstration and justification. Traditionally, COTS components have been justified by attempting to show compliance with relevant standards. This presents challenges when otherwise high-quality components were developed in accordance with older or different standards, or just meet industrial good practice, and therefore not developed specifically to the nuclear industry. Recently, there has been a great deal of research into justification processes of digital processes.

In this project, we reviewed the use of COTS components in safety and safety related applications in both the nuclear industry and other non-nuclear, safety-critical industries. From our review, we have extracted and analyzed several common themes. The focus of the work was on the specific aspects related to the justification of the software of the smart devices, and it does not discuss in detail aspects of the justification common to analogue devices, e.g., environmental qualification and type testing. The project was presented at a seminar that took place in Stockholm on 22 October 2019.

List of content

1 Introduction

This report contains the results of our review of the use of COTS components in safety and safety related applications in both the nuclear industry and other non-nuclear, safety-critical industries. The approaches adopted in different countries are presented in Section 3, while our survey of other safety-critical industries is set out in Section 4. The common themes that we have identified are developed and discussed in Section 5.

The IAEA has recently published guidance for nuclear power plant operators on the justification of commercial industrial digital instrumental and control equipment [1]. This guidance is summarised in Appendix A:. Appendix B: reproduces the consultation brief used to gather information and Appendix C: summarises the seminar that took place in Stockholm on 22 October 2019.

2 Scope and methodology

The scope of this study has focussed on COTS digital industrial devices, also called "smart devices". These are devices that are designed to perform a specific function and are usually not programmable by the end-user. However, in some industries, it was identified that the use of non-programmable devices is not common, and so a generic qualification and licensing process for digital/software-based systems were also considered.

While digital devices are also subject to hardware qualification requirements (such as environmental and seismic tolerance), we have not focussed on this aspect, instead concentrating on software-specific concerns.

Information was gathered through a combination of consultations and informal discussions with representatives from the relevant industries, research of the publicly available relevant literature, and by capturing Adelard's experience in the use of COTS products in NPPs. The selection of sectors was based on the expected ease of access to relevant information and knowledgeable experts and the expected variety of approaches. 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 B. We are grateful to our consultees for their assistance.

The results of the project were presented at a seminar that took place in Stockholm on 22 October 2019. The program of the work and some of the topics discussed are included in Appendix C.

3 Nuclear power industry

3.1 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 [2].

Classification of Finnish nuclear facilities' systems, structures and components is described in YVL B.2 [3]. The approach is primarily based on deterministic methods, which may be supplemented by a probabilistic risk assessment 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), in a similar way to that described by IEC 61226 [4].The guide contains descriptions and criteria for assigning classes to systems, based on the significance of the function they are performing.

The qualification of smart devices should be done according to YVL E.7 [5]. Component qualification plan and a preliminary suitability analysis should be submitted to STUK for devices in safety classes 2 and 3.

For safety 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

Section 6 of YVL E.7 expands on the requirements for qualification of safety-classified software, including, for example, compliance with standards for the design and implementation of software (for class 2, this should be against nuclear standards; for class 3, other safety-related standards could be used). Any deficiencies in the documentation and implementation of the design process may be substituted by analysis or testing. For software in safety class 2, YVL E.7 refers to the approach shared by international regulators [6].

The approach takes into account information and requirements of the intended application of the smart device during the qualification (right from the start in the qualification plan). The concept of assessing components independently of a specific application is not part of the regulatory framework. Nevertheless, some parts of the qualification could be re-used between applications.

3.2 SWEDEN

The Swedish Radiation Safety Authority (SSM) guidance provided in SSMFS 2008:1 on general advice on safety in nuclear facilities [7] states that software should be thoroughly verified and validated, and that all the development process should be planned and documented. The regulator task force report of 2018 on

safety critical software [8] is included in the regulations by introducing a separate section on the justification of smart devices.

The common position requires that the production process is compared with an applicable standard, but they do not endorse compliance to any particular standards. If any gaps are revealed during the compliance assessment, these must be addressed by compensating activities and justified that they are not applicable or have been mitigated.

In addition to compliance with standards, additional independent (from the supplier) confidence building activities should be performed. These may include commissioning test, analysis of operating experience or static analysis.

Safety justification is typically provided in the preliminary and final Safety Analysis Reports (SARs). These documents provide a summary of the plants' most important radiation protection features, explain how requirements for these have been met, and reference the wider document set that is produced during design and safety assessment of the system described. The licensee and the regulator have several options, but the aim 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".

3.3 UNITED KINGDOM

Nuclear power plants in the United Kingdom make use of smart devices in a variety of applications, such as temperature, pressure and level sensors and transmitters, electrical protection relays, trip amplifiers and specialist controllers for electromechanical equipment.

Operators of Nuclear Power Plants (NPPs) are required to be licensed by the Office for Nuclear Regulation (ONR). As part of their licence conditions, they must comply with the ONR's Safety Assessment Principles (SAPs) [9] and Technical Assessment Guides (TAGs). In particular, for computer-based safety systems, the ONR SAP clause ESS 27 provides that "…compliance with appropriate standards and practices throughout the software development lifecycle should be established in order to provide assurance of the final design." COTS products containing microprocessors used in performance of a safety function are considered computer-based safety systems for these purposes.

The regulatory regime in the UK is largely goal based, so it is in the first instance for the licensee to determine the assurance activities that must be carried out in accordance with ESS 27 and TAG 46 [10]. Licensees are responsible for ensuring that their use of COTS devices complies with these principles. In order to do so, licensees conduct or commission assessments of devices. This process leads to a documented formal qualification of a device for its intended application, backed by evidence.

The level of justification required for a smart device depends on a number of factors, but broadly aligns with the safety function categories and system classes of IEC 61226 [11]. The system of which a COTS product forms part will determine the safety relevance of a COTS device. TAG 46 contains guidance for assigning reliability claims to particular devices. The reliability claim and safety integrity level 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.

The safety justification of software-based systems, and COTS smart devices in particular, is divided in two legs – production excellence, in which the quality of the design and development processes is assessed, and independent confidence building, which requires a thorough, independent examination of the device and/or its software. Independent confidence building measures are carried out so as to be independent of the device manufacturer. At the highest integrity levels, corresponding to Class 1 of IEC 61226, independent review and/or analysis of the source code is required. Source code access is occasionally desirable at lower integrity levels, particularly if any type of source code analysis is identified as to compensate for shortcomings in production excellence.

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" [10]. IEC 61508 [12], IEC 61513 [13] and IEC 60880 [14] are typical of the standards recommended for this role.

Production excellence for smart devices is typically assessed using the Emphasis approach [15], which is a questionnaire derived from IEC 61508, and has been adopted as an industry consensus. Emphasis can be used with different target Safety Integrity Levels (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. Items of interest are identified through the responses given by the device's designers and developers to Emphasis questions. For components with a lower integrity aim, other processes may be used, which do not typically reach the same level of detail as an Emphasis assessment. Third-party product certifications (e.g., commercial certificates of compliance to IEC 61508) can be taken into account in the assessment of production excellence, but are neither necessary nor sufficient for successful assessment. Compensatory activities must be carried out if the production excellence leg falls short of the standard expected.

A justification for the use of a COTS product can be re-used with provisos. If the original justification contained assumptions or restrictions on use that are inapplicable to the destination application, or if its scope was restricted to a different functional envelope, or if the reliability requirements were different, then significant further work would be required to justify the device in the new application. The ONR takes a sampling approach to these justifications, and the risk remains with the licensee relying on the assessment that it is and continues to

be suitable for its purpose. Occasionally, parts of assessments can be re-used by other licensees subject to a suitable commercial agreement.

3.4 UNITED STATES

It is generally expected that any product being used to fulfil a safety function in an NPP (a "basic component") 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]. However, for COTS items (which by their nature will not have been designed specifically to meet the requirements of the NRC), the expectation is to show them to have been produced with equivalent quality.

The main approach followed for equipment classified as "safety related", the highest level, is the dedication process described in EPRI 3002002982 [17]. The dedication process has two main elements: a "Technical Evaluation" and an "Acceptance Process".

The "Technical Evaluation" phase includes activities such as

- safety function definition
- development of appropriate technical and quality requirements
- identification of critical characteristics, typically accomplished through a failure analysis based on the safety function
- identification of acceptance criteria for each critical characteristic

The acceptance process aims at "providing reasonable assurance" that the component meets its requirements. The critical characteristics are verified using one or more of the following methods:

1. special tests and inspections
2. commercial-grade survey
3. source verification
4. item/supplier performance records

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.

The commercial dedication process assumes that suitability of the design has been checked. The dedication is an acceptance process that cannot change the design and is not a means to verify the suitability of design. The suitability of the design can be done through dependability review, environmental testing, seismic testing and EMC testing.

The main EPRI document [17] does not describe specific activities to be carried out on the software aspects of digital systems in any detail, though there are several supplementary guidance documents for accepting digital devices referenced. EPRI 1011710, "Handbook for Evaluating Critical Digital Equipment and Systems" [18], is based around a review that seeks to establish the systematic integrity and reliability of the device, which in turn can include "Critical Digital Review", which assesses dependability properties in relation to the requirements made of the device.

It is possible to use an application-specific dedication plan or a generic one. In the application-specific case, or where an application falls outside the scope of a previous generic CGD plan, the EPRI guidance [17] makes clear in its objectives that each commercial-grade item dedication plan should be based on the specific end-use for the item. This does not prevent the party undertaking the dedication from reusing some information from a previous dedication. In particular, the dependability review, which examines systematic integrity and reliability of the device, is likely to be broadly similar in content for any application, but its exact scope and approach should be informed by the particular use case. If a generic dedication plan is used, it must encompass the application-specific requirements and this must be verified.

The dedicating entity "is responsible for identifying and evaluating deviations, reporting defects and failures to comply for the dedicated item, and maintaining auditable records of the dedication process." It may be a licensee, manufacturer or third party. A third party can conduct a CGD on behalf of a licensee, and often does. They then supply the component as a nuclear grade item, and take on the regulatory burden associated with this, including ongoing requirements under the NRC's regulations.

3.5 FRANCE

The Nuclear industry in France is regulated by the Autorité de Sûreté Nucléaire (ASN). The RFS (fundamental safety rules) describe the safety objectives to be met in approximately 40 technical areas and give examples of techniques and methods for achieving these objectives. On a more operational level, AFCEN industrial codes represent consensus between main industrial partners in France and are used for defining requirements on a contractual basis. For example, RCC-E [19] constitutes a technical design code for electrical and I&C systems for pressurised water reactors. The most recent versions of RCC-E have included more detailed information concerning industrial digital devices of limited functionality (as defined by IEC 62671 [20] – a similar concept to smart devices), and introduce alternative qualification methods that credit IEC 61508 [12] certifications. For the I&C aspects, the RCC-E relies heavily on IEC standards but clarifies an interpretation at a national level. The RCC-E identifies what is and is not relevant in a standard such as IEC 62671 within the context of equipment qualification. Électricité de France (EDF) is the sole operator of commercial nuclear power plants in the country.

The approach to qualification of software and programmed digital aspects of smart devices in France relies on the idea that smart devices are pre-existing components bought off the shelf, and that requirements cannot therefore undermine previous design choices. Requirements essentially address quality assurance processes, including verification and validation activities as implemented by the design, and the way smart devices are used and implemented within a system. According to the qualification method, suppliers may be subjected to audit; such audits are likely to require more if there are no third-party product certifications available. Certifications by themselves cannot be used as a basis for qualification as the licensee is solely responsible for nuclear safety and cannot pass on this

responsibility. However, certifications can be audited, checking what should have been and what has been done. Other documents need to be supplied – for example, general QA and V&V evidence, technical descriptions of instrument, how operational experience has been taken into account and how modifications are handled.

Qualification is carried out on a case-by-case basis for the required functional envelope with parameters within defined ranges, and there may be restrictions on how a device is used. Suppliers are required to inform EDF of any changes to a device. EDF then analyses whether the change is major or minor and what action to take.

A system of grading is used, following a classification system with three safety classes for safety equipment. The same approach is used for all safety classes, with variations according to the safety class. Complementary testing may be needed to compensate for shortfalls as identified in the audit-based process. Examination of source code is not performed.

3.6 GERMANY

The German approach to qualification of digital systems is based on the requirements defined by the German government [21] and nuclear regulator [22]. The approach is based on IEC standards such as IEC 61513 [13], IEC 60880 [14] and IEC 62138 [23]. VDI/VDE 3528 [24] sets the regulatory expectations for COTS products.

The most commonly used route for qualification is to build on an existing commercial certificate of compliance to an industrial standard (e.g., IEC 61508 [12]). An analysis is performed by an assessor (e.g., TÜV) contracted by an NPP operator to identify any gaps between the existing certification and the nuclear requirements, with any such gaps being closed using supplementary tests and/or analysis. Differences between the nuclear approach and industrial standards mainly concern aspects such as fault tolerance and redundancy to ensure the overall reliability of the I&C system.

When a COTS product is to be used for a category A or B function, an independent expert appointed in accordance with German law also performs a suitability assessment (focussing on development process, testing and proven performance/experience).

In addition to the qualification requirements, VDI/VDE 3528 sets up selection criteria for the device. These focus on the areas of documentation, technical properties, quality and operation.

Access to information is typically arranged contractually. This is aided by position of the assessment body as independent of the nuclear industry.

When an already-qualified device is to be re-used in another application, the qualification process can claim credit for an existing pre-qualification. Generic qualification is also possible, which can be used as a basis for an application-specific qualification.

3.7 CANADA

The Canadian Nuclear Safety Commission (CNSC) is the nuclear safety regulator in Canada and issues Power Reactor Operating Licences (PROLs) to NPP operators. The governing standard used with respect to COTS-software containing products is CSA N290.14-15 [25], which defines a process to be followed. The requirements of N290.14-15 apply to any pre-developed software and not necessarily just the firmware found in smart devices.

The process has the following main components:

- identification and categorisation of the digital item
- addressing of concerns
- failure analysis
- digital item activities
- reporting

N290.14-15 [26] requires identification and categorisation of the safety functions of the candidate product. The category of the overall product is the highest such category. The categories used map to the approach of IEC 61226, with CNSC categories 1-3 mapped to Categories A-C in IEC 61226. An additional non-safety related category, Category 4, is not considered here.

The candidate product is then assessed for "qualification concerns", which are a list of commonly encountered issues/vulnerabilities associated with the use of software-containing products. For each qualification concern, the objective is to identify if the concern is not relevant, can be addressed or cannot be addressed (thereby preventing qualification of the device).

Pre-developed software may be assessed using any of a number of routes: the "recognized program method", the "mature product method", "proof through testing" and the "preponderance of evidence". Not all methods are permitted for all categories.

The "recognized program" route requires third-party certification of conformance to one of several standards, including IEC 61508 [12]. The assessment must still be examined to determine its suitability. "Mature product", which cannot be used at Category 1, builds on proven-in-use data. The amount of data needed depends on both the Category and the complexity of the pre-developed software. "Proof through testing", which can only be used at Category 3, and only for low-complexity items, requires a certain level of in-use tests in a configuration representative of the application.

The last option, "preponderance of evidence", allows partial compliance with elements of the other routes, along with activities such as complementary testing and analysis to be combined to achieve qualification. This route also allows a previous qualification to be taken into account when qualifying the device, provided that the scope and applicability are justified.

Typical hardware assessment elements are also addressed, such as electromagnetic and seismic tolerance, production process and testing.

4 Non-nuclear safety critical industries

4.1 OIL AND GAS INDUSTRY IN THE UNITED KINGDOM

The UK oil and gas industry uses a range of COTS instruments. The same ranges of instruments designed for the process sector are commonly used in both safety and ordinary process applications. Compliance is based on IEC 61511 [27], which is the functional safety specialisation of IEC 61508 applicable to the process industry.

If it is intended to use a COTS device in a safety application, it is expected that the device will have a safety manual provided by a manufacturer, a complete functional safety assessment has been performed and the device has a certification for safety applications. Certificates are not in themselves sufficient. The end user or operator owns and manages the risk, and is expected to ensure that the necessary information to make a functional safety assessment is gathered. This might be by an employee of the end user organisation or a suitably qualified consultant.

The approach to functional safety assessment varies where the device being justified has been in long use or is being introduced into the end user's plant for the first time:

- Legacy equipment often has no safety manual or certificate and a proven-in-use argument must be relied on. Such an approach will take account of the quality system used in the design of the item and the details of its use on the end user's site.
- New equipment is expected to comply with IEC 61511, including the existence of safety manual.

All SILs can be approached, both in cases where comprehensive manufacturer information is available and where proven-in-use arguments must be relied upon, although in the latter case the process becomes difficult at higher SILs. In these cases, it is sometimes necessary to use voting systems among devices to achieve an overall subsystem with the necessary reliability characteristics. Diversity is usually needed in any case where SIL 3 is needed. Plant logic solvers often use cross-comparison between different sensors and diagnostics on valves.

It is rare for COTS components to be used for a safety function with SIL 3. Most devices are justified to SIL 1 (approximately 90%), and the overwhelming majority of the rest are at SIL 2.

The processes are in general guided by IEC 61511. Clause 11 of Part 1 concerns appropriateness to applications and is relevant where a new functional safety assessment needs to be carried out for a device that has already been assessed. IEC 61511 defines a life cycle process. In practice, validation corresponds to factory acceptance testing.

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 smart devices.

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 specific railway signalling applications.

When devices or systems are to be used in a safety-related application, their use needs to be supported by a safety case. Three types of safety cases are used:

- generic product safety case (independent of application)
  - a generic product can be re-used for different independent applications
- generic application safety case (for a class of application)
  - a generic application can be re-used for a class/type of application with common functions
- specific application safety case (for a specific application)
  - a specific application is used for only one particular installation

The details of what a safety case must contain are laid out in EN 50129 [28]. A safety case must show all of the following:

- 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. This includes evidence that all requirements have been demonstrated (e.g., a validation report), specification of environmental conditions and application pre-requisites, as well as other technical principles that assure the safety of the design, such as calculations, analyses and tests. Additionally, the report must consider the effect of faults, and demonstrate how the system will continue to meet its safety requirements in the event of random hardware faults.

The level of detail and extent of evidence provided is graduated by the Safety Integrity Level (SIL), a concept re-used from IEC 61508.

The safety case for a specific application is dependent on the safety case of the generic product and as part of the application's safety justification, it is necessary to show that all of the safety-related application conditions for the generic product have been satisfied and that the product has been configured and installed correctly.

A safety case must be independently assessed before safety acceptance is granted. This is documented in a safety assessment report, and the relevant safety authority issues a safety certificate.

A typical railway signalling system is integrated from a collection of smaller sub-systems, 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 AVIATION INDUSTRY IN THE UNITED STATES

The commercial aviation industry can be roughly divided into airframes/airborne equipment and ground-based equipment.

In the United States, the Federal Aviation Authority issues approvals for airframes as a whole (i.e., individual pieces of equipment are not certified). The regulatory regime is similar to that operated by the European Aviation Safety Agency (EASA). The market for aviation-related equipment is large enough that there is an industry that supplies COTS devices that have been specifically designed with the aviation industry in mind. Typically, there tends to be a large supply chain, where sub-systems are integrated into more complex systems, which are themselves integrated into even larger systems, until the system is incorporated into the aircraft itself.

Aviation-specific COTS tend to be more programmable than is usually associated with the simple functionality of industrial digital devices. One reason for this is the fact that aviation places a premium on weight savings, so a more integrated solution (combining sensor acquisition, processing and output) is desired. Additionally, the cost associated with certifying a device for use on an aircraft means that a more flexible platform, which can be programmed or configured to perform any of a number of roles, is often popular.

Systems containing software on airframes are required to comply with standard DO-178C [29]. However, only the complete aircraft is subject to approval, not the individual systems. This means that the entire aircraft and all sub-systems and components are assessed as a single unit, but the requirements of the standard propagate to and apply to the sub-systems.

In the industry, the expectation is that a supplier provides full visibility of the design and development lifecycle to the airframe manufacturer and this is secured via appropriate contractual arrangements. Compliance is demonstrated through documentary evidence, auditing, code review, and testing.

DO-178C defines a number of criticality levels, corresponding to the severity of the consequences of the software failing. The higher the consequence, the more safety objectives have to be met and the more rigorous the demands on the design and development lifecycle are. Fulfilment of each of the safety objectives is needed before the airframe is certified by the regulator (FAA) and can enter service. While DO-178C is applicable to both bespoke and COTS systems, a sub-chapter of the standard is devoted to COTS-specific concerns.

If a particular component from an already-certified aircraft is to be re-used on a new aircraft, the certification process starts from the beginning and re-evaluates

the component's compliance with DO-178C, without making use of the existing certification. However, any operational experience gained can be used to provide confidence in the acceptability of the system in the new certification.

A similar standard exists for ground-based communication, navigation and surveillance (CNS) equipment, DO-278 [30]. However, ground-based systems do not require regulatory approval, and assurance mechanisms are driven by the operator's assessment of the risk and are built into procurement contracts. When an operator is considering deploying a system, they identify any gaps between the information provided by the equipment supplier and the requirements of the standard, and identify appropriate mitigations or justifications of why the equipment is suitable for use in spite of the gaps. As with airborne equipment, software itself is not certified, even if re-used within other systems. However, once a COTS device is purchased and procured, it can be re-used multiple times, subject to an assessment of its suitability for the application.

Regulations set by the International Civil Aviation Organization (ICAO) require states to recognise the certification of an airframe provided that it meets certain minimum requirements. How this works in practice varies depending on the specific processes followed by the certifying state and the registering state. However, the two largest aviation markets, the United States and the European Union have harmonised their regulations and processes for airframe certification so that US certification performed by the FAA can be recognised by EASA, the EU agency, and vice-versa.

4.4 AUTOMOTIVE INDUSTRY IN THE UNITED KINGDOM

Similar to the rail and aviation industries, the automotive industry is also organised as a complex supply chain, where automotive-specific components and subsystems are integrated into systems of increasing complexity until becoming part of a complete car.

Regulatory approval is given to a vehicle as a whole before it is offered for sale, and there is no formal regulatory approval or licensing of vehicle sub-systems or sub-components.

The industry is currently transitioning to compliance with ISO 26262 [31], though different actors are at different levels of maturity in their transition, and widespread adoption has not yet been achieved. ISO 26262 is derived from IEC 61508, and categorises the risk and consequences of a system failure using four ASILs (Automotive Safety Integrity Levels). Similar to IEC 61508, a higher ASIL rating means that more lifecycle activities are required to claim compliance.

Though ISO 26262 envisions sharing of lifecycle and technical information between suppliers and customers in the supply chain, traditional practice has been to supply components as "black boxes" along with evidence that the requirements of the procurement contract have been met, typically in the form of requirements-based testing. The customer might also conduct their own testing, both on the product standing alone, and when it is integrated into the larger system.

As compliance with ISO 26262 (which is currently voluntary) becomes more widespread, there is a growing expectation that the procuring organisations have visibility into the development processes as well and potentially the on-board software. In the terminology of ISO 26262, a COTS product that is intended for use in a safety application is a “Safety Element out of Context” (SEooC). Because it is not possible to conduct a complete hazard analysis without knowledge of the eventual use case, such components are developed to a defined set of assumed requirements, and an estimated ASIL. When an integrator wishes to use an SEooC in a larger system, ISO 26262 requires them to validate that there are no conflicts or gaps between the system’s requirements and the assumed requirements.

5 Analysis

In this section we identify certain key themes that have emerged from the sectors we have analysed.

5.1 USE OF SMART DEVICES VS PROGRAMMABLE PRODUCTS

Though the scope of the project focussed on COTS digital industrial devices/smart devices, some industries do not commonly make use of such products. In some sectors, such as aviation and automotive, space and weight constraints appear to favour a more integrated approach to systems, with sensor acquisition/actuation and processing performed by a single device. Such integrated systems more closely resemble programmable logic controllers (PLCs), where a COTS platform and application-specific software is combined to produce the final system. In most cases, the same platform can be re-used in many different applications by changing the application software.

Furthermore, as discussed in Section 5.5, some of these industries benefit from a dedicated supply of products intended for their use. Therefore, it can also be the case that it is more economical to produce the systems with characteristics required as a single unit rather than construct a system by integrating a larger number of smaller sub-systems to give the same result.

5.2 COMPLIANCE WITH STANDARDS

In all sectors and countries, compliance of the development process and quality assurance approaches with relevant standards played an important role in the assessment of the digital COTS components. Standards could be standard specific, e.g., IEC 60880, or generic, IEC 61508. The way that compliance was assessed, however, varied from acceptance of third-party certifications (see Section 5.3) and an assessment done entirely by the licensee (e.g., UK nuclear industry).

5.3 USE OF THIRD-PARTY CERTIFICATIONS

Certain industries rely heavily on the use of third-party certifications for products to be used in safety applications. Here we define third-party certifications to be instances where an independent assessor (who may be funded by the manufacturer) performs an assessment of the device and produces a report/certificate that it conforms to a certain specification or standard. The most commonly-used standard is IEC 61508, and many industrial device manufacturers that market to safety-critical industries prominently use the fact that their devices have been certified as a selling point.

The extent of use of certifications varies to a great degree. In some industries (e.g., German nuclear, UK rail and UK oil and gas), the report or certificate can be used in the safety justification of a larger system without needing access to the underlying evidence. In others (e.g., UK nuclear) certification is not required, but where available, it does not replace the need for examination of the relevant

underlying evidence. However, the evidence developed during the certification can be used as evidence to support the justification. This is consistent with the guidance given in IAEA SSG-39 [32].

Additionally, we have not seen instances where third-party certification of COTS products are used at the highest integrity levels. Rather, the processes observed appear to be mostly confined to lower integrity levels (SIL 2 or lower), though there are a few exceptions.

A central question regarding the use of third-party certifications is which organisation might own the risk of the assessment being incorrect. For example, in the UK nuclear industry, license holders/NPP operators by law are responsible for all equipment used in their facilities, and cannot rely on certifications produced by a third party without a degree of independent review. On the other hand, commercial grade dedication as practiced by the US nuclear industry involves assumption of some risk by the dedicator.

5.4 ASSURANCE ACTIVITIES INDEPENDENT OF THE MANUFACTURER/SUPPLIER

Independently of the level of acceptance of certification, in all cases that we have seen, the end-user must perform at least some level of assurance activity themselves, even though independent certification may be in place. This may range from a review of testing activity, to performing supplemental tests, to potentially an independent analysis of the software. For example, in the UK nuclear sector, the concept of Independent Confidence Building Measures at safety class one, require a number of code analysis performed independently of the supplier of the COTS components; while in other countries and sectors, commissioning tests might be enough. In some cases (e.g., Germany), regulations allow for the use of COTS components with industrial certification to be mitigated through (for example) architectural considerations such as redundancy and diversity.

5.5 SECTOR-SPECIFIC SUPPLY CHAINS

Sectors with potentially large markets and stringent regulations (particularly aviation and rail) tend to attract sector-specific devices to be put on the market. These tend to be designed with compliance to the relevant standards in mind and arranging access to the required information for assurance and licensing is less challenging.

On the other hand, the market related to the nuclear industry is significantly smaller, especially for general-purpose components such as pressure sensors, and the investment in specialised devices and certification does not yield an economic benefit for the manufacturers.

Potentially interesting questions are how suitable the products from those industries are for use in the nuclear industry, and what is the scale of the gaps between the certifications/assurance already in place and those needed for use in nuclear power.

5.6 GENERIC AND APPLICATION-SPECIFIC ASSESSMENTS

The industries surveyed vary in their approaches for the re-use of an already-qualified product in a new application. In some industries the idea of a generic qualification/safety case is formally recognised (e.g., rail), while in others, a common approach allows a qualification to be re-used, provided that there is an assessment of suitability. On the other hand, in some industries (e.g., aviation), qualification re-use is not common. For example, in the UK nuclear industry, the notion of pre-qualification of smart devices, and a previous Energiforsk report discussed the possibility of a similar approach in the Finnish nuclear industry [33].

A possible driver for the different approaches is the potential scope for re-use and the associated cost-benefit analysis. In sectors where there is relatively frequent implementation of new applications, re-use seems to be favoured, while in cases such as aviation, where certification of a new airframe is infrequent, it is not used, as there would be little efficiency benefit.

5.7 CATEGORISATION AND CLASSIFICATION

Though the details of the methods vary, most sectors we have surveyed make use of a scheme of classification that indicates the required level of reliability or safety. The most common classification is the system of Safety Integrity Levels (SILs) defined in IEC 61508, though some sectors use variations (e.g., the automotive standard ISO 26262 defines Automotive Safety Integrity Levels (ASILs)). Nuclear industries make use of the classification and categorisation approach of IEC 61226. Additionally, many nuclear industries, including the UK and Canada, make an approximate mapping between the system classification and the required SIL.

The aviation industry (following DO-178) defines a system of Design Assurance Levels (DALs), which are similar in concept to SILs.

The idea of classification using integrity/assurance levels means that there is an approximately common language across the different sectors that might be an enable for re-use of existing assessments.

6 Conclusions

In this report, we reviewed the use and safety justification of digital COTS-components in a number of safety-related countries and sectors, with a focus on the digital aspects of the safety justification.

Digital COTS-components are becoming more widely used in a number of areas, where their use is more common in application with relatively modest safety requirements, but they may also be accepted for more onerous safety requirements.

Compliance with standards that prescribe requirements on quality assurance and development process approaches is a common characteristic of most sectors/countries we surveyed. However, the implementation of such compliance varies from acceptance of third-party certification to the assessment done by the licensees/end-users against their interpretation of relevant standards.

It is clear that commercial factors drive the availability of components assessed against nuclear standards. A more harmonised approach across countries that operate NPPs would increase the business case for suppliers and would make the availability of suppliers willing to support the assessment increase. Nevertheless, there are several cases where digital-COTS components are currently being used in critical safety applications, and therefore, it should be feasible to develop an approach for their justification that would be acceptable in the Nordic countries.

7 Glossary

ASIL	Automotive Safety Integrity Level
CGD	Commercial Graded Dedication
COTS	Commercial-Off-The-Shelf
EASA	European Aviation Safety Agency
FAA	Federal Aviation Administration
EPRI	Electrical Power Research Institute
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
PLC	Programmable Logic Controllers
SIL	Safety Integrity Level

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. To be published.

[2] 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-

[3] YVL B.2. Classification of systems, structure and components of a nuclear facility, 15.6.2019.

[4] International Electrotechnical Commission, IEC 62166 Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions, 2009.

[5] YVL E.7. Electrical and I&C equipment of a nuclear facility. 15.3.2019.

[6] Licensing of safety critical software for nuclear reactors - Common position of international nuclear regulators and authorised technical support organizations, Bel V, BfS, CNSC, Consejo de Seguridad Nuclear, ISTec, KAERI, KINS, NSC, ONR, SSM & STUK, http://www.onr.org.uk/software.pdf. 2018.

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

[8] Regulator task force on Safety Critical Software, rev 2018, Licensing of safety critical software for nuclear reactors. Common position of international nuclear regulators and authorised technical support organisations, report 2018:19.

[9] Office for Nuclear Regulation. Safety Assessment Principles for Nuclear Facilities, 2014 Edition, ONR, Liverpool, 2014.

[10] Office for Nuclear Regulation, Technical Assessment Guide – Computer Based Safety Systems, NS-TAST-GD-046, Rev. 5, ONR, Liverpool, 2019.

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

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

[13] International Electrotechnical Commission, IEC 61513, Nuclear Power Plants: Instrumentation and Control Systems Important to Safety, General Requirements for Systems, 2011.

[14] 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.

[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] EPRI Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications: Revision 1 to EPRI NP-5652 and TR-102260, Rep. 3002002982, EPRI, Palo Alto, CA (2014).

[18] EPRI Handbook for Evaluating Critical Digital Equipment and Systems, EPRI 1011710, EPRI, Palo Alto, CA (2005).

[19] RCC-E Design and construction rules for electrical and I&C systems and equipment. Afcen 2016.

[20] 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.

[21] Federal Ministry for the Environme4nt, nature conservation and nuclear safety, Safety Requirements for Nuclear Power Plants, SiAnf, BMU, Berlin, 2015.

[22] Kerntechnische Ausschuss (KTA), Reactor protection system and surveillance devices of the safety system, Safety Standard 3501, KTA, 2015.

[23] 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.

[24] The Association of German Engineers/Association of German Electricians, Requirements of commercial grade products and criteria for their use in the instrumentation and control systems important to safety in nuclear power plants - General part, Guideline 3528 Blatt 1, VDI/VDE, Düsseldorf/Frankfurt am Main, 2017.

[25] Canadian Standards Association Qualification of pre-developed software for use in safety-related instrumentation and control applications in nuclear power plants, N290.14-07, CSA, Mississauga, ON, 2007.

[26] Canadian Standards Association, Qualification of digital hardware and software for use in instrumentation and control applications for nuclear power plants, CSA N290.14-15, CSA, Mississauga, ON, 2015.

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

[28] CENELEC, EN 50129 – Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling, 2018.

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

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

[31] International Standards Organisation, ISO 26262 Road vehicles – Functional safety, 2011.

[32] IAEA Safety Standard SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants. 2016.

[33] S Guerra, G Flecher and N Chozos. Harmonized Component Level Safety Demonstration. Energiforsk Report 2018:475.

[34] S Guerra, S Arndt, J Eiler, R Jarrett, H Miedl, A Nack, M Nemier and P Picaa. Justification of Commercial industrial instrumentation and control equipment for nuclear power plant application. In 11th International conference on nuclear plant instrumentation, control & human-machine interface technologies (NPIC&HMIT 2019). Orlando. Florida.

Appendix A: IAEA guidance

IAEA publication on the justification of digital COTS devices [1] describes some of the challenges related to the use and justification of such devices, and suggests a justification strategy and a process for justification. It also provides guidance on how to develop and implement a justification process for digital COTS devices of limited functionality for nuclear application.

This appendix summarises the strategy and process suggested in the publication, as it is based on [34].

STRATEGY

Although typically the justification of digital COTS devices has been done considering the specific application in an NPP where the device will be deployed, this work suggests the development of a generic approach, where the digital COTS device is considered independently of the application. This allows for re-use of a significant number of the justification's activities. There will still be necessary to justify their suitability for a specific application when the device is to be deployed.

The justification of a COTS device includes the phases in Figure 1.

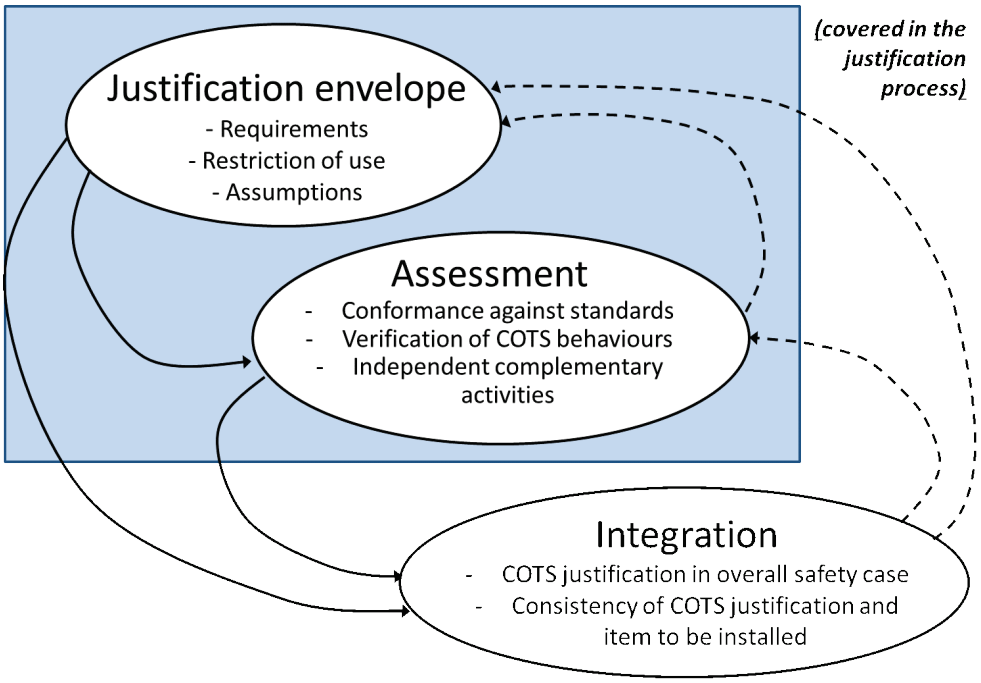


Figure 1: Typical phases of a COTS justification

The assessment phases considers the three key aspects of the strategy triangle in Figure 2.

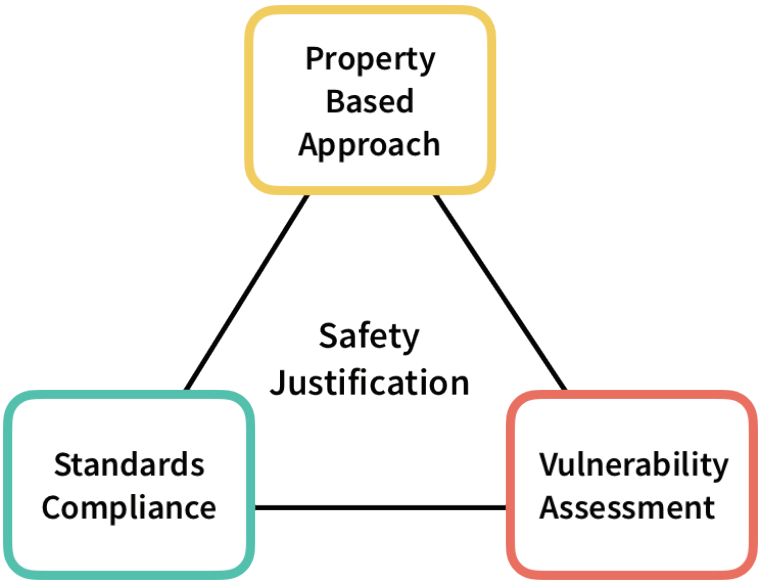


Figure 2: The strategy triangle of justification

A combination of all three perspectives provides a sound basis for an adequate justification:

- The property-based approach verifies how the key claims on the behaviour of the COTS device (e.g. safety attributes, reliability, accuracy, response time, functionality, testability, maintainability, human factors/usability) are satisfied.
- The vulnerability assessment identifies potential weaknesses in the COTS device (both in the hardware and in the software), which then need to be accepted or mitigated as part of the justification process.
- Standards compliance shows whether the COTS device satisfies the requirements of the relevant standards. It is typically focussed on the design, development and manufacturing processes.

An important part of the assessment process is to perform activities that are independent of the manufacturer. Independence from the manufacturer is important as a way of challenging and evaluating the evidence provided by the manufacturer These activities could focus on any of the perspectives of the strategy triangle (Figure 2); although usually they will address behavioural aspects, i.e., either confirm or otherwise conformance with behavioural properties or show absence of vulnerabilities.

The justification of a COTS device is concluded when the COTS device is implemented in the I&C architecture and its safety justification is integrated in the overall safety justification. This activity typically includes:

- A review of the justification in the context of the application: verify if the behaviour, restriction of use and any assumptions considered in the generic justification are suitable for the application.
- Common cause failure (CCF) analyses: the same device or devices of similar characteristics may be used in other parts of the overall I&C architecture, possibly at a different levels of the defence in depth of the plant. The impact of systematic failures of these devices at plant level should be considered.

- Application-specific vulnerability assessment: when a specific application is identified for the COTS device, an assessment of the impact of the failure modes identified in the vulnerability assessment on the plant is required.

JUSTIFICATION PROCESS

The digital device justification process consists of the following steps:

1. Definition of the requirements and prerequisites applicable to the digital COTS device
2. Selection of candidate devices
3. Establishment of (contractual) relationship with the manufacturer: agree assessment process, access to information and versions of components of the device to be justified
4. Planning the assessment
5. Assessment
6. Identification of lifetime issues
7. Production of summary justification document

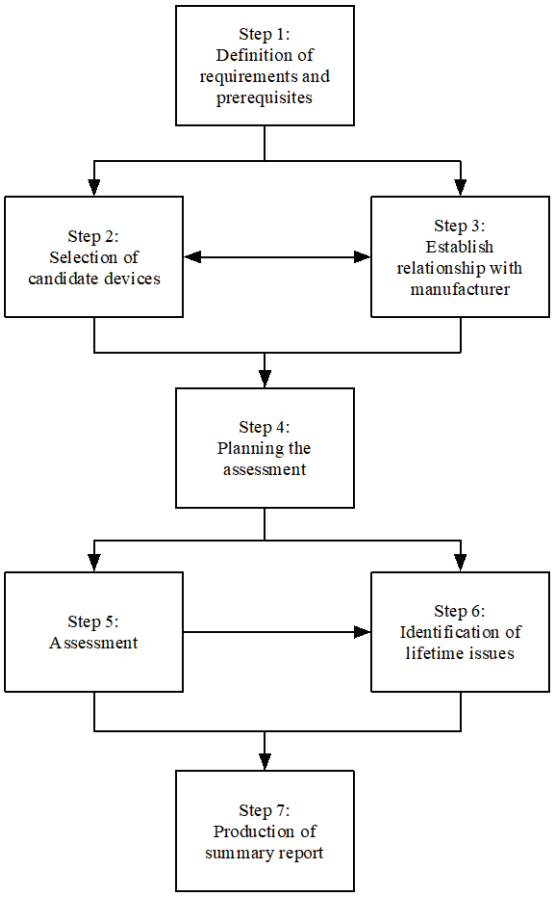


Figure 3: Justification process steps

The steps do not necessarily need to be performed strictly sequentially. For example, some steps are more likely to be performed iteratively or in parallel (e.g. Steps 2 and 3), as illustrated in Figure 3.

Table 1: Summary of justification process steps

Assessment process step	In this step:
Step 1: Definition of requirements and prerequisites	• Identify the device requirements that are necessary to be considered during the justification. • Identify the prerequisites of the device to be met by the application in order to guarantee that the requirements are achieved.
Step 2: Selection of candidate devices	• Select candidate devices. • Review the functionality and other characteristics of the device to decide whether they meet the application requirements or are of sufficient interest to perform a generic qualification. • Investigate commercial arrangement including the willingness of the manufacturer to engage with the justification process and to give access to information on the development process and design. • Assess the complexity of the devices to evaluate the likelihood of completing the justification. • Review the existing documentation to determine the likelihood of completing the justification.
Step 3: Manufacturer information and support	• Establish contractual relationship with the manufacturer. • Agree and sign an NDA, if required. • Agree the evidence and documentation that will be made available to carry out the justification. • Agree assessment process and access to information. • Agree versions of components (including software and hardware) of the device to be justified. • Agree on justification report content that users will receive (what can be shared with the user).
Step 4: Planning	• Develop the device justification plan for each of the devices selected for justification.
Step 5: Assessment	• Examine whether: – The device has been developed and manufactured using appropriate design techniques and processes that are commensurate with the safety role of the device.

Assessment process step	In this step:
	– The functional, performance and dependability behaviour meet the requirements. – Potential vulnerabilities and systematic faults have been managed. – The environmental qualification data exists that is representative of the in-service conditions. – Additional confidence is achieved through independent complementary activities.
Step 6: Identification of lifetime issues	• Identify the limitations and conditions necessary for the preservation of the behaviour properties of the component during the lifetime of the component.
Step 7: Justification documentation package	• Complete and issue the device justification report (DJR). • Identify and update user documentation and safety manual.

Step 5: Assessment is the main part of the justification process. Details on what to consider when doing the assessment are discussed in [1] and summarized in Table 2.

Table 2: Summary of Step 5 - Assessment

Assessment	Description
The device has been developed and manufactured using appropriate design techniques and processes that are commensurate with the safety role of the device.	This part of the assessment looks at the processes implemented by the manufacturer for the development and production of the COTS product and identifies any gaps in the requirements for a nuclear grade product. It includes evidence of the use of appropriate processes, techniques and tools and competent personnel. It is likely that a number of 'gaps' are identified, where the manufacturer is not able to provide evidence that a certain QA, development or manufacturing requirement was met. Gaps will need to be addressed by specific compensatory measures, or by justifying that the gap is not significant or can be mitigated, e.g. by restricting the use of the device.
The functional, performance and dependability behaviour meet the requirements.	The functional, performance and dependability assessment focusses on showing that the component meets the requirements. Evidence might exist prior to the assessment (e.g. evidence resulting from the manufacturer's quality assurance and development processes, evidence produced as part of device's certification) or may be produced for the assessment.

Assessment	Description
	The specific attributes of interest will vary with the device and the possible application that will use and may include functionality, accuracy, timing and robustness.
Potential vulnerabilities and systematic faults have been managed.	Vulnerabilities are possible defects or deficiencies in a component that could lead to a hazard or to a failure to perform the safety function. Vulnerability assessment considers those aspects of the component design and implementation technology that could commonly be a source of defects. Vulnerability assessment considers the specific characteristic of the device. It covers the specific components of the architecture, e.g. software, hardware, operating system, FPGAs, and also generic component vulnerabilities, e.g. security, modes of operation, etc. The possible hardware, software or component vulnerabilities are evaluated to determine postulated failure modes and their causes (as well as their credibility), or to provide evidence that they were considered and avoided during the design (for example, through the use of design tools and methodologies that improve the quality of the design and implementation).
The environmental qualification data exists that is representative of the in-service conditions.	A test program needs to be executed to demonstrate that the COTS device will perform its safety functional during all seismic and environmental parameters specified. The qualification program can be addressed by test, analysis or a combination of the two methods.
Additional confidence is achieved through independent complementary activities.	The justification of a COTS device includes some complementary assessment activities such as analysis and testing that are performed independently from the manufacturer. The level of independence and the specific activities to be performed will depend on the grading of the component and vary from country to country and may include: • Commissioning tests. • Source code static analyses. • Simulation-based testing. • Additional types of testing.

Appendix B: Consultation brief

- What types of COTS products are typically used in safety applications in the sector?
  - *Focus on embedded systems, or smart devices – COTS products with simple, well-defined functionality.*
  - *Focus on safety applications, particularly at Cat A/1E (nuclear) or equivalent.*
  - *As well as the functionality, consider if the COTS product is designed for the particular industry/sector in mind, or if it is more of a generic product.*
- In what applications or for what functions are they used?
  - *Again, focus on safety-critical and/or safety relevant applications. Is there grading used?*
- COTS product licensing
  - *Licensing can be considered synonymous with approval or qualification.*
- What are the regulatory requirements regarding the licensing of COTS products?
  - *These requirements might come from governmental and regulatory bodies (both national and supra-national), or from international standards.*
  - *What are these? (i.e., what boxes need to be ticked?)*
- Do the requirements identify different classes/categories/levels of licensing?
  - *Are SILs (or a related/similar concept) used? Are there different levels of criteria for more or less onerous requirements?*
- Is compliance to standards required in the licensing process?
- Do third-party certifications play a role in the licensing process?
  - *For example, third –party certifications might be those done by an independent organization (e.g., Exida, TUV) against a standard.*
  - *What is the role they play? Is a certification all that is required or is a certificate just one more piece of evidence?*
- What artefacts/evidence items are typically required during the licensing process?
  - *Particularly, is access to internal manufacturer IP (development documents) required? Is access to source code required? If so, how is access to manufacturer IP/source code arranged?*
- Are there assurance activities that must be carried out by the licensee on the product?
  - *Here we mean in addition to those already performed by the manufacturer. For example, is black-box testing or software analysis carried out?*
- Once licensed, can a COTS product be re-used in different applications?
  - *Particularly, can the product be re-used without doing another qualification? What are the requirements?*

Appendix C: Seminar on industry standard components in nuclear I&C applications

A seminar on industry standard components in nuclear I&C applications took place in Stockholm on 22 October 2019. The program is reproduced below.

9:30	**Welcome** *Monika Adsten*
9:40	**Use and licensing of COTS digital devices in safety critical industries – Project summary** *Sofia Guerra, Adelard, UK*
10:10	**Dedication of Digital COTS Components for Use in the U.S. Nuclear Industry** *Steven Arndt, NRC, US*
10:50	**Justifying COTS Products using Commercial Grade Dedication** *Andrew M Nack, Isotek Systems, LLC, US*
11:30	**Lunch**
12:20	**Use of Smart Devices in Safety Related Computers** *Kevin McKay, OPG Canada*
13:00	**Justification of COTS smart devices within EDF Energy Nuclear Generation UK** *Silke Kuball, EDF Energy, UK*
13:40	**Justification of commercial industrial instrumentation and control equipment for nuclear power plant applications – IAEA report** *Sofia Guerra, Adelard, UK*
14:10	**Coffee**
14:30	**The use of Commercial Grade Dedication in Sweden** *Pär Lansåker, Vattenfall, Sweden*
15:00	**Developing the licensing and qualification of industrial standard components in Finland – the KELPO-project** *Maria Palo, ÅF-Consult Ltd, Finland*
15:30	**Panel on challenges of licensing COTS digital components** *Steven Arndt, NRC, Mark Bowell, ONR, Silke Kuball, EDF Energy, Anders Johansson, Vattenfall*
16:15	**End of seminar**

During the seminar, the results of the project were presented. This was followed by presentations of current practices and experiences with smart devices in nuclear power plants 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 justifying smart devices, and the need for transparency of the certification process
- how to consider simplicity/complexity of devices, including the development of quantifying measures of simplicity
- harmonization of approaches across different countries

- the importance of articulating explicit claims about what the justification is trying to demonstrate
- the fact that the justification is not only a quality assurance process, and it should not be based on a tick-box approach

The IAEA report on commercial industrial instrumentation and control equipment was discussed as a way of achieving a common understanding of what is expected across a number of countries.

COTS DIGITAL DEVICES IN SAFETY CRITICAL INDUSTRIES

In this project, we reviewed the use of Commercial-Off-The-Shelf components, COTS in safety and safety related applications in both the nuclear industry and other safety-critical industries.

From our review, we have extracted several common themes. The focus of the work was on the specific aspects related to the justification of the software of the smart devices, and it does not discuss in detail aspects of the justification common to analogue devices, e.g., environmental qualification and type testing.