OVERVIEW OF APPROACHES TO THE USE AND LICENSING OF COTS DIGITAL DEVICES IN SAFETY CRITICAL INDUSTRIES

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

[Digital Object Identifier (DOI) placeholder]

ABSTRACT

Although Commercial-Off-The-Shelf (COTS) components are increasingly used in nuclear Instrumentation and Control (I&C) applications, there are several challenges related to their safety demonstration and justification. This paper describes work funded by Energiforsk that reviewed the use of COTS components in several safety applications, both within the nuclear sector and in other safety-critical sectors. The objective of the work was to investigate whether the use of COTS products in the Nordic Nuclear Power Plants (NPPs) may be feasible.

Key Words: Embedded digital devices, COTS components, safety justification approach

1 INTRODUCTION

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 chances 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.

This paper summarises a report that considered the use of COTS components in a range of safety-critical applications [1]. The scope of the work and methodology are described in Section 2. The approaches adopted in different countries to use and justify COTS components in the nuclear industry are presented in Section 3. The original work [1] also surveyed other safety-critical industries, but this is not included in this paper. The common themes that we have identified are developed and discussed in Section 4.

The study considered COTS digital industrial devices of limited functionality, also described as “smart” devices. These are digital devices that are designed to perform a specific function and are usually not programmable by the end-user. The focus was on software-specific concerns and, although hardware qualification is also an important part of the justification requirements (such as environmental and seismic tolerance), these were not considered in this study.

We performed a number of formal consultations that were structured using a set of related topics. In addition, information was gathered through 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. We are grateful to our consultees for their assistance.

2 NUCLEAR POWER INDUSTRY APPROACHES TO LICENSING OF COTS DEVICES

2.1 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, 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 qualification of smart devices should be done according to YVL E.7 [5]. For devices in safety classes 2 and 3, a qualification plan should be 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. Any deficiencies in the documentation and implementation of the design process may be substituted by analysis or testing.

The approach takes into account information and requirements of the intended application of the smart device during the qualification. 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.

2.2 Sweden

The Swedish Radiation Safety Authority (SSM) guidance provided in SSMFS 2008:1 on general advice on safety in nuclear facilities [6] states that software should be thoroughly verified and validated, and that all the development process should be planned and documented. The regulations refer to the regulator task force report on safety-critical software [7], which includes a section on the justification of smart devices. This report 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.

The 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 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.

2.3 United Kingdom

Licensees in the UK must comply with the Office for Nuclear Regulation (ONR) Safety Assessment Principles (SAPs) [8] and Technical Assessment Guides (TAGs). In particular, for computer-based safety systems, the ONR SAP clause ESS.27 states that "…compliance with appropriate standards and practices throughout the software development lifecycle should be established in order to provide assurance of the final design." The regulatory regime in the UK is largely goal based, so it is for the licensee to determine the assurance activities that must be carried out in accordance with ESS.27 and associated TAG 46 [9].

The level of justification required for a smart device depends on the safety function categories (Category A, B or C) and system classes of IEC 61226 [4] (Safety Class 1, 2 or 3). TAG 46 contains guidance for assigning reliability claims to particular devices. 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.

The safety justification of software-based systems, and COTS smart devices in particular, is divided into 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.

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" [9].

Production excellence for smart devices is typically assessed using the Emphasis approach [10], which is a questionnaire derived from IEC 61508 [11], 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 [11]) 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.

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, significant work would be required to justify the device in the new application.

2.4 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 [12]. 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 that they 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 [13] that is conditionally endorsed by US NRC Regulatory Guide 1.164. 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

The commercial dedication process assumes that suitability of the system level 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 [13] 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 referenced for accepting digital devices. EPRI, "Handbook for Evaluating Critical Digital Equipment and Systems" [14] an update to the methodology provided in EPRI TR-107339, is based around a review that seeks to establish the systematic integrity and reliability of the device. This includes a "Critical Digital Review", which assesses dependability properties in relation to the requirements made of the device.

2.5 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 several 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 [15] constitutes a technical design code for electrical and I&C systems for pressurised water reactors. The most recent versions of RCC-E include more detailed information concerning industrial digital devices of limited functionality (as defined by IEC 62671 [16] – a similar concept to smart devices), and introduce alternative qualification methods that credit IEC 61508 [11] certifications.

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. Qualification considers quality assurance processes, including verification and validation activities, 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 be more onerous 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.

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.

2.6 Germany

The German approach to qualification of digital systems is based on the requirements defined by the German government [17] and nuclear regulator [18]. The approach is based on IEC standards such as IEC 61513 [19], IEC 60880 [20] and IEC 62138 [21]. VDI/VDE 3528 [22] 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 [11]). An analysis is performed by an assessor 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 safety 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 nuclear safety function (in accordance with IEC 61226 [4]), 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 [22] sets up selection criteria for the device. These focus on the areas of documentation, technical properties, quality and operation.

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.

2.7 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 [23], which defines a process to be followed. The requirements of N290.14-15 [23] 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 [23] requires identification and categorisation of the safety functions of the candidate product. The categories map to the approach of IEC 61226 [4], with CNSC safety categories 1-3 mapped to safety Categories A-C in IEC 61226 [4]. 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, it 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 [11]. 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 (as determined by Appendix B of CSA N290.14-15), 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.

3 ANALYSIS OF APPROACHES TO LICENSING

3.1 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 [20], or generic, IEC 61508 [11]. The way that compliance was assessed, however, varied from acceptance of third-party certifications (see Section 3.2) and an assessment done entirely by the licensee (e.g., UK nuclear industry).

3.2 Use of Third-Party Certifications

Certain industries rely heavily on the use of third-party certifications for products to be used in safety applications, 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 [11], 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 countries (e.g., Germany), 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) 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 [24].

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.

3.3 Assurance Activities Independent of the Manufacturer

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.

3.4 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.

3.5 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 with 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 [25].

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.

3.6 Categorisation and Classification

Though the details of the methods vary, most safety-related sectors make use of a scheme of classification that indicates the required level of reliability or safety. The most common classification is the system of SILs defined in IEC 61508 [11]. Many nuclear industries make use of the classification and categorisation approach of IEC 61226 [4]. Additionally, many nuclear industries, including the UK and Canada, make an approximate mapping between the system classification and the required SIL.

4 CONCLUSIONS

This paper summarises the work done for Energiforsk, where we reviewed the use and safety justification of digital COTS components in a number of safety-related countries and safety-critical 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 applications 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.

5 ACKNOWLEDGMENTS

This work was funded by Energiforsk within the research program ENSRIC, Energiforsk Nuclear Safety Related Instrumentation and Control systems. The work was performed with our colleagues Dr Eoin Butler, Dr Sam George and Dr Heidy Khlaaf.

6 REFERENCES

1. E Butler, G Fletcher, S George, S Guerra and H Khlaaf. “COTS Digital Devices in Safety Critical Industries”. Energiforsk Nuclear Safety Related I&C – ENSRIC Report 2019:627, https://energiforsk.se/media/27303/cots-digital-devices-in-safety-critical-industries-energiforskrapport-2019-627.pdf.
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. STUK, “YVL B.2. Classification of systems, structure and components of a nuclear facility”, 15.6.2019.
4. International Electrotechnical Commission, IEC 61226 Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions, 2009.
5. STUK, “YVL E.7. Electrical and I&C equipment of a nuclear facility”. 15.3.2019.
6. SSM, SSMFS 2008:1 The Swedish Radiation Safety Authority’s Regulations concerning Safety in Nuclear Facilities, ISSN 2000-0987.
7. Bel V, BfS, CNSC, Consejo de Seguridad Nuclear, ISTec, KAERI, KINS, NSC, ONR, SSM & STUK, “Licensing of safety critical software for nuclear reactors - Common position of international nuclear regulators and authorised technical support organizations”, http://www.onr.org.uk/software.pdf. 2018:19.
8. ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Liverpool, 2014.
9. ONR, “Technical Assessment Guide – Computer Based Safety Systems”, NS-TAST-GD-046, Rev. 5, Liverpool, 2019.
10. 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.

11. International Electrotechnical Commission, IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, 2010.
12. U.S. NRC, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Facilities”, U.S. Code of Federal Regulations, Title 10, Chapter 1, Appendix B to Part 50, Office of the Federal Register, National Archives and Records Administration, U.S. Government Printing Office, Washington, DC.
13. EPRI, “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).
14. EPRI, “EPRI Handbook for Evaluating Critical Digital Equipment and Systems”, EPRI 1011710, EPRI, Palo Alto, CA (2005).
15. Afcen, “RCC-E Design and construction rules for electrical and I&C systems and equipment” 2016.
16. 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.
17. Federal Ministry for the Environment, nature conservation and nuclear safety, “Safety Requirements for Nuclear Power Plants”, SiAnf, BMU, Berlin, 2015.
18. Kerntechnische Ausschuss (KTA), “Reactor protection system and surveillance devices of the safety system”, Safety Standard 3501, 2015.
19. International Electrotechnical Commission, IEC 61513, Nuclear Power Plants: Instrumentation and Control Systems Important to Safety, General Requirements for Systems, 2011.
20. 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.
21. 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.
22. 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.
23. 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.
24. IAEA Safety Standard SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants. 2016.
25. S Guerra, G Fletcher and N Chozos. “Harmonized Component Level Safety Demonstration”. Energiforsk Report 2018:475.