JUSTIFICATION OF COMMERCIAL INDUSTRIAL INSTRUMENTATION AND CONTROL EQUIPMENT FOR NUCLEAR POWER PLANT APPLICATIONS

Sofia Guerra
Adelard LLP
24 Waterside, 44-48 Wharf Road, London N1 7UX, UK
aslg@adelard.com

Steven Arndt
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555, USA
steven.arndt@nrc.gov

Janos Eiler
International Atomic Energy Agency
Vienna International Centre, 1400 Vienna, Austria
j.eiler@iaea.org

Ron Jarrett
Tennessee Valley Authority
Chattanooga, TN 37363, USA
rajarrett@tva.gov

Horst Miedl
TÜV Rheinland
85399 Hallbergmoos, Germany
horst.miedl@de.tuv.com

Andrew Nack
Paragon
Knoxville, TN 37922, USA
ANack@ParagonE.S.com

Paolo Picca
Office of Nuclear Regulation
4N.1 Redgrave Court, Merton Road, Bootle, L20 7HS, UK
Paolo.picca@onr.gov.uk

ABSTRACT

This paper discusses work done by the authors to develop an IAEA Nuclear Energy Series report to provide guidance on what would constitute an adequate justification process for a COTS device to be installed in a NPP for important to safety applications such that there is reasonable assurance of high quality and that the application of the COTS does not introduce new, unanalysed failure modes. The publication provides a process for justification of digital COTS devices that may be used to guide the incorporation of these devices into the design of I&C systems important to safety, such that there is sufficient evidence to demonstrate that these products have adequate integrity to meet the requirements for their intended nuclear applications.

Key Words: Justification, Dedication, Commercial Grade, COTS

1 INTRODUCTION

Historically, instrumentation and control (I&C) systems in nuclear power plants (NPPs) were custom-developed to implement functions important to safety and specifically to meet nuclear quality assurance requirements. They originally used conventional analog technology. The gradual decrease of market availability of nuclear qualified products and the worldwide transition to digital technology, resulting in more rapid obsolescence, have made NPP designers increasingly integrate commercial I&C products within new development or modernization projects. NPP designers and operators are increasingly expressing the desire to use these commercial off-the-shelf (COTS) digital devices (including systems, components and sub-components) in safety or safety-related applications as economic alternatives to custom-designed nuclear grade systems and equipment. The incentives for the adoption of digital technology in systems important to safety at NPPs are strong. COTS products can offer such benefits as an extensive history of operation, a large installed user base, improved reliability with a proven operating history, self-monitoring and a larger group of technical personnel experienced with them. A COTS device also provides solutions to address user obsolescence and lack of spare parts issues.

The use of COTS devices in safety-related applications, however, raises concerns because their quality and reliability have not been demonstrated or documented throughout their development in strict accordance with nuclear standards. Prior to use in a NPP, there is a need to demonstrate that COTS digital devices adhere to the functional, safety and environmental requirements with an equivalent level of quality and reliability to a comparable nuclear product. Some special considerations need to be given to using products based on digital technology in NPPs because they may be subject to unique vulnerabilities and failure modes that will need to be evaluated in the context of how these products are to be used in the NPP. It should be recognized that many traditionally non-digital products (e.g. sensors, motor-control centres, device actuators, panel displays, and even power supplies) offered in the commercial market now often include embedded digital devices (EDDs) even though this may not be evident. How these products may be affected by external environmental conditions present in NPPs such as heat, humidity, vibration, and electro-magnetic interference needs to be thoroughly evaluated and tested to ensure that the components will behave in a known and predictable manner, especially under failure conditions.

This paper summarizes an IAEA publication on the justification of digital COTS devices. The IAEA publication describes some of the challenges related to the use and justification of such devices, suggests a justification strategy and a process for justification.

2 CHALLENGES

With the benefits of using COTS devices come challenges in the justification process and the maintenance of the justification. This section discusses some of the challenges in the justification and application of COTS devices and points to potential solutions.

2.1 Challenges in the Use of Digital COTS Devices

The scope of this work is limited to digital devices of limited functionality and is aligned with IEC 62671 [1]. The introduction of software adds the potential for undefined states of operation and failure modes. In addition, digital components have a significant variation of complexity due to the ability to add increased functionality and diagnostics. The complexity level applicable to the specific safety function should be evaluated prior to beginning the justification processes to ensure the digital component is not too complex for justification. Even with limited functionality, with respect to a specific safety function along with restrictive configurability, the actual COTS device can be too complex for use.

The application of digital devices to perform redundant safety functions challenges the independence of the built-in redundancy. By having the same software in redundant components/systems, this subjects the safety function to a potentially fatal software flaw triggered by a common cause. In general, CCF is a matter associated with a potentially new failure mode at the system or plant level application that has not been previously analysed. The potential for CCF needs to be assessed and the justification should provide evidence to support the user's assessment that failures due to CCF are sufficiently low [2].

2.2 Hardware and Software Vulnerabilities

Due to the added complexity of digital devices and the possibility of new failure mechanisms (e.g. infinite loop states) and modes (e.g. silent lock-ups), a failure and/or hazards analysis of the COTS device should be performed. These types of analyses can be very challenging due to the complexity and skill set required to perform them.

As digital content has become increasingly available and more cost effective to incorporate into devices, many analog components are being replaced with digital devices that are able to offer more options, reduce subcomponent part counts, and provide increased configurations at a reduced cost to the manufacturer. Since the device function remains the same, the product literature and part number for the device may not be revised to reflect this change. If the digital subcomponent(s) are not identified, its (their) digital/software quality would not be assessed, and the COTS device may have new failure mechanisms and modes that were not considered.

All COTS devices are vulnerable to counterfeit activities especially as procurement has become more global. Counterfeit devices are those that are fraudulently represented as a genuine item from the manufacturer and the definition is not limited to the final product assembly but also the sub-components and raw materials. This also increases the risk of malware to be inserted into the device.

Since COTS devices may not be designed with established computer security requirements, measures should be implemented in order to provide protection of the digital device from malicious activity for both external and internal threats. Computer security vulnerabilities can occur or be introduced at the manufacture, in shipment, and at the user's facility, so multiple reviews and assessments for vulnerabilities and mitigation activities will be required.

2.3 Organisational Challenges

As the trend moves from justifying analog components to justifying digital components, a new quality aspect is added to the justification process involving the design architecture and software development process. The user needs to align the COTS safety function and the digital specific requirements to the assessor's COTS justification. This should be in a contractual form to ensure implementation of requirements by the assessor.

Assessment of the COTS design, development and manufacturing information is essential to justification tasks. Being a commercial product, development activities can widely vary from manufacturer to manufacturer. In addition, for COTS manufacturers, design information will most likely be sensitive Intellectual Property (IP) and protected by the manufacturer. However, it will not be possible to complete the justification without sufficient evidence to support the assessment.

Users and stakeholders plan and conduct justifications by using a combination of various methodologies. It is expected to involve competence and experienced personnel supported by an adequate quality system.

3 STRATEGY

The flowchart in Figure 1 presents the typical phases expected in the justification of a COTS device. The integration of the COTS device justification in the overall safety justification is not addressed in the justification process because expectations for the safety justifications in various countries are different.

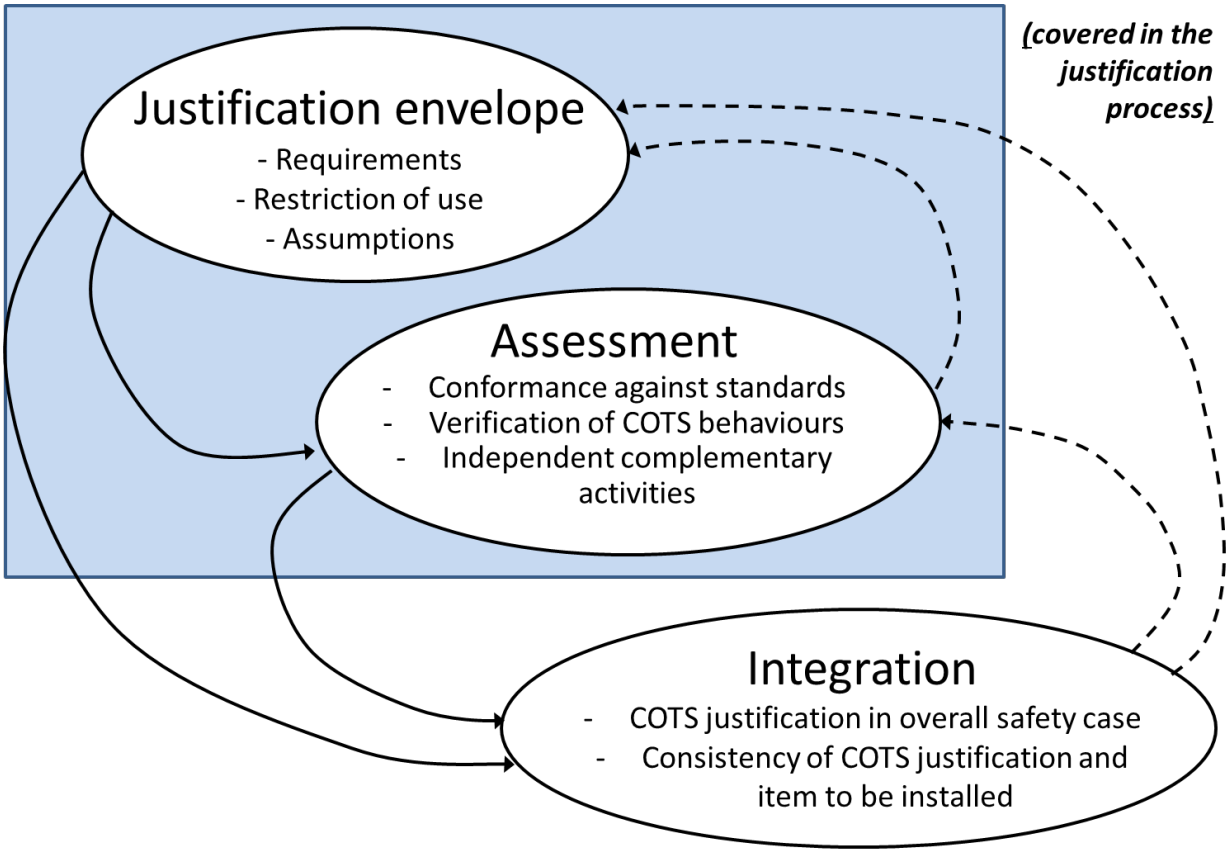

Figure 1. Typical flowchart for a COTS justification

The acceptability of a digital COTS device for a given nuclear application needs to address both nuclear safety and security. Whilst they could, in principle, be justified separately, there is an advantage for them to be covered at the same time because the same key documentation and the availability of the manufacturer to clarify aspects of the design or of the development process are required for both.

Although typically the justification of digital COTS devices has been done considering the specific application in a 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 reuse of a significant number of the justification's activities. It 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 has a meaning only when its domain of validity (or justification envelope) is specified [1]. A clear definition of the envelope is vital to ensure that the assessment is complete and that the COTS device is suitable for the specific application. The definition of the justification envelope may also depend on whether the justification is intended to be generic or application specific. For a generic justification, the assessor typically wants to keep the envelope of the justification as large as possible.

The strategy triangle in Figure 2 [3] identifies three key aspects that are generally relevant in a safety justification.

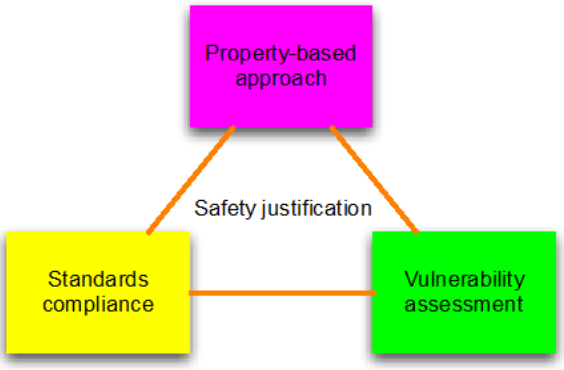

Figure 2. The strategy triangle of justification

A combination of all of the 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.
- The standards compliance shows whether the COTS device satisfies the requirements of the relevant standards. It is typically focused on the design, development and manufacturing processes.

An important part of the assessment process is to perform activities that are independent of the manufacturer [4]. Independence from the manufacturer is important as a way of challenging and evaluating the evidence provided by the manufacturer. The type of activities performed varies from country to country. While under certain regulatory regimes this may consist of commissioning, black-box testing or independent technical review of activities performed by the manufacturer, for other countries the review may be commensurate with the safety class of the system and could range from commissioning at lower safety classes, to extensive additional static/dynamic analyses at the higher safety classes.

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.

4 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: agreed assessment process, access to information on the device to be justified;
4. Planning the assessment;

5. Assessment;
6. Identification of lifetime issues;
7. Production of summary justification document.

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

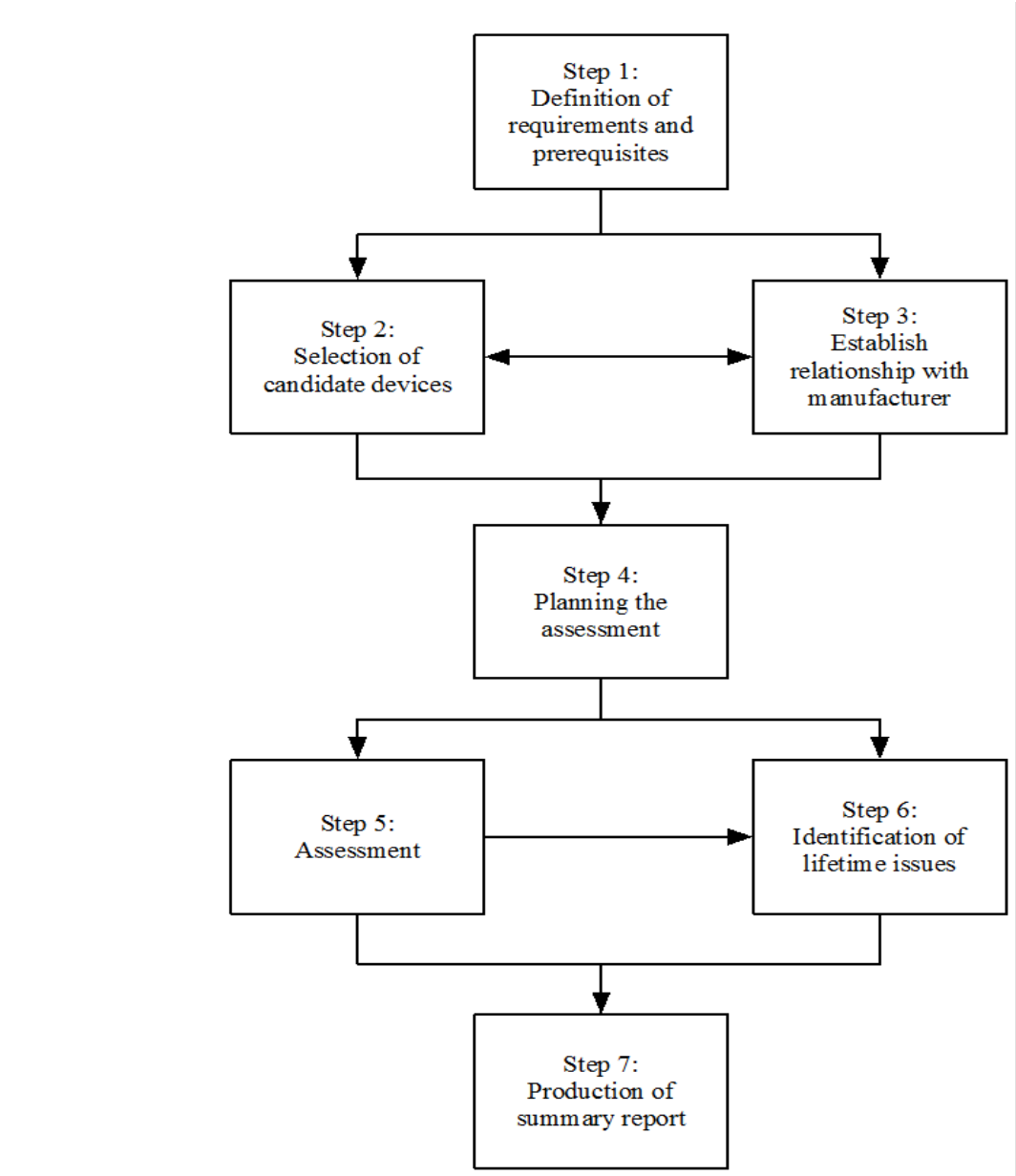

Figure 3. Justification process steps

4.1 Step 1: Definition of Requirements and Prerequisites

In this step:

- Identify the device requirements that are necessary to be considered during the justification and

- Identify the prerequisites of the device to be met by the application in order to guarantee that the requirements are achieved.

An essential input to evaluating a device is to identify all the requirements that will need to be considered during the justification to provide reasonable assurance that the device is capable of performing its intended safety function(s). The requirements definition will include the functional, performance and dependability requirements as well as the system class [5, 6, 7]. The justification of the device will be based on the requirements identified in this step, and it will evaluate the device against these requirements (either for the target application or those considered for a generic justification).

The description also needs to specify the prerequisites of the device to be met by the application in order to guarantee that the described behaviour is achieved (e.g. power, environmental constraints or operational requirements).

Documenting these requirements and prerequisites will be the basis to the justification process to ensure that the justification will provide reasonable assurance that the COTS device will and can perform the safety function over the defined range of use and the specific environmental conditions [8].

4.2 Step 2: Selection of Candidate Devices

In this step:

- 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 a successful justification;
- Review the existing documentation to determine the likelihood of completing a succesful justification.

The selection of the device is based on the functionality and other behavioural characteristics (such as performance and dependability) it is capable of, as well as the information available to support the justification. The availability of information depends on the willingness of the manufacturer to engage with the assessment and make available documentation, operating history or the source code.

The complexity of the architecture and design of the device will also have an impact of the likelihood of success in justifying them. Although the boundary for complexity is difficult to define, it is useful to have an initial assessment to identify the high-risk areas in its design, and reject any devices that are clearly too complex to be able to justify.

4.3 Step 3: Manufacturer Information and Support

In this step:

- Establish contractual relationship with the manufacturer;
- Agree and sign a non-disclosure agreement, if required;
- Agree the evidence and documentation that will be made available to carry out the justification;
- Agree the 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).

It is necessary to agree with the manufacturer the level of information that will be made available (e.g. detailed design information, verification and validation records or even the source code of the device) and

the manufacturer resources necessary to support the justification (e.g. support an audit to the factory or answering any questions that may arise from the analysis performed).

At the end of Steps 2 and 3, there will be one or more devices that have been selected.

4.4 Step 4: Planning

In this step, develop the device justification plan (DJP) for each of the devices selected for justification.

The DJP documents the feasibility of the justification and the methods to be used, taking into account factors such as technologies used to implement the device, the development process followed, operating data available and any existing certification. It also explains how the activities planned will meet any considered national approaches, and that any areas not covered are identified and a rationale is given for their omission.

4.5 Step 5: Assessment

In this step, the assessment is carried out to 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;
- The functional, performance and dependability behaviour meet the requirements;
- Potential vulnerabilities and systematic faults have been managed;
- The environmental qualification data that is representative of the in-service conditions exists;
- Additional confidence is achieved through independent complementary activities.

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 [1, 6, 7, 9]. It includes evidence of the use of appropriate processes, techniques and tools and competent personnel.

The functional, performance and dependability assessment focuses 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 the device's certification) or may be produced for the assessment.

The specific attributes of interest will vary with the device and the possible application and may include functionality, accuracy, timing and robustness. Some of the evidence may be related to the hardware, some related to the software, and some to the integration or the component as a whole.

Vulnerabilities are possible defects or deficiencies in a component that could lead to a hazard or to a failure to perform the safety function. A vulnerability assessment considers those aspects of the component design and implementation technology that could commonly be a source of defects.

A 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 consequences of these failure modes must then be evaluated to identify preventative and mitigating measures that may be used to offset these vulnerabilities.

As part of the justification program, a qualification program needs to be executed to demonstrate that the COTS device will perform its safety function during all seismic and environmental parameters specified. The qualification program can be addressed by test, analysis or a combination of the two methods, for

example, in accordance with IEC/IEEE 60780/323 [10], RG 1.209 [11] (Digital), IEC 61000 [12] (EMI/RFI), EPRI TR-102323 [13] or RG 1.180 [14] (EMC) and IEEE 344 [15] (Seismic).

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.

The general principle is that the end user will perform (or commission) assessment to challenge the assessment performed by the manufacturer. Depending on the grading of the component and the national practices, this may include:

- Commissioning tests;
- Source code static analyses;
- Simulation-based testing;
- Additional types of testing.

4.6 Step 6: Identification of Lifetime Issues

In this step, identify the limitations and conditions necessary for the preservation of the behavioural properties of the component during the lifetime of the component.

The suitability assessment considers the behaviour of the device at the time of commissioning. However, after installation, any product is subject to changes both internally and in its operating context (material aging mechanisms, environment, the operators and their management, the requirements placed on it, etc.). Therefore, it is important to consider the preservation of suitability during the lifetime of the component. This will include demonstrating that each change, be it deliberate, planned, accidental, or out of the users' control, can be appropriately managed in order to keep the component's behaviour within acceptable boundaries.

From the manufacturer's point of view, evidence will be primarily process-based. Ideally, the manufacturer would demonstrate that they have procedures in place to maintain the technical know-how and the resources to ensure that adequate support can be provided to the end user during the product's life.

From the application point of view, the end user will be required to produce evidence that there are arrangements in place to maintain the behaviour of the product in its application environment. Evidence for this may involve the operating and maintenance procedures and appropriate security provisions.

4.7 Step 7: Justification Documentation Package

In this step:

- Complete and issue the device justification report (DJR);
- Identify and update user documentation and safety manual.

The device justification report has to be completed and issued following a process of review, comments and challenging. The DJR will refer to a number of documents produced during the justification, as well as evidence that existed before the justification started (including manufacturer's documents and any existing certification).

5 MAINTENANCE OF JUSTIFICATION

Once a device has been successfully justified, care must be taken to maintain the integrity and validity of that justification in respect to the future items that are procured and installed in the end use applications. Changes to the hardware, software, or manufacturing process all have the potential to invalidate the

justification and may cause additional actions to be taken to re-establish it. Figure 4 illustrates what this process typically consists of.

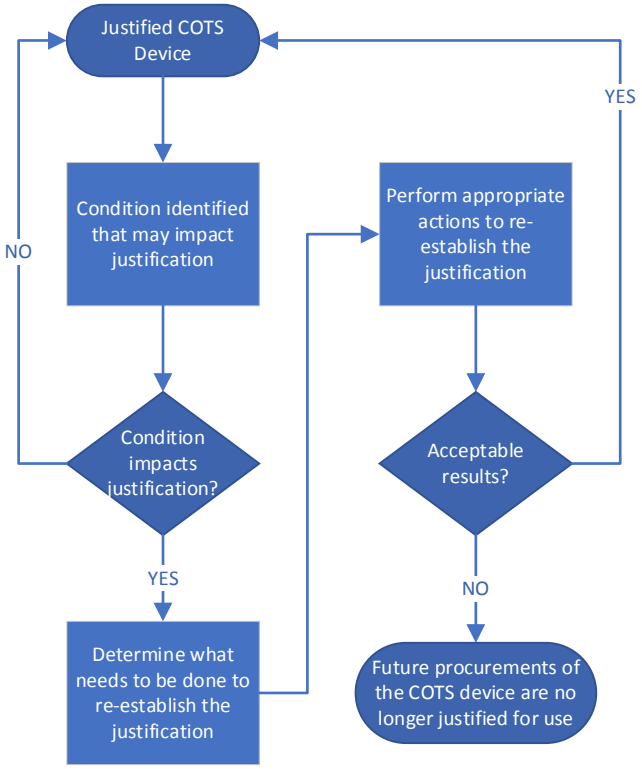

Figure 4. Typical process for maintaining the justification

5.1 Change Management and Deficit Reporting

An agreement will exist between the manufacturer and the end user (or assessor), so that the manufacturer will provide notification if any changes are made, or if any design defects are identified. If the notification agreement is between the manufacturer and the assessor, the assessor is then responsible for forwarding on the notification to the end user.

Certified COTS devices may possess certificates with a time-limited validity. At the end of the validity period, the third-party certifier re-evaluates the certificate. In case of changes of COTS devices or of their components, the effects of these changes with respect to the original COTS device certification are to be analysed and assessed. The modifications have to be evaluated with respect to the components' function and interfaces. The accumulation of many minor changes on the same part may result in the need for supplementary certification. Any circumstances that lead to a change in certification will most likely lead to a need to re-evaluate the justification. Major changes such as a new component part or a limited modification in software functional requirements may result in the need for a supplementary certification. Essential changes as in hardware or software design criteria or properties, or a new CPU, will probably result even in a new certification. There might be other reasons to question the COTS device's certification, e.g. changes in manufacturer or supplier competence affecting e.g. the manufacturing process, or adverse

observations coupled to the COTS device. In addition, new standards and regulations may invalidate a previously obtained COTS device certification.

Some regulatory frameworks require suppliers of nuclear grade items (e.g. basic components as defined by US Title 10 CFR Part 21 [16]) to report the identification of defects that have the potential to cause significant safety concerns. It is important to communicate with manufacturers the importance of notifying the assessor in a timely manner. When the potential of a significant safety concern exists, it would not be considered acceptable to wait for a regular auditing activity to share that new defect information. It is best not to depend on the manufacturer to evaluate whether a defect can result in a significant safety concern. That evaluation would be the responsibility of the entity that holds the defect reporting responsibility within the regulatory framework (e.g. the assessor). It is best to arrange for the manufacturer to notify the assessor (e.g. assessor) of all defects and design changes.

5.2 Periodic Quality Assurance Measures

When audits or certifications of the manufacturer's processes are part of the basis for the justification and repetitive procurements are made, a periodic schedule is recommended to be established to repeat some or all the original audit scope to ensure the manufacturer is continuing to maintain compliant processes. These activities are helpful also to keep the manufacturer mindful of reporting defects and design changes to the assessor.

5.3 Configuration Management

The assessor tracks the software and hardware versions that have been justified. Typically, efforts are made to encourage manufacturers to maintain the previously justified versions (unless defects are identified), but changes are expected concerning a COTS item. A common driver of changes is obsolescence of subcomponents and periodic communication with the manufacturer can be helpful to anticipate such issues. A methodology for evaluating the changes should be established.

It is common for manufacturers to identify multiple subcomponents as acceptable for use within their hardware designs and include all those subcomponents in their bill of materials (BOM). It is possible that the environmental conditions of the end-use application, targeted by the justification, impose tighter requirements on the BOM than what the manufacturer originally considered. For these scenarios, qualification testing may need to include the multiple hardware variations, or tighter BOM controls must be arranged with the manufacturer.

The ease of detecting hardware changes is often dependent on the transparency of the manufacturer. Typically, only very significant hardware changes will cause the part number of the item to change. If a manufacturer is very disciplined with configuration management and change reporting, then it may be able to be trusted to identify hardware changes. If the manufacturer is not so disciplined, side by side hardware comparisons between the original item justified and the new item may be necessary.

When evaluating hardware changes, the German nuclear guideline KTA 3507 [17], for example, considers four types: i) original equipment, ii) same type of equipment but from a different component manufacture, iii) different type of component with equivalent properties, and iv) different type of component part with different properties. According to the type, different measures (e.g. supplementary type testing) may be required to re-validate the justification.

Software changes can usually be detected through changes in the version number. If the version number is not clearly labelled on the item or declared by the manufacturer, then it may be necessary to perform a checksum or hash verification of the stored firmware in memory to monitor for changes. When any software changes are detected, an impact assessment should be initiated. Software changes usually require re-working some of the activities that provide the basis of the justification unless it can be shown that they do not call into question any of those previously performed activities and have no impact on the integrity of

the previously established justification basis.

6 CONCLUSIONS

Digital COTS components are increasingly being used in NPPs, as they provide several advantages compared to custom designed devices developed to nuclear standards (e.g. cost, time to market, operational experience) and because of obsolescence issues with their analog counterparts. However, the justification of their use in nuclear safety applications can be challenging due to a number of factors including the complexity inherent to digital technologies, the fact that they were not developed to nuclear standards and may not have the needed documentation of their development, and the need to access sensitive intellectual property information from the manufacturer (e.g. development processes and design documentation).

The aim of this paper and the IAEA publication on the justification of digital COTS devices is to describe some of the challenges related to the justification and use of such devices and to suggest a justification strategy. It also provides guidance on how to develop and implement a justification process for digital COTS devices of limited functionality for nuclear applications.

7 ACKNOWLEDGMENT

The authors wish to acknowledge the valuable contribution made by Marie S. Nemier, Qualtech (USA) as the original chair of the working group. Very unfortunately, she passed away while this project was under way.

8 REFERENCES

1. *International Electrotechnical Commission, Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Selection and Use of Industrial Digital Devices of Limited Functionality,* IEC Standard 62671, IEC, Geneva (2013).
2. *International Electrotechnical Commission, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, IEC Standard 61508, IEC, Geneva (2010).
3. *International Atomic Energy Agency, Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plants*, IAEA Nuclear Energy Series No. NP-T-3.27, IAEA, Vienna (2018).
4. "Licensing of safety critical software for nuclear reactors, Common position of international nuclear regulators and authorised technical support organisations", Revision 2018 (also known as the 7 party paper), http://www.onr.org.uk/software.pdf (2018).
5. *International Atomic Energy Agency, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series No. SSG-30,* IAEA, Vienna (2014).
6. *Institute of Electrical and Electronics Engineers, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Standard 603*, IEEE, New York (1998).
7. *International Electrotechnical Commission, Nuclear Power Plants: Instrumentation and Control Systems Important to Safety, General Requirements for Systems*, IEC Standard 61513, IEC, Geneva (2011).
8. *Nuclear Regulatory Commission, Dedication of Commercial-Grade Items for Use in Nuclear Power Plants, Regulatory Guide 1.164*, US NRC, Washington, DC (2017).

9. *Institute of Electrical and Electronic Engineers, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*, IEEE Standard 7-4.3.2-2003, IEEE, New York (2003).
10. *Institute of Electrical and Electronics Engineers, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations*, IEEE Standard 323-1974, IEEE, New York (1974).
11. *Nuclear Regulatory Commission, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants, Regulatory Guide 1.209*, US NRC, Washington, DC (2006).
12. *International Electrotechnical Commission, "Electromagnetic Compatibility (EMC), IEC Standard 61000*, IEC, Geneva (2001).
13. *Electric Power Research Institute, Guidelines for Electromagnetic Interference Testing in Power Plants, EPRI TR-102323*, EPRI, Palo Alto, CA (1994).
14. *Nuclear Regulatory Commission, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems, Regulatory Guide 1.180*, US NRC, Washington, DC (2003).
15. *Institute of Electrical and Electronics Engineers, IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, IEEE Standard 344-2004,* IEEE, New York (2004).
16. *Nuclear Regulatory Commission, Reporting of Defects and Noncompliance, 10 CFR 21*, US NRC, Washington, DC (2015).
17. *Kerntechnischer Ausschuss, Factory Tests, Post-Repair Tests and the Certification of Proven Performance of Modules and Devices of the Instrumentation and Control System Important to Safety, Safety Standard 3507*, KTA, Salzgitter (2014).