IAEA Nuclear Energy Series

No. NR-T-3.31

Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for Use in Nuclear Power Plant Applications

IAEA
International Atomic Energy Agency

IAEA NUCLEAR ENERGY SERIES PUBLICATIONS

STRUCTURE OF THE IAEA NUCLEAR ENERGY SERIES

Under the terms of Articles III.A.3 and VIII.C of its Statute, the IAEA is authorized to "foster the exchange of scientific and technical information on the peaceful uses of atomic energy". The publications in the **IAEA Nuclear Energy Series** present good practices and advances in technology, as well as practical examples and experience in the areas of nuclear reactors, the nuclear fuel cycle, radioactive waste management and decommissioning, and on general issues relevant to nuclear energy. The **IAEA Nuclear Energy Series** is structured into four levels:

(1) The **Nuclear Energy Basic Principles** publication describes the rationale and vision for the peaceful uses of nuclear energy.

(2) **Nuclear Energy Series Objectives** publications describe what needs to be considered and the specific goals to be achieved in the subject areas at different stages of implementation.

(3) **Nuclear Energy Series Guides and Methodologies** provide high level guidance or methods on how to achieve the objectives related to the various topics and areas involving the peaceful uses of nuclear energy.

(4) **Nuclear Energy Series Technical Reports** provide additional, more detailed information on activities relating to topics explored in the **IAEA Nuclear Energy Series**.

The IAEA Nuclear Energy Series publications are coded as follows: **NG** – nuclear energy general; **NR** – nuclear reactors (formerly **NP** – nuclear power); **NF** – nuclear fuel cycle; **NW** – radioactive waste management and decommissioning. In addition, the publications are available in English on the IAEA web site:

www.iaea.org/publications

For further information, please contact the IAEA at Vienna International Centre, PO Box 100, 1400 Vienna, Austria.

All users of the IAEA Nuclear Energy Series publications are invited to inform the IAEA of their experience for the purpose of ensuring that they continue to meet user needs. Information may be provided via the IAEA web site, by post, or by email to Official.Mail@iaea.org.

CHALLENGES AND APPROACHES FOR SELECTING, ASSESSING AND QUALIFYING COMMERCIAL INDUSTRIAL DIGITAL INSTRUMENTATION AND CONTROL EQUIPMENT FOR USE IN NUCLEAR POWER PLANT APPLICATIONS

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BARBADOS
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D’IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ESWATINI
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GRENADA
GUATEMALA
GUYANA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE’S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORTH MACEDONIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAINT LUCIA
SAINT VINCENT AND THE GRENADINES
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
TURKMENISTAN
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VANUATU
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency’s Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is “to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world’’.

IAEA NUCLEAR ENERGY SERIES No. NR-T-3.31

CHALLENGES AND APPROACHES FOR SELECTING, ASSESSING AND QUALIFYING COMMERCIAL INDUSTRIAL DIGITAL INSTRUMENTATION AND CONTROL EQUIPMENT FOR USE IN NUCLEAR POWER PLANT APPLICATIONS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2020

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 26007 22529
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
www.iaea.org/publications

Printed by the IAEA in Austria
September 2020
STI/PUB/1871

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Challenges and approaches for selecting, assessing and qualifying commercial industrial digital instrumentation and control equipment for use in nuclear power plant applications / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2020. | Series: International Atomic Energy Agency, ISSN 1995–7807 ; no. NR-T-3.31 | Includes bibliographical references.
Identifiers: IAEAL 20-01343 | ISBN ISBN 978–92–0–105019–9 (paperback : alk. paper) | ISBN 978–92–0–109920–4 (pdf) | ISBN 978–92–0–110020–7 (epub) | ISBN 978–92–0–110120–4 (mobipocket)
Subjects: Nuclear power plants — Instruments. | Nuclear power plants — Electronic equipment. | Digital control systems. | Commercial products.
Classification: UDC 621.039.56 | STI/PUB/1871

FOREWORD

One of the IAEA's statutory objectives is to "seek to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world." One way this objective is achieved is through the publication of a range of technical series. Two of these are the IAEA Nuclear Energy Series and the IAEA Safety Standards Series.

According to Article III.A.6 of the IAEA Statute, safety standards establish "standards of safety for protection of health and minimization of danger to life and property". The safety standards include the Safety Fundamentals, Safety Requirements and Safety Guides. These standards are written primarily in a regulatory style, and are binding on the IAEA for its own programmes. The principal users are the regulatory bodies in Member States and other national authorities.

The IAEA Nuclear Energy Series comprises reports designed to encourage and assist R&D on, and practical application of, nuclear energy for peaceful uses. This includes practical examples to be used by owners and operators of utilities in Member States, implementing organizations, academia and government officials, among others. This information is presented in guides, reports on technology status and advances, and best practices for peaceful uses of nuclear energy based on inputs from international experts. The IAEA Nuclear Energy Series complements the IAEA Safety Standards Series.

The focus of this publication is on the justification of digital commercial off the shelf (COTS) devices with limited functionality for use in safety applications of industrial nuclear facilities. Numerous plants in a number of Member States are currently in the process of replacing analogue instrumentation and control equipment with new digital devices (e.g. to address obsolescence as well as to take advantage of the greater capabilities of digital devices). Digital equipment is also proposed for safety applications in new build projects. The use of COTS devices is appealing because of their reduced cost and time to market compared with nuclear grade devices and the significant operational experience often available from their use in other industries. However, their implementation in a nuclear safety application needs to be justified to identify potential vulnerabilities and to minimize the risk for their systematic failures. The literature is limited on the justification of digital COTS devices with limited functionality.

This publication discusses the key challenges associated with the use of digital COTS devices in nuclear applications. The publication outlines the overall strategy for COTS device justification and identifies its interface with the overall safety justification at the plant level. It also discusses key steps in assessing a digital COTS device and managing changes to the device. Examples of practices in various Member States are available in the annexes. The primary intent of this publication is to provide a starting point for Member States to develop or improve their processes for justifying the use of digital COTS devices. The information provided may be particularly useful to licensees and COTS device assessors when engaging with manufacturers during the justification process.

This publication was written by a committee of international experts and advisers from numerous countries. The IAEA wishes to acknowledge the valuable assistance provided by the contributors and reviewers listed at the end of the report, especially the contributions made by M.S. Nemier (United States of America) and P. Picca (United Kingdom) as the co-chairs of the authoring group. The IAEA officer responsible for this publication was J. Eiler of the Division of Nuclear Power.

EDITORIAL NOTE

Guidance provided here, describing good practices, represents expert opinion but does not constitute recommendations made on the basis of a consensus of Member States.

This report does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

The IAEA has no responsibility for the persistence or accuracy of URLs for external or third party Internet web sites referred to in this book and does not guarantee that any content on such web sites is, or will remain, accurate or appropriate.

CONTENTS

1. INTRODUCTION 1

1.1. Background 1
1.2. Objective 2
1.3. Scope 3
1.4. Structure 4

2. CHALLENGES ASSOCIATED WITH COMMERCIAL INDUSTRIAL DIGITAL INSTRUMENTATION AND CONTROL EQUIPMENT 5

2.1. Challenges in the use of commercial off the shelf devices 5
2.1.1. Complexity of the component, multifunction, primary and support functions 5
2.1.2. Common cause failure considerations 6
2.2. Specific hardware and software vulnerabilities of digital commercial off the shelf devices 6
2.2.1. Potential new failure modes and hazards 6
2.2.2. Identification of embedded digital devices with undeclared content 6
2.2.3. Counterfeit, fraudulent and suspect items 7
2.2.4. Computer security considerations 7
2.3. Organizational challenges 7
2.3.1. Procurement and definition of safety requirements with contractual ties 7
2.3.2. Device selection 7
2.3.3. Generic and limited justification/qualification. 8
2.3.4. Evidence required to address the commercial off the shelf device's justification 8
2.3.5. Change management 9
2.3.6. Lack of qualified and experienced personnel. 10

3. STRATEGY FOR THE JUSTIFICATION OF COMMERCIAL INDUSTRIAL INSTRUMENTATION AND CONTROL EQUIPMENT 10

3.1. Key elements to consider in the definition of the justification strategy 11
3.1.1. Definition of the justification envelope 12
3.1.2. Assessment of a commercial off the shelf device 13
3.1.3. Integration of the commercial off the shelf device in the overall instrumentation and control architecture. 15
3.2. Other considerations for defining a justification strategy 17
3.2.1. Evidence 17
3.2.2. Selection of personnel involved in the justification 19
3.2.3. Graded approach. 20
3.2.4. Generic versus specific justifications of a commercial off the shelf device 20
3.2.5. Computer security 21
3.2.6. Engineering judgement. 22

4. JUSTIFICATION PROCESS 22

4.1. Step 1: Defining requirements and prerequisites 22
4.2. Step 2: Selecting candidate devices. 24
4.3. Step 3: Obtaining manufacturer information and support. 26
4.4. Step 4: Planning 27

4.5. Step 5: Assessing . . . 28
4.5.1. Quality assurance, development and manufacturing processes . . . 28
4.5.2. Functional, performance and dependability assessment . . . 31
4.5.3. Vulnerabilities and failure modes assessment . . . 33
4.5.4. Environmental and seismic qualification . . . 34
4.5.5. Independent complementary assessment . . . 35
4.6. Step 6: Identifying lifetime issues . . . 35
4.7. Step 7: Preparing the justification documentation package . . . 36

5. MAINTENANCE OF JUSTIFICATION . . . 38

5.1. Overview . . . 38
5.2. Change and defect reporting . . . 38
5.2.1. Item certification maintenance . . . 38
5.2.2. Regulatory defect reporting responsibility . . . 39
5.3. Periodic quality assurance measures . . . 40
5.4. Security management . . . 40
5.5. Configuration management . . . 40
5.5.1. Changes to hardware . . . 40
5.5.2. Changes to software . . . 41
5.6. Commercial off the shelf device justification maintenance . . . 42

6. REGULATORY ASPECTS . . . 43

7. SUMMARY . . . 44

APPENDIX I: SPECIFIC ASPECTS OF CERTIFICATION . . . 47

APPENDIX II: FAILURE ANALYSIS TOOLS AND TECHNIQUES . . . 51

REFERENCES . . . 55

ANNEX I: PRACTICE IN CANADA . . . 59

ANNEX II: PRACTICE IN GERMANY AND SWITZERLAND . . . 62

ANNEX III: PRACTICE IN THE UNITED STATES OF AMERICA . . . 67

ANNEX IV: PRACTICE IN THE UNITED KINGDOM . . . 72

GLOSSARY . . . 77
ABBREVIATIONS . . . 79
CONTRIBUTORS TO DRAFTING AND REVIEW . . . 81
STRUCTURE OF THE IAEA NUCLEAR ENERGY SERIES . . . 82

1. INTRODUCTION

1.1. BACKGROUND

Historically, instrumentation and control (I&C) systems in nuclear power plants (NPPs) were custom developed to implement functions important to nuclear safety,[1] specifically to meet nuclear quality assurance requirements by using conventional analogue technology. The gradual decrease of market availability of nuclear qualified products and the worldwide transition to digital technology, resulting in obsolescence issues, have made NPP designers increasingly dependent on integrating commercial I&C products within new development or modernization projects. Commercial off the shelf (COTS) devices that are produced in large quantities with a varied widespread use and significant operating experience provide a large user based test bed where problems are identified and fixed. NPP designers and operators are increasingly expressing the desire to use these digital COTS devices in systems, components and subcomponents of safety or safety related applications as economic alternatives to custom developed systems and equipment. These digital solutions can be used for applications involving systems important to safety in NPPs provided they can be shown to be of adequate quality to meet functional, safety, environmental and other requirements. Although this may be a challenging task, the incentives for the adoption of digital technology in systems important to safety at NPPs are strong. COTS devices may offer benefits such as an extensive history of operation, a large installed user base, improved reliability with a proven operating history, proven technology, self-monitoring and a larger group of technical personnel experienced with them. A COTS device also provides solutions to address obsolescence and lack of spare parts.

The use of COTS devices in systems important to safety raises concerns because their quality and integrity are not commonly developed in accordance with nuclear standards. Prior to use in an NPP, there is a need to demonstrate that digital COTS devices adhere to the functional, safety and environmental requirements (including heat, humidity, vibration, electromagnetic interference/radiofrequency interference (EMI/RFI), and seismic requirements as appropriate) with a level of quality and reliability comparable to that of a nuclear product. Special consideration needs to be given to the use of products based on digital technology in NPPs since they may be subject to unique vulnerabilities and failure modes (e.g. latent systematic faults[2]) related to nuclear safety applications. It should be recognized now 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 often include embedded digital devices even though this may not be evident. Digital devices, including embedded digital devices, may be affected by external environmental conditions present in NPPs and need to be thoroughly evaluated and tested to ensure that the components will behave in a known and predictable manner, especially under failure conditions.

When COTS devices are used in NPPs, it is important that a suitable process is in place to gather sufficient evidence and confidence to demonstrate that these products will meet specific quality, functional and non-functional requirements expected in the intended application. This process, referred to in the following as the *justification*[3] process, has to consider the behaviour of the device during normal operation as well as abnormal, transient and accident conditions. A systematic approach is needed so that, when applied appropriately and with sound judgement, it will facilitate the demonstration of evidence necessary to support the justification of these devices for nuclear safety applications.

[1] There are also applications for which the main concern is security (including computer security) because a security failure will affect nuclear safety. This is particularly important when considering digital devices. In those cases, it is assumed that the ultimate impact of a security breach could be linked to a nuclear safety issue. For this reason, the publication refers to nuclear safety rather than separately referring to safety and security.

[2] As defined in Ref. [1], systematic failure means those deriving from design errors (e.g. software faults).

[3] Common terminology also used in some countries in lieu of ‘justification’ includes ‘qualification’, ‘substantiation’ or ‘dedication’.

1.2. OBJECTIVE

The primary intent of this publication is to provide a starting point for Member States to develop or improve their processes for digital COTS justification. While high level expectations are identified in IAEA Safety Standards Series No. SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants [2], the practical methods to justify digital COTS devices in nuclear safety applications often vary among Member States. In this context, this publication helps identify good practices, based on the combined experience of Member States involved in related discussions.

The key objectives of the publication are:

- To identify the key challenges associated with the use of digital COTS devices in nuclear safety applications;
- To provide guidance on the requirements for what would constitute an adequate justification process.

In this publication, 'justification' is defined as an acceptance process undertaken to establish confidence that a digital COTS device is suitable for installation in an NPP, in a given safety application. The assurance of quality and reliability of these digital COTS devices may come, in part, from their operational experience and maturity achieved through ongoing development and improvements needed to support their commercial use. However, to minimize the risk of systematic failures and their potential nuclear safety impact, additional information and analyses are needed as part of the justification evidence. The attributes[4] to be considered in this respect vary depending on the regulatory context and the practices for digital devices in different countries.[5] A typical justification generally also includes an assessment of the robustness of the design process and the verification of the device's behaviours[6] in various operating conditions. Other elements that are not specific to digital COTS devices but that are essential in a justification include hardware reliability analyses and environmental qualification.

The justification of the digital COTS device generally needs to consider the specific requirements associated with its target application in the NPP. For example, depending on the application in the NPP, certain failure modes of the digital COTS device may result in a dangerous fault. Specific performance requirements such as accuracy or response time may also be specific to the target application in the NPP and would need to be assessed as part of the justification process. The justification rigour applied to a digital COTS device may also be commensurate with the specific safety significance of the application. The breadth and the depth of certain activities in the justification may vary depending on the safety classification of the device in the intended application (see IAEA Safety Standards Series No. SSG-30, Safety Classification of Structures, Systems and Components in Nuclear Power Plants [11])[7].

The justification activities of COTS devices described in this publication may require significant resources and, in some cases, require as much time and effort as developing these devices to nuclear standards. Because of this, the decision to use a justification process needs to be a carefully considered one, based on factors such as the application's safety classification, the willingness of an industrial supplier to participate in the justification process

[4] In some countries (e.g. the United States of America, USA), the key attributes are identified as 'critical characteristics' as part of the commercial dedication process (see US NRC Regulatory Guide 1.164, Dedication of Commercial-Grade Items for use in Nuclear Power Plants [3]).

[5] Typical expectations for digital devices for nuclear applications are defined, for example, in IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Std. 603 [4]; IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations, IEEE Std. 7-4.3.2 [5]; Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — General Requirements for Systems, IEC 61513 [6]; Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Software Aspects for Computer-Based Systems Performing Category A Functions, IEC 60880 [7]; Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Software Aspects for Computer-Based Systems Performing Category B or C Functions, IEC 62138 [8]; and Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Selection and Use of Industrial Digital Devices of Limited Functionality, IEC 62671 [9]. Other relevant requirements for safety applications are identified in Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, IEC 61508 [10].

[6] In addition to expected behaviours, consideration has to be given in the justification to potential for hidden, unwanted functionalities and spurious actuations.

[7] An example of the mapping between safety classification/categorization in different countries is provided in Ref. [12]. Additional information on criteria methods for classification and categorization is available in Nuclear Power Plants — Instrumentation, Control and Electrical Power Systems Important to Safety — Categorization of Functions and Classification of Systems, IEC 61226 [13] and IEC 61513 [6].

and the availability of alternative suppliers. The cost to procure and justify a COTS device needs to be considered since it is sometimes more appropriate to procure a higher quality COTS device with a lower effort to justify it. In addition, it may be more efficient to choose a COTS device supplier that is more willing and able to collaborate in the justification process.

The intended audiences for this report are the primary stakeholders for a justification of a COTS device, which include:

- The end user (e.g. NPP licensee or system designer for an NPP), who has to ensure that the device is suitable for installation in their NPP application;
- The assessor,[8] who is carrying out the justification activity (the assessor can be the end user or a third party);
- The manufacturer (supplier or vendor), who supplies much of the needed information for the justification, including documentation/code, and assurance about availability of a version that is justified.

Although the primary stakeholders are defined above, others (e.g. third party nuclear suppliers) may play a role in the justification process.[9] It is important to highlight that the ultimate responsibility to determine whether the device is suitable for a specific nuclear application lies with the end user, who ultimately owns the nuclear liability. The regulator is typically not part of the justification process to maintain independence from the assessor. However, depending on the Member State, the regulator may be involved in the evaluation of the justification evidence or be responsible for the approval of the final results of the justification process.

1.3. SCOPE

The focus of this publication is on the activities required to demonstrate justification of COTS I&C digital equipment,[10] for use in safety applications[11] in NPPs, with a well defined and limited functionality (IAEA SSG-39 [2]), which the end user can configure,[12] but not reprogram[13]. These devices typically contain digital components with executable code or software developed programmable logic contained in firmware.[14]

Examples of digital COTS devices considered in the scope of this publication may include but are not limited to:

- Time delay relay, relay, timer;
- Process switch, controller or transducer (temperature, pressure, etc.);
- Sensor with embedded digital devices;
- Circuit breaker;
- Isolator;
- Variable frequency drive, motor starter, motor and damper motor;
- Controller or valve positioner;

[8] In some countries (e.g. the USA), ‘assessor’ is also referred to as ‘dedicator’.

[9] For example, in cases where only a specific subcomponent is to be justified, in some Member States the component manufacturer might assume both the role of assessor for the subcomponent and of manufacturer for the primary component. Similarly, a systems integrator might also play the role of assessor, or simply of manufacturer of the complete systems, with a third party completing the justification.

[10] All remaining sections of the report will use the terminology COTS device or COTS equipment. The term will primarily refer to a COTS I&C digital device; however, it may also be a COTS I&C device, COTS digital device, or COTS device.

[11] Depending on the classification scheme used in each Member State, the definition of safety application may vary. It is here intended to cover any application which has an impact on nuclear safety as per IAEA SSG-30 [11].

[12] Examples of configurability are set point changes or operating mode selection.

[13] An example of programmability is the possibility to embed new functions (not in the original design), even if using pre-existing function blocks.

[14] Firmware in this context includes, but may not be limited to, devices such as programmable logic devices, field programmable gate arrays, application specific integrated circuits, erasable programmable read only memory, electrically erasable programmable read only memory, and complex programmable logic devices (CPLDs) (see IEC 62671 [9] or Embedded Digital Devices in Safety-Related Systems, US NRC RIS 2016-05 [14]).

- Meter or indicator;
- Inverter/uninterruptable power supply, power supply;
- Component with battery backup;
- Signal conditioner and electrical filter;
- Component with the following attributes/features: selector switch, potentiometer, liquid crystal/digital display, external connection port.

While reprogrammable components, large platforms or systems are beyond the scope of this publication, the justification strategy and activities outlined herein could be used, with suitable modifications and additions, to develop a justification process that addresses the unique features of those more complex systems.[15]

It is worth mentioning that I&C architectural solutions are sometimes designed that reduce the reliability requirements and other requirements on individual components and this may reduce the burden of the justifications, such as diversity considerations.[16] The discussions of such solutions are typically plant specific and strongly depend on the application of the device, hence they are out of scope for the purpose of this publication.

1.4. STRUCTURE

Section 2 of this publication provides a detailed discussion of the typical challenges associated with the use of COTS devices in NPPs, including issues associated with unique vulnerabilities and features of digital products such as those associated with security, obsolescence, access to commercial product information and common cause failure (CCF).

Section 3 outlines the strategy for digital COTS device justification. This section also describes the typical elements expected in the justification process and the type of evidence that supports a justification document. Section 3 also provides indications regarding how the justification can be graded to the safety significance/classification of the device.[17]

Section 4 outlines the process and specific steps in the justification process, including identifying the requirements, selecting the supplier and candidate equipment, planning, assessing and identifying equipment life issues, evaluating suitability and documenting the process. This section also provides the structure of a successful justification that will provide the information needed to support use of COTS devices in NPPs.

Section 5 provides guidance on maintaining a COTS device's justification. This topic is included to provide information on how both the justification and the documentation of the justification need to be maintained.

Section 6 discusses the regulatory aspects associated with the use of digital COTS devices. Although this publication is not primarily intended for regulators, the typical expectations of regulatory authorities are provided. Additionally, this section also discusses the typical challenges associated with regulatory reviews of COTS device justification.

Section 7 provides the summary of the publication. The publication also contains two appendices that provide additional information on specific aspects of certification (Appendix I) and on failure analysis tools and techniques (Appendix II) that are involved in the justification process.

Four annexes are attached to this publication, describing digital COTS justification practices in various Member States.

[15] One of the elements that differentiate the digital COTS in this publication with more complex systems is the communication between different devices.

[16] One architecture solution that could reduce the justification burden could be using digital COTS devices for normal operation and non-digital equipment for safety functions.

[17] There are a number of different safety classification systems used in the various Member States. Grading refers to the concept that for higher safety classes, more confidence is needed to justify that device.

2. CHALLENGES ASSOCIATED WITH COMMERCIAL INDUSTRIAL DIGITAL INSTRUMENTATION AND CONTROL EQUIPMENT

Along with the positive benefits of using COTS devices come challenges in the justification process and the maintenance of the justification. This section aims to raise awareness about typical challenges in the justification and application of COTS devices and to point to potential solutions. COTS devices are commonly subject to frequent version changes and contain functionality that is not required for the intended application. For COTS devices being applied in safety applications, there are technical issues due to the added complexity of digital components and software/firmware that present challenges and require specific review and evaluation. The following section addresses some of these issues. This is not a complete listing, however; it is a minimum list of issues requiring further evaluation.

2.1. CHALLENGES IN THE USE OF COMMERCIAL OFF THE SHELF DEVICES

2.1.1. Complexity of the component, multifunction, primary and support functions

When software is introduced into a component, it adds a new software to hardware interface with new and potentially undefined states of operation and failure modes. This section provides an overview of the difficult task of defining this additional level of complexity. The following definition of complexity is from a global industry standard (see IEC 61513 [6]) and is provided for context on the difficulty in defining and bounding the term ‘complexity’: the degree to which a system or component has a design, implementation or behaviour that is difficult to understand and verify.

Digital components vary in complexity owing to their ability to add increased functionality and diagnostics. The complexity level applicable to the specific safety function needs to be evaluated prior to beginning the justification process to ensure that 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. Note that this publication aligns closely with the scope of IEC 62671 [9] with respect to complexity (see section 5.2.2 of IEC 62671 [9]). The user of this publication needs to be aware that some COTS devices are more complex than others, with multiple functions that require additional considerations and analysis. Although the overall justification process outlined may be used, care needs to be taken when trying to justify the use of these more complex COTS devices, as their unique failure modes may require additional analysis, testing and verification, which are beyond the scope of this publication. The boundary for complexity is difficult to define (e.g. number of devices, interfaces, interrupts) but needs to have an initial assessment to identify, first, if the device is analysable and, if so, the high risk areas in its design and the use of defensive design measures. The device’s complexity needs to be considered in several different high risk areas such as:

- The operating system;
- Multiple microprocessor cores and software threads uses;
- Interrupt uses;
- Internal and external communications;
- Self-diagnostic that initiates actions;
- Devices used that have non-deterministic behaviour.

See Sections 3.2.3, 4.2 and 4.5.2 for more information and potential solutions.

2.1.2. Common cause failure considerations

The application of digital devices to perform redundant safety functions challenges the independence of the built in redundancy. Having the same software in redundant components/systems subjects the safety function to a potentially fatal software flaw, triggered by a common cause. This CCF is defined in the IAEA Safety Glossary [15] as "*Failures* of two or more *structures, systems or components* due to a single specific *event* or 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. This can result from a complete system upgrade or replacement of a single component of a safety system. For COTS devices intended for systems important to safety, the potential for CCF needs to be assessed; the justification will provide evidence to support the user's assessment that failure due to CCF is sufficiently low (see section 7.6.2.7 in Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems — Part 1: General Requirements, IEC 61508-1 [16]).

See Sections 3.1.3.1 and 4.5.3 and Appendix II for more information and potential solutions.

2.2. SPECIFIC HARDWARE AND SOFTWARE VULNERABILITIES OF DIGITAL COMMERCIAL OFF THE SHELF DEVICES

2.2.1. Potential new failure modes and hazards

Owing to the added complexity of digital devices and the possibility of new failure mechanisms (e.g. infinite loop states) and modes (e.g. silent lockups), a failure and/or hazards analysis of the COTS device needs to be performed. These types of analysis can be very challenging owing to the complexity and the skill set required to perform them. For COTS devices, the level of detail needed to perform failure and/or hazard analysis is generally not known by the end user or assessor, and is not commonly disclosed by the manufacturer. The failure and/or hazards analysis needs to be based on the defined safety function, include the device and all interfaces (e.g. electrical, communications, human) and may identify new critical characteristics that need to be justified. A hazard analysis can have many different forms (e.g. failure modes and effect analysis (FMEA), failure modes, effects and diagnostics analysis (FMEDA), fault tree analysis (FTA), hazards and operability analysis (HAZOP)). The Electric Power Research Institute document EPRI 3002000509 , Hazard Analysis Methods for Digital Instrumentation and Control Systems [17], provides guidance for different types of hazards analysis (see Appendix II of this publication).

2.2.2. Identification of embedded digital devices with undeclared content

COTS devices that are used in mechanical or electrical systems may not be considered as an I&C device. These COTS devices may consist of digital components with embedded software (i.e. firmware, field programmable gate array (FPGA)) and this fact may be unknown to the user or assessor. Even for I&C devices, it may be difficult for the user or assessor to identify an embedded digital component. As digital content has become increasingly available and more cost effective to incorporate into devices, many COTS device analogue subcomponents are being replaced with a digital device that is 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 any digital subcomponent is not identified, its digital/software quality would not be assessed, and the component (i.e. COTS device) may have new failure mechanisms and modes that were not considered. This may also be referred to as COTS with undeclared content. This challenge is beyond the scope of the digital COTS justification process but two sources of information associated with this challenge are: US NRC RIS 2016-05, Embedded Digital Devices in Safety-Related Systems [14] and EPRI 3002008010, Guideline on Prevention and Detection of Undeclared Digital Content [18].

See Sections 2.3.5, 4.2 and 5.2 for more information and potential solutions.

2.2.3. Counterfeit, fraudulent and suspect items

All COTS devices are vulnerable to counterfeit activities, especially as procurement has become more global. Counterfeit devices are those that are fraudulently represented as genuine items from the manufacturer; the definition is limited not only to the final product assembly but also to the subcomponents and raw materials. Integrated circuits have been identified by the military industry as having a high risk of fraudulent events; this also increases the risk of malware being inserted into the device. The end user or assessor may have regulatory requirements to address and identify potentially counterfeit components.

See Sections 3.1.3.2 and 4.1 for more information and possible solutions.

2.2.4. Computer security considerations

Since COTS devices may not be designed with established computer security requirements, measures need to be implemented in order to protect the digital device from malicious acts. These protective measures begin with procurement requirements and are completed with management of any vulnerabilities identified by the user. Computer security vulnerabilities can occur or be introduced at manufacture, in shipment, and at the user’s facility, so multiple reviews and assessments for vulnerabilities and mitigation activities will be required, such as the following:

- Manufacturer’s software verification and validation (V&V) and configuration controls and a secure development and operational environment (SDOE);
- Manufacturer’s supply chain from trustworthy suppliers;
- Computer security hardening of the COTS device (i.e. password protection, logging capabilities, disabling unused communication ports, locking enclosures);
- Packaging and shipping requirements in the procurement specification and implementation;
- User’s internal protection and control measures in which the mitigation needs will be assessed based on the application of the COTS device.

See Section 3.2.5 for more information and potential solutions.

2.3. ORGANIZATIONAL CHALLENGES

2.3.1. Procurement and definition of safety requirements with contractual ties

As we move from analogue to digital justification, a new quality aspect is added to the justification process involving the design architecture and software development process, dependability critical characteristic (see Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, EPRI TR-106439 [19]); this needs to be part of the digital specification of the COTS device. This is sometimes overlooked in the process and the assessor may treat the justification using only methods for an analogue justification. The user needs to align the COTS safety function and the digital specific requirements to the assessor’s COTS justification. This needs to be in a contractual form to ensure linkage and proper implementation of requirements by the assessor. These requirements establish a communication vehicle between the purchaser and the assessor to ensure that all requirements are identified.

See Sections 3.2.2.2 and 4.3 for more information and potential solutions.

2.3.2. Device selection

In selecting a suitable COTS device, the assessor needs to engage the manufacturer as early as possible to consider the following areas, associated with the manufacturer, to determine if the COTS device is a suitable candidate for justification:

- Whether the supplier would be able to provide long term support;

- Whether the reputation of the supplier's products, including the COTS device that is being selected, is positive among users;
- Whether the manufacturer will supply and support the type of COTS devices being selected for long enough and at the necessary production volume;
- Whether the manufacturer has an appropriate process for design change management;
- Whether the manufacturer is ready to support the collaboration that is necessary for the assessor in obtaining evidence supporting justification of the COTS device.

See Section 4.2 for more information and potential solutions.

2.3.3. Generic and limited justification/qualification

A COTS device may not be tied to a specific plant safety function during the justification process. Bounding technical requirements may be used to cover a large percentage of applications. The user is then responsible for ensuring these bounding requirements align with the specific plant safety function under the user's design processes.

2.3.3.1. Generic justification

A supplier of a COTS device may perform a generic justification of the device, not to a user specified safety function but to a set of specific functions and qualifications or to the justification envelope. The assessor or the user can perform additional work for the specific justification under their approved quality assurance programme. The generic qualification needs to highlight both those areas covered by the qualification and those areas not covered.

See Sections 3.2.4 and 4.5.4 for more information and potential solutions.

2.3.3.2. Limited justification

Some suppliers of COTS devices may limit their justification to specific functions of the component. Common examples of limited functionality include:

- Qualified digital communication ports for external communications (e.g. electrical and data isolation, potential CCF trigger). If the communication port is not justified, the port cannot be used.
- Only specific input types are qualified (voltage and current, but not resistance temperature detector or thermocouple).
- Power supply input (alternating current, but not direct current).
- Variable configurability using predefined simple math function blocks (i.e. +, −, ×, ÷). Note that use of these function blocks would require additional V&V by the end user.
- Limited or bounding qualification:
  - Seismic qualification profile — ensure tested spectrum is bounding for the application specific location (i.e. use of conservative multiplication factors) and mounting (i.e. rigid).
  - Environmental qualification — ensure that the type testing is bounding. If the digital device is in an enclosure, factor in internal cabinet/panel temperature rise.
  - EMI/RFI qualification — ensure that the type testing is bounding and determine which configuration it was tested in (e.g. in an enclosure, with a door open, cabling in a conduit).

All limits associated with the justification need to be clearly established in the documentation/certification so that the device is not used in an inappropriate function.

See Sections 3.2.4 and 4.5.4 for more information and potential solutions.

2.3.4. Evidence required to address the commercial off the shelf device's justification

Assessment of the COTS design, development and manufacturing information is essential to justification tasks. Being a commercial product, its development activities can vary widely from manufacturer to manufacturer. Also, for COTS manufacturers, design information will most likely be considered intellectual property and protected by the manufacturer. Several areas could present challenges working with a commercial manufacturer in the performance of the justification activities, such as the following:

- The development of the essential or critical characteristics (essential and critical characteristics are used interchangeably within this publication) for the defined safety function into verifiable tasks may be difficult due to the complexity, multiple states, ability to verify design features, safe state definition, testing and review requirements, acceptance criteria, etc.
- The manufacturer may have limited evidence to support justification.
- Access to the manufacturer's intellectual property may be limited or denied.
- Evidence may be lacking to address systematic fault or CCF and identify their triggering mechanisms.
- Functions that are not required may have an adverse impact on the safety function and need mitigation.
- Adequate configuration controls are needed to identify design changes that require evaluation and the quality of software/configuration tools being used during development.
- Self-diagnostics that could adversely affect the safety function, for example a built in diagnostic for equipment protection that actively shuts down the device when the safety function is to run.
- Applicability of operating history with operating failure history details and metrics.
- Definition of operational states (i.e. running, standby, loss of power with reboot).
- Unknown gaps that the justification identifies and how to mitigate or compensate for them.
- How to deal with the manufacture's product life cycle and identification of future design changes and impact on the justification evidence.
- No previous qualification testing (e.g. seismic and EMI/RFI testing).
- Lack of sufficient component ageing information for definition of service life for the COTS device.
- Lack of evidence to address specific regulatory requirements.

See Sections 3.2.1, 4.2 and 4.5.1.9 for more information and potential solutions.

2.3.5. Change management

Since justification is normally an activity that requires significant resources, including money, an evaluation needs to be performed to address how to efficiently and effectively manage change. This is a life cycle issue and the assessor and/or end user needs to develop a periodic programme for continued assessment of the COTS device throughout the life cycle.

2.3.5.1. Obsolescence management

An evaluation needs to be performed of the current and future expected obsolescence of the digital device and key subcomponents (i.e. microprocessor, analogue to digital converter).

2.3.5.2. Hardware and software updates

Both hardware and software changes are frequent for COTS devices owing to the market driven environment for improvement, more functionality and changes in mechanical components such as sensors that can drive software changes. Since the justification is specific to particular hardware and software versions working together as an integrated digital device, methods need to be established to minimize future re-justifications and qualifications.

Usually, design changes initiated by the manufacturer can be related to:

- The needs of a wide variety of end users and the desire of the supplier to cover the market formed by these users.
- Improvements and changes in development technology for the manufacturer's efficiency.
- The need to eliminate shortfalls, deficiencies or weaknesses in the COTS device design discovered through operational experience.
- Obsolescence of subcomponent parts.
- The need to address potential computer security vulnerabilities.

- Configuration control challenges due to:
  - Frequency of changes — Hardware and software changes are inherent to the life cycle of COTS devices and need to be managed to remain aligned with the justification.
  - Undeclared changes — Design and version changes may be specified well by the manufacturer but sometimes they are not declared to the end user. It is common for the COTS vendor to make changes without a part number change.
  - Various versions available — There can be COTS devices available on the market that have numerous versions, releases and version changes.

Note that these changes may affect functionality and could also have adverse effects on existing qualification testing such as EMI/RFI susceptibility.

See Sections 4.5.1.6, 4.5.5, 5.2 and 5.5 for more information and potential solutions.

2.3.6. Lack of qualified and experienced personnel

Users and stakeholders plan and conduct justifications by using a combination of methodologies. Experienced/trained/familiarized technical personnel need to be involved with the support of an adequate quality system. Examples of problem areas that have been seen in past justifications are:

- Treating the commercial grade item as hardware/black box — Some items that have software or complex digital devices have been treated as a black box, without software functionality and dependability being identified.
- Misappropriately defining the critical characteristics — There can be several types of critical characteristics regarding physical, functional, performance, dependability, interfaces and other installation, operation and maintenance critical characteristics. Achieving completeness and establishing viable acceptance criteria can be a challenge.
- Inability to deal with supply chain management and tracking — Managing the complicated supply chain is one of the difficulties in accomplishing justification.
- Lack of impartiality for justification — An end user or assessor who has a financial interest in the success of justification or who is not adequately trained in the justification process could overlook weak areas or inappropriately compensate for gaps in the justification. As a result, some level of independence is needed organizationally, managerially and financially.

See Sections 3.2.2 and 4.5.5 for more information and potential solutions.

3. STRATEGY FOR THE JUSTIFICATION OF COMMERCIAL INDUSTRIAL INSTRUMENTATION AND CONTROL EQUIPMENT

This section outlines the strategy for the justification of a digital COTS device, identifying the key elements expected in the substantiation. The principles defined in this section are then developed in Section 4, which details the typical steps expected in a justification process. While the strategy in Section 3 outlines 'what' is trying to be achieved through the justification of a COTS device, Section 4 describes 'how' this can practically be achieved.

The key elements of the justification are outlined in Section 3.1. Then Section 3.1.1 identifies the justification envelope, capturing the key requirements, restriction of use, and assumptions. Section 3.1.2 identifies the key elements expected in the assessment of the COTS device, and Section 3.1.3 outlines the considerations to be made when integrating the COTS device justification for a specific application into the overall I&C architecture and in the plant more generally. Section 3.2 identifies some additional considerations to be accounted for when defining the justification approach.

3.1. KEY ELEMENTS TO CONSIDER IN THE DEFINITION OF THE JUSTIFICATION STRATEGY

The flow chart in Fig. 1 presents the typical phases expected in the justification of COTS devices in a nuclear application. Figure 1 also clarifies the area covered in the justification process outlined in Section 4. The integration of the COTS device justification into the overall safety justification is not addressed in detail in the justification process section of this report because expectations for the overall safety justifications in various countries are different. Section 3.1.3 outlines the common elements to consider in this final phase.

The acceptability of a digital COTS device for a given nuclear application needs to address both nuclear safety and security. While safety and security could in principle be justified separately (either in parallel or sequentially), 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 specific aspects of the design or of the development process are required for both. Where appropriate, the joint consideration of safety and security in the assessment allows for the consideration of trade-offs and synergies in the implementation of recommendations arising from the assessments. The justification strategy refers generically to both safety and security (see also Section 3.2.5 for additional considerations on security).

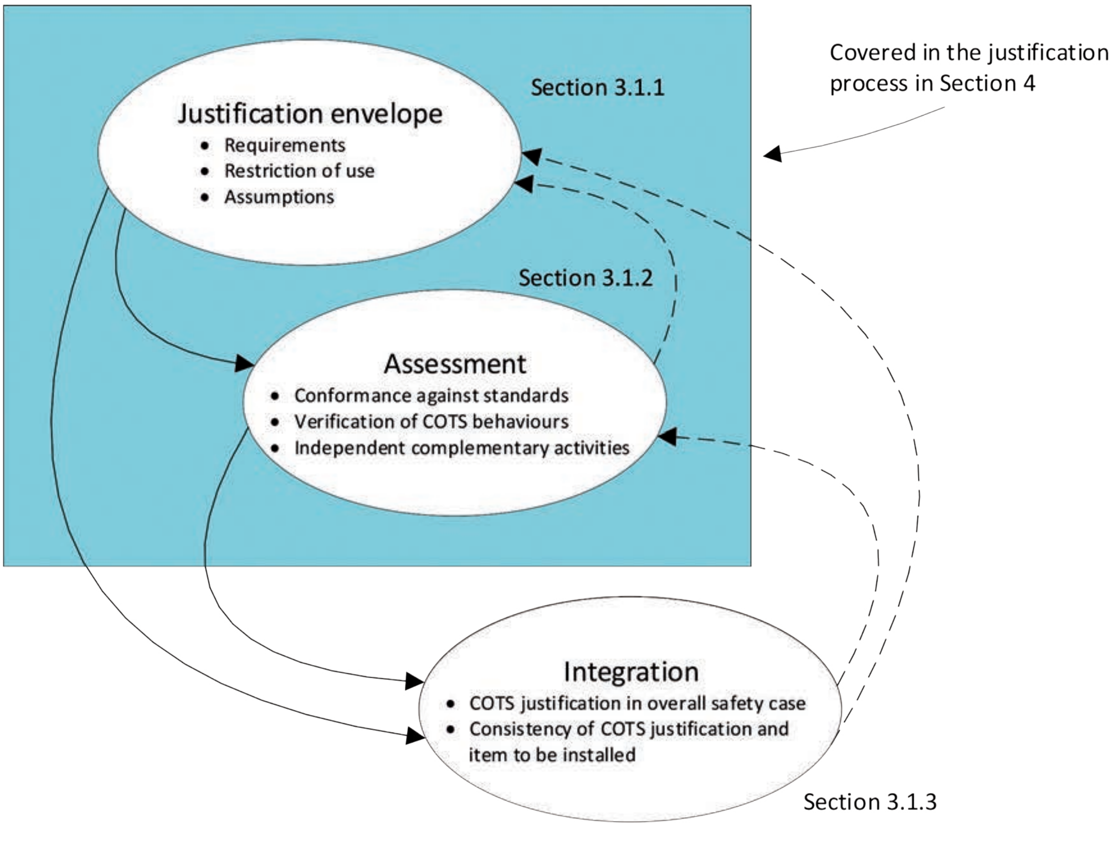

Covered in the justification process in Section 4
Section 3.1.1
Justification envelope
• Requirements
• Restriction of use
• Assumptions
Section 3.1.2
Assessment
• Conformance against standards
• Verification of COTS behaviours
• Independent complementary activities
Integration
• COTS justification in overall safety case
• Consistency of COTS justification and item to be installed
Section 3.1.3

FIG. 1. Typical flow chart for a commercial off the shelf justification. Solid lines identify functional links between the different activities (e.g. the results from the assessment and the justification envelope phases are clearly input into the integration phase). The dashed lines identify potential iterations needed as part of the process (e.g. the justification envelope may need to be changed during the assessment phase).

3.1.1. Definition of the justification envelope

The justification of a COTS device has meaning only when its domain of validity (or justification envelope) is specified (see IEC 62671 [9]). A clear definition of the envelope is vital to ensure that the assessment is complete (Section 3.1.2) and that the COTS device is suitable for the specific application (Section 3.1.3). While there is an incentive for the justification envelope to be as large as possible (e.g. covering all of the functions delivered by the COTS device), it may be more efficient to restrict the scope to avoid the justification becoming too onerous (scope restriction may also apply during the assessment itself). For this reason, there may be iterations between the definition of the envelope in Section 3.1.1 and the assessment in Section 3.1.2.

The definition of the justification envelope may also depend on whether the justification is intended to be generic or application specific (see discussion in Section 3.2.4). For a generic justification, the assessor typically wants to keep the envelope of the justification as large as possible. If the justification is targeted for a specific application and there is no intention to use the same device for another application, the justification envelope may be reduced.

The following subsections characterize various elements that contribute to the definition of the justification envelope. They are covered in Section 4.1 in the definition of requirements and prerequisites.

3.1.1.1. Requirements

The justification of a digital COTS device needs to start from the identification of requirements (Section 4.1). These are likely to include:

- The safety function(s);
- The target safety classification;
- Any undesired behaviours (e.g. causing spurious actuation);
- The non-functional requirements;
- The computer security requirements (e.g. security level);
- The scope of the environmental and seismic qualification.

Depending on whether the justification is generic or application specific (see discussion in Section 3.2.4), the requirements may be directly derived from a target application or more generally defined based on the potential need. When defining the requirements, it is often useful to have an understanding of candidate devices on the market (Section 4.2), as this may avoid iterations when assessing options.

3.1.1.2. Restriction of use

Restrictions of use may arise because some properties or attributes of the COTS device are not of interest for the end user applications. Such restrictions can reduce the complexity of the justification. For example, a digital recorder is typically used in a safety application for recording and data storage, but it may also deliver other functions such as trip and control functions with communication ports for digital interfacing to other digital systems. To simplify the justification task, the end user may decide to restrict the use of communication functions.

Typical restrictions of use may include:

- Limitation of the set of functions or options covered by the justification;
- Constraints on non-functional properties (e.g. time response or accuracy);
- Justification of a subset of input types or power supply input;
- Limits on user configurability;
- Limits on design life;
- Limits on environmental qualifications;
- Divisions for installation in the NPP.[18]

[18] Depending on the diversity requirements at plant level and the integrity of the digital COTS device, it may only be possible to implement the device in a subset of the redundancies (e.g. two divisions in a fourfold redundant architecture).

When restricting the functions covered by the justification, unless they can be physically disabled in the device, a non-interference argument would be needed as part of the justification, to demonstrate that these cannot affect safety functions in the envelope.

Because some of the restrictions of use are identified as part of the assessment, there may be iterations between Sections 3.1.1.2 and 3.1.2. It is key that, at the end of the justification, there is complete consistency between the justification and its domain of validity.

3.1.1.3. Assumptions

During the justification process, assumptions may be made by the assessors regarding some aspects that can affect the validity of the justification. These can be interpreted as prerequisites in Section 4.1. For example, the maintenance strategy (e.g. testing interval) will have an impact on the practical reliability achieved by the device, which determines whether a certain device is suitable for a given safety application. Similarly, the normal operation/accident environmental conditions can have an impact on the failure rate of the device and its accuracy. Other assumptions may relate to the device's use in redundant configurations or the physical security arrangements assumed to be in place to protect the device.

It is important that any assumptions are recorded so that they can be verified at a later time if the COTS device is proposed for different applications or if there is a change in the way the device is operated/maintained.

3.1.2. Assessment of a commercial off the shelf device

Assessment of a COTS device can generally be approached from different perspectives. The strategy triangle in Fig. 2 identifies three key aspects that are generally relevant in a safety justification (Ref. [20]).[19]

Although not explicitly required, a combination of all three perspectives provides a sound basis for an adequate justification, because:

— 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. Failure and hazard analyses are often used to identify vulnerabilities (see Appendix II).

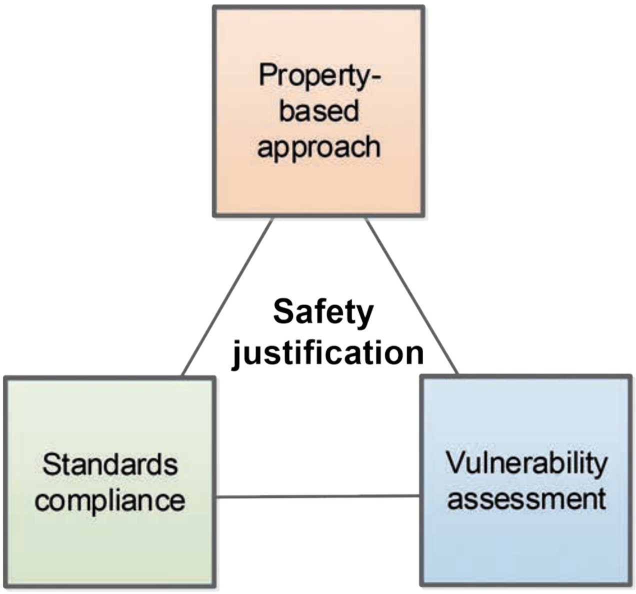


FIG. 2. The strategy triangle of justification.

[19] From the perspective of regulations in the USA, the property-based box would be 'critical characteristics' development and verification and 'standards compliance' would be used to support the dependability evaluation of critical characteristics.

- The *property based approach* verifies how the key claims on the behaviour of the COTS device are satisfied (e.g. safety attributes, reliability, accuracy, response time, functionality, testability, maintainability, human factors/usability).
- The *standards compliance* exercise shows whether the COTS device satisfies the requirements of the relevant standards. It is typically focused on the design, development and manufacturing processes.

In the following, the three approaches identified in Fig. 2 are used to define the elements in the assessment, which are then detailed further in Section 4.5.

3.1.2.1. Conformance against relevant standards

This part of the assessment is focused on the verification of how the requirements of the relevant standards are met by the COTS device (i.e. the standard compliance aspect of the strategy triangle in Fig. 2). Because of the complexity of digital devices, special attention is given to the processes utilized in their design and development. As part of the standard conformance exercise, an assessment of the manufacturing process and quality assurance is also expected "to provide a basis for accepting identical replications of the device" [21].

The definition of the relevant standards to be considered for a COTS justification may differ from Member State to Member State (e.g. IEC or Institute of Electrical and Electronics Engineers (IEEE)) and may depend on the scope of the justification (e.g. computer security may be relevant if that is part of the justification). In general, nuclear standards are expected to be considered as the primary benchmark, unless a country considers other general non-nuclear standards to be equally applicable (e.g. IEC 61508 [10], IEEE Standard for System, Software, and Hardware Verification and Validation, IEEE 1012-2016 [22]).

The purpose of this part of the assessment is:

- To understand the standards used for developing and manufacturing the device.
- To understand the development and quality assurance processes used for development and manufacturing.
- To compare the processes used for the COTS device against the requirements in nuclear standards: this is aimed at looking at the process(es) and outputs implemented by the manufacturer for the design, development and manufacture of the COTS device and identifying gaps in the requirements for a nuclear grade device.
- To compensate for the gaps identified above: This is aimed at determining whether the gaps can be satisfactorily compensated for and, if so, identifying targeted additional activities/measures to mitigate the gaps.

It is realistic to expect that a significant number of gaps in documented evidence will be identified because the COTS device was not initially developed for a nuclear application. Examples of how gaps may be compensated for are provided in IEC 62671 [9]). While some of these gaps can be readily compensated for, the justification of others can be onerous (e.g. because they lack a robust and well documented development process). In some instances, it may not be possible to retrospectively mitigate for some gaps and, in such cases, the outcome of the justification of the COTS device for a particular safety class may be negative.

In order to make the justification process more efficient and to avoid unnecessary work, it may be appropriate to identify specific milestones in the assessment that re-evaluate the chances of success (e.g. considering the answers to key areas of interest that could prevent the COTS device from being used in a safety application).

3.1.2.2. Assessment of commercial off the shelf device behaviour

Another key element of the assessment is the confirmation that the COTS device behaves as expected. This can be approached considering two complementary tactics:

(1) Verifying that the functional and non-functional requirements identified in the justification envelope are met (the property aspect in the strategy triangle in Fig. 2).

(2) Verifying how the potential vulnerabilities of the COTS device and underlying technologies are avoided or mitigated in the design to ensure they do not jeopardize expected behaviour and, where necessary, identifying measures to address them (the vulnerability aspect in the strategy triangle in Fig. 2).

As part of this assessment, several assumptions may be identified or restrictions of use specified. As discussed in Section 3.1.1, it is important that any assumptions/restriction of use are captured as part of the justification envelope.

When assessing the functional and non-functional properties, it is also important to identify any requirements for maintaining the performance of the device across its life cycle (Section 4.6). These need to be recorded as assumptions in the scope of the justification (Section 3.1.1).

3.1.2.3. Independent complementary assessment

A possible part of the assessment process is to perform activities that are independent of the manufacturer (see Ref. [23]). These activities can focus on any of the perspectives of the strategy triangle in Fig. 2, although usually they will address behavioural aspects (i.e. either confirm or otherwise show conformance with behavioural properties or show absence of vulnerabilities).

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 Member State to Member State. 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 Member States the actions may be commensurate with the safety class of the system (see Section 3.2.3) and could range from commissioning at lower safety classes to extensive additional static/dynamic analyses at higher safety classes.

In general, it is preferable that the activities are different from those performed by the manufacturer during the design and development of the device.

These activities may conclude that the device is not suitable for a certain safety application or safety class, that additional analyses are required or that the scope of the justification needs to be restricted.

3.1.3. Integration of the commercial off the shelf device in the overall instrumentation and control architecture

The justification of a COTS device is concluded when the COTS device is implemented in the I&C architecture (Section 3.1.3.2) and its safety justification is integrated into the overall safety justification of the plant (Section 3.1.3.1).

3.1.3.1. Integration of the commercial off the shelf device justification into the overall instrumentation and control justification

When integrating a COTS device into an I&C architecture of an NPP, the assessment (Section 3.1.2) and the scope of its validity (Section 3.1.1) need to be considered in the context of the overall I&C architecture (see Refs [9] and [23]). This activity typically includes:

- A review of the justification scope in the context of the specific application: This needs to verify whether the behaviour, restriction of use and any other assumptions considered in the generic justification are suitable for the specific application. This requires the verification of requirements (Section 4.1), discharge of prerequisites (Section 4.1) and verification of any lifetime issues (Section 4.6). This may require an impact assessment of the application specific constraints on the validity of the justification. Typical areas of interest cover the maintenance and testing regime (e.g. frequency and extent), environmental qualification requirements, user configuration and calibration requirements.
- 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 level of the defence in depth of the plant. The impact of systematic failures of these devices at the plant level needs to be considered (see Refs [9] and [24]). This could require some additional activities to confirm that the measures needed to protect against or mitigate CCF have been implemented in the I&C overall architecture and are acceptable. For example, two different devices may share parts of the software (e.g. operating system), making them vulnerable to the same initiating event.

- 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. Spurious events need to be considered as part of this exercise.

Based on the outcome of the activities above, the justification may need to be expanded or clarified (hence the iteration loop in Fig. 1). In other cases, the COTS device may be identified as not suitable for the application.

For this activity, an adequate understanding of the overall I&C safety justification is necessary.

3.1.3.2. Verification of consistency between the commercial off the shelf device justified and item to be installed

An evaluation is produced by looking at evidence from many separate devices that may have different versions (e.g. during testing) or from the process in general. Before the COTS device can be used, the COTS device justification needs to be applicable to the device being deployed. To achieve this, confidence is required in the production process as well as in the configuration management approach, the consistency of the justification and the delivery process.

Evidence to support achieving confidence includes:

- Manufacturer's quality assurance processes;
- Manufacturer's configuration management processes;
- Version and model identification;
- Security arrangement during manufacturing and delivery, including SDOE.

Quality assurance and control on the manufacturer's part are required to ensure a consistent product during the production process (see Ref. [23]). Configuration management applies to the device and the versions of its constituent parts. A robust configuration management approach will identify changes to low level components as changes to the device's hardware.

Assessments of the quality assurance and controls procedures (Section 4.5.1.2) and manufacturing procedures (Section 4.5.1.7) have to establish whether the version and model identification correspond to a unique set of components of specified versions. If that is not the case, for example when the part number does not change with internal part changes, it may be necessary to use the bill of materials (BOM) to ensure that the assessed device is the same as that to be deployed.

Security processes and practices at the manufacturer's site may reduce the possibility of the devices being maliciously modified before delivery (Section 4.5.1.5). Once the devices leave the manufacturer's site, it is important to ensure that they are not modified in transit between the manufacturer and end user. This may be achieved in different ways, for example by using tamper proof packaging.

One possible reason for the installed device to be different from that assessed is if a counterfeit, fraudulent or suspect item has been substituted for a genuine one. To prevent this from happening, special procurement activities need to be undertaken. Procurement documents ought to include language to ensure COTS devices provided fully conform to the description, technical and quality requirements, including prohibition of the introduction of suspect or counterfeit COTS devices. A way to minimize the potential for counterfeit is to define criteria for trusted suppliers, which can be monitored more closely (e.g. through periodic audits or through dedicated contractual arrangements). Following is an example evidence of potential counterfeit or fraudulent activity:

- Screwdriver marks, different screw types or materials on terminals;
- Missing terminals;
- Broken or damaged solder terminations or termination lugs;
- Pitted, scarred or worn contacts and lugs;
- Contact surfaces that do not mate properly;
- Buildup of debris and dirt in termination guards;
- Not in manufacturer's box or container (no manufacturer bar code);
- Signs of paint or smoke;
- Screws used in place of rivets;
- Body worn or discoloured;

- Plastic parts of different colours;
- Rough metal edges;
- Polished or painted surfaces scratched, marred or dented;
- Metal colour inconsistencies;
- Modified or re-stamped nameplates or insufficient nameplate information;
- Handwritten or typed rather than stamped tags;
- Missing tags (usually an Underwriters Laboratories or Conformité Européene marking tag);
- Improper fastening of nameplates;
- Discoloured or faded manufacturer's labels;
- Lubrication that appears to be old.

3.2. OTHER CONSIDERATIONS FOR DEFINING A JUSTIFICATION STRATEGY

3.2.1. Evidence

The evidence supporting a COTS device justification is effectively an integral part of the justification (see Refs [21] and [23]). Its availability allows external reviewers to evaluate the adequacy of the COTS device for use in a nuclear application. It also supports the overall I&C architecture decisions, for example component selection to cope with CCFs.

3.2.1.1. Evidence from the manufacturer

When engaging with the manufacturer (e.g. in audits), it is important to verify that the claims on the development process or on the product are supported by evidence. As discussed in Section 2.3.4, this may be challenging, but is key to enabling the justification. Examples of evidence sought from the manufacturer are requirement specifications, design documents, verification records, quality assurance procedures and competence records. For higher safety classes, access to the software source code may be necessary (e.g. see discussions in Ref. [23] regarding the expectations for various device reliabilities). Ideally, the entire package of manufacturer evidence needs to be an integral part of the justification (see Ref. [23]). This typically helps in cases where the justification needs to be updated (see Section 5) or in discussions with the regulator (see Section 6). Where it is not possible to integrate specific documentation into the evidence package (e.g. because of proprietary information), the assessor is expected to capture key aspects of the evidence and why it is satisfactory for the safety application/class defined in the justification envelope (Section 3.1.1). Where specific evidence cannot be included in the justification package, depending on the regulatory context, a non-disclosure agreement with the manufacturer may be needed (e.g. to allow the regulator or an external reviewer to gain access to relevant proprietary information).

3.2.1.2. Other pre-existing safety assessments

Some COTS devices may have already been assessed for safety applications in the nuclear industry (e.g. by other licensees) or non-nuclear industries (including certifications, see Section 3.2.1.3.).

These pre-existing assessments could represent a useful part of the justification if the whole body of documentation developed to support the decision is made available to the assessors. The relevance of pre-existing COTS device justification can be influenced by the standard against which the analysis is carried out (e.g. IEC 61508 [10] or nuclear standards such as IEC 62671 [9]) and by the contractual arrangements (e.g. scope of the assessment and independence from the manufacturer).

3.2.1.3. Certifications

Certain COTS devices may also have been certified or developed under a certified process. Although not essential for a successful justification, the certification of the product for a safety application can represent a valuable input in the selection of the candidate COTS device (Section 4.2). For example, for an IEC 61508 [10] safety integrity level (SIL) certified product, the manufacturer may already have available relevant evidence, which could simplify the justification process for nuclear applications. There are various types of certifications and the value of each of them needs to be assessed in the context of the justification process. Additional details regarding certification types[20] and applicable relevant quality standards are presented in Appendix I. For example, Conformity Assessment — Requirements for Bodies Certifying Products, Processes and Services, ISO/IEC 17065 [25] and Conformity Assessment — Fundamentals of Product Certification and Guidelines for Product Certification Schemes, ISO/IEC 17067 [26] identify, respectively, the requirement for certification bodies and for product certification. Depending on the regulatory context, the certification may not be accepted instead of the COTS device justification, although it may be used as part of the justification (see Ref. [21]).

3.2.1.4. Additional testing and analyses

Evidence will not necessarily have been generated by the manufacturer as part of the design and development process. In some instances, additional testing and analyses can be generated to compensate for certain gaps in the design process and documentation (e.g. omissions in the functional requirements and validation testing) and to identify responses to specific input conditions (such as abnormal inputs). Additional testing and analyses can also be used as independent complementary activities, where appropriate. Specific environmental qualifications may also be needed for the specific nuclear applications (e.g. temperature or humidity beyond the original manufacturer qualification).

When additional activities are required, their specification and the relevant results have to be recorded as evidence. An explanation of how the testing and analyses are addressing the gaps is expected as part of the justification.

3.2.1.5. Operational experience

Operating experience can be used as part of the justification of a device, although it needs to be specific to the product/version and provide evidence that the device has been exercised in the same way as for the proposed application (IEC 62671 [9], IEC 61508 [10], Ref. [23], Handbook for Evaluating Critical Digital Equipment and Systems, EPRI 1011710 [27] and Evaluating Commercial Digital Equipment for High-Integrity Applications, EPRI TR-107339 [28]). Applicable operational experience may be based on real use in many environments and applications over significant periods of time. The significance of the operational experience in the context of the COTS device justification typically depends on a number of factors such as the following (see Ref. [23]):

— Robustness of the software configuration management;
— Effectiveness of problem reporting;
— Relevance of the product operating profile and environment;
— Impact of maintenance and changes.

Operational experience uncovers user interface issues that were never anticipated by the manufacturer, such as issues not identified by the manufacturer or certifier (i.e. software bugs) or weakness in component reliability due to environment conditions. Operational experience may not be an adequate argument by itself, so it must be supported by other evidence of dependability (i.e. software and hardware assessments). Examples of attributes characterizing the quality of the operational history include revision traceability, impact assessment of configuration variations, the problem reporting process (e.g. failure reporting and warranty period), use of metrics, coverage (only hardware or both hardware/software), corrective actions to resolve reported issues (fixes, work arounds, bug tracking, etc.), and the number of demands on the system (as opposed to total operating hours).

Since COTS devices are updated frequently, applicable operating experience must be defined, and the assessor needs to document evidence of the applicability baseline (i.e. revision/version levels). Due to the frequency of change, it can be useful to look at past revision changes and the multiple revision operating history for possible expansion of the applicability baseline based on the common digital design features and the manufacturer’s

[20] As detailed in Appendix II, there are different types of certifications, including corporate quality certifications, product safety certifications, equipment certifications (e.g. environmental) and software development process certifications to standards (e.g. IEEE and IEC).

processes for possible use for future change impact evaluations. This evidence may also demonstrate the quality of the manufacturer's change process.

3.2.2. Selection of personnel involved in the justification

3.2.2.1. Competence

As discussed earlier, evaluating the suitability of a device for a nuclear application generally requires a significant element of technical expertise. The competence of the assessor[21] is hence a key ingredient for a quality justification, as the assessor needs:

- To understand the development and quality assurance processes followed;
- To understand the information provided on the design and behaviour of the device;
- To understand the relevance of the gaps;
- To evaluate confidence in the device's behaviour.

In a generic assessment of a COTS device (i.e. not application specific, see Section 3.2.4), the assessor may not be aware of the nuclear safety implications of the failure of the device. In that case, this assessment will need to be carried out by the end user.

Typical elements needed to produce an assessment of the required quality are understanding of the following:

- Hardware/software architecture of the device;
- Safety critical I&C equipment features;
- Design and verification features of safety critical hardware/software (including FPGA and application specific integrated circuit (ASIC) element, if appropriate);
- Failure modes and vulnerabilities;
- Requirements of the device in the overall architecture;
- Impact of a failure of the device on nuclear safety;
- Regulatory context;
- Basic design of the system where the device will be introduced and in-depth knowledge of the overall safety philosophy of the nuclear plant.

It is important that the arrangements for the COTS device justification ensure that there is a suitable mix of competence. The specialist competence requirement needs to recognize the specific features of the COTS device (e.g. hardware architecture, extent of the code, complexity). Depending on the safety class for which the COTS device is intended to be used, specific competence may be required to carry out/assess certain techniques and measures.

In the evaluation of personnel against the competence requirement, consideration needs to be given to their qualifications, specific training, experience in techniques and measures expected for the safety class (e.g. Refs [9], [10], [27]) and previous experience in justification activities. Demonstrating the competence of the assessor is an integral part of the justification and must be documented as such.

3.2.2.2. Outsourcing

Depending on the commercial strategy of the end user, the assessment in Section 3.1.2 might be outsourced by the end user to a third party. In such a case, it is important that the end user maintains, as an 'intelligent customer,' a sufficient level of understanding of the key engineering judgement in the justification and the key findings. This is important to ensure that the integration of the COTS device justification into the overall I&C justification is carried out properly. When defining the contract specification for outsourcing the activity, a good understanding of the process is key to achieve a quality justification. This should ideally cover typical challenges

[21] In the following, the reference is to 'assessor', although it is understood that more than one person may be needed. In such cases, the key competencies identified in this section have to be covered by a team of assessors.

in the justification process, expectations in terms of documentation, evidence gathering, definition of criteria for successful justifications of a COTS device, and the depth of the assessment for the safety class.

Key aspects in case part of the justification is outsourced to a third party include ensuring a clear definition of roles and responsibilities, good communication between the parties involved and a comprehensive documentation in the justification document (e.g. assumptions in Section 3.1.1). For example, if an external assessor is performing the justification of the COTS device in Section 3.1.2, the end user needs to understand the vulnerabilities associated with the failure of the device and how they can be compensated for at the overall I&C architecture level. Similarly, the assessor needs to have a level of appreciation of the nuclear safety implication of a failure of a COTS device to inform its assessment activities.

3.2.3. Graded approach

The rigour of justifying a COTS device needs to be commensurate with the safety categorization of the function to be performed by the device (i.e. according to its safety classification).[22] When the COTS device performs more than one safety function, it needs to be classified according to the most stringent safety function. Various approaches to classification exist in different Member States (see Ref. [12]). As discussed in Ref. [23], the graded approach is "not intended to define concessions and relaxations allowing lower quality standards of design and development." However, the graded approach can be defined to identify minimum expectations for each safety class, both in terms of development process and verification (see Ref. [23]).

Typically, for higher safety classes (e.g. Class 1 in IEC 61513 [6]):

- Additional documentation may be required from the manufacturer (e.g. access to source code);
- Additional discussions with the manufacturer may be necessary to ensure that processes/tools used are suitable for the nuclear safety application;
- Additional V&V may be required at different safety classes (e.g. IEC 61508 [10] techniques and measures);
- Additional independent complementary activities may be required (e.g. additional static/dynamic testing, statistical testing).

Other examples of a graded approach are provided in IEC 62671 [9]. The graded approach generally influences the assessment strategy (e.g. extent of the audit or access to source code), but does not affect the quality of the justification (e.g. in terms of clarity of the engineering judgement or recoding of the rationale to support the justification conclusion).

3.2.4. Generic versus specific justifications of a commercial off the shelf device

All devices used in a system important to safety in a nuclear installation must be qualified for the intended service in terms of their capability to perform the required functions, and to perform these functions under any adverse service conditions that are consistent with the function to be performed. This verification is generally done as part of the integration phase (Section 3.1.3). The first part of the justification (Sections 3.1.1 and 3.1.2) can be developed at a generic level (i.e. without a target application in mind) or for a specific application (e.g. use of a COTS device to measure level in a tank).

While the application specific approach can be more targeted, and the integration part of the justification can be less time consuming, the advantage of the generic justification is that the end user can take advantage of the effort made in the justification for other applications. In fact, if the same COTS device was needed for different applications or for the same application but under different operating conditions (e.g. maintenance or other changes in the overall I&C architecture), the broader scope of the justification could make its reuse more efficient (e.g. parts of the assessment in Section 3.1.2 may need to be significantly reviewed).

Additionally, while the integration of the COTS device justification into the overall I&C architecture justification (Section 3.1.3) is also required for the application specific justification, this phase can typically be less

[22] Examples of a graded approach based on safety integrity are provided in IEC 62671 [10] and IEC 61508 [11].

onerous compared with generic justifications. In fact, in order to use a generic justification in a specific application, work is typically required showing (see Section 3.1.3):

- That the behaviour and other characteristics of the component considered in the generic justification are adequate to perform the safety function and any other application requirements or constraints.
- That the application and its environment will provide a suitable environment for the component to perform adequately. This may include environmental conditions such as temperature and vibration, infrastructure conditions concerning the power supply, and physical requirements such as space required to fit and maintain the component or interfacing requirements such as connectors.
- That any other constraints or prerequisites identified during the justification are or will be addressed during deployment. This may include any restrictions on use (e.g. restrictions on the range of functionality permitted during deployment, or any maintenance requirements such as calibration or reconfiguration).

The generic COTS device justification strategy outlined in Sections 3.1.1 to 3.1.3 includes the application specific justification as a limiting case.

3.2.5. Computer security[23]

As the COTS device may not be designed and developed with established computer security requirements, security measures need to be identified in order to protect the digital device from malicious acts.

Both external and internal threat actors (i.e. insider threats) need to be considered when performing a vulnerability assessment. COTS device features can either provide protection or be a vulnerability. The assessment needs to verify the robustness of the integrated protective features (e.g. protective write jumpers, changeable passwords) along with potential vulnerabilities. Where the protections in place are not sufficient and physical protection/enhanced security assessment of the COTS device is required, that needs to be captured as part of the assumption of the justification (Section 3.1.1.3) and then verified in the integration phase (Section 3.1.3). The end user will also assess and implement any of the needed protective measures. As part of the COTS device justification, tasks that could be performed include:

- Assessing the computer security vulnerability of the COTS device. This assessment reviews designed inherent protection mechanisms such as password protection, disabled ports, broadcast only external communications, lockable cabinets and/or covers, along with potential vulnerabilities. This will point the user to additional protection measures that may be required. (It is important to highlight that the measures are highly dependent upon the application and hence need to be evaluated in depth by the end user, considering the specific target application. It is also important that the requirements provide a direction for cyber hardening activities.)
- Reviewing and documenting the COTS device supplier's SDOE for acceptability and their secure coding practices.
- Assessing the COTS device for any complex, unwanted or unused code such as malicious code, or code that could adversely affect the performance of the safety function.
- Assessing the COTS device for vulnerabilities in its communication capabilities such as wireless (Wi-Fi, Bluetooth, Zigbee, etc.), Ethernet, highway addressable remote transducer (HART), and memory card slots.
- Assessing the COTS device for software and services providing remote access and their removal or disablement.
- Verifying the material handling and shipping processes for the digital device, and providing protection from changes between shipment from the vendor to receipt by the end user. (One best practice is that the software is sent independently from the hardware. Software can be cryptographically signed to verify its authenticity. Hardware is sent with tamper proof seals. Software is then loaded onto the hardware at the site. This significantly increases the difficulty for an adversary to compromise the system in transit.)

[23] Various standards are available in the literature regarding computer security (see Ref. [29], Nuclear Power Plants — Instrumentation Control and Electrical Power Systems — Cybersecurity Requirements, IEC 62645:2019 [30] and Nuclear Power Plants — Instrumentation and Control Systems — Requirements for Coordinating Safety and Cybersecurity, IEC 62859 [31]). This publication only provides high level considerations and refers to these specific standards for more detailed analyses.

3.2.6. Engineering judgement

The assessor will need to exercise engineering judgement throughout the complete assessment process. For example, the assessor will need to consider whether the quality assurance programme, and the development and manufacturing processes are adequate. The notion of adequacy will be framed by relevant applicable standards, but it is engineering judgement that will identify potential shortfalls. In addition, engineering judgement is also required for other assessment activities, which may result in findings that would need to be sentenced according to their importance and potential safety impact. Finally, considering all of the findings, shortfalls and their compensations, the assessor will need to determine whether or not the device is suitable for a nuclear application, using engineering judgement again.

All of the activities identified above require technical, engineering judgement, which requires competent and experienced assessors (see also Section 3.2.2.1). In a good quality justification, the rationale behind this judgement needs to be captured so that it can be reviewed by an independent specialist at a later time.

4. JUSTIFICATION PROCESS

The COTS device justification process consists of the following steps:

(1) Defining requirements and prerequisites;
(2) Selecting candidate devices;
(3) Obtaining manufacturer information and support;
(4) Planning;
(5) Assessing;
(6) Identifying lifetime issues;
(7) Preparing the justification documentation package.

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

4.1. STEP 1: DEFINING REQUIREMENTS AND PREREQUISITES

In this step the following are identified:

- Device requirements to be considered during the justification;
- Prerequisites to be met by the application in order to guarantee that requirements are achieved.

An essential input when evaluating a device is identifying 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). As described in Section 3.2.4, this can be done by defining all the necessary requirements for the application or by performing a generic assessment by considering the functionality of the device as claimed by the manufacturer (e.g. in data sheets or user manuals). For the generic justification, it may be that the justification only considers a subset of the overall functionality and characteristics (e.g. only considers the 4–20 mA output of a pressure transmitter and excludes any alarm features). In a generic justification, an application specific justification would still be needed to show that the device and its justification are suitable for the application (e.g. by including traceability from the generic justification to the application safety function). This can be done as part of the integration of the COTS device justification in the overall plant safety justification (see Section 3.1.3).

In either case, the requirements definition will include the functional, performance and dependability requirements as well as the system class (IAEA SSG-30 [3], IEEE 603 [4] or IEC 61513 [6]).

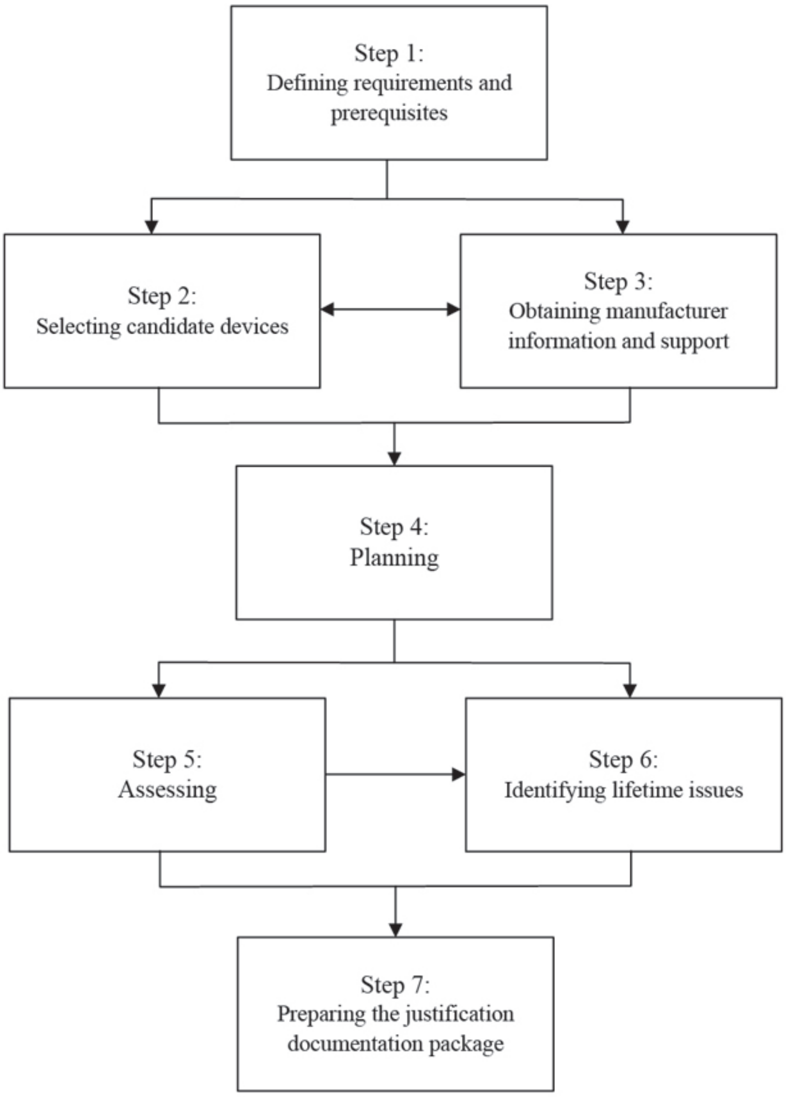

Step 1:
Defining requirements and prerequisites
Step 2:
Selecting candidate devices
Step 3:
Obtaining manufacturer information and support
Step 4:
Planning
Step 5:
Assessing
Step 6:
Identifying lifetime issues
Step 7:
Preparing the justification documentation package

FIG. 3. Justification process steps.

For older plants, it may be the case that the requirements are not well documented, the classification may not have been performed or the available documented requirements may not adequately address all the operational conditions in which the product must perform. In such cases, the first step in the justification process is to reconstruct the requirements from the plant design basis.

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 requirements will typically include the following:

— System level safety role (design basis function), to explain the safety purpose of the candidate device within the target system in sufficient detail to support the categorization of the function of the target system (for application specific justifications as written in Section 3.2.4).
— Potential constraints in the selection of the devices based on considerations of the overall I&C architecture such as CCF issues or security issues (for application specific justifications).
— Regulatory requirements based on the safety category (or system class) of the target application depending on its nuclear safety relevance (e.g. IAEA SSG-30 [11], IEEE 603 [4] or IEC 61226 [13]).
— Primary functionality of the device, including functional and performance requirements such as accuracy or response time. These are typically the requirements associated with performing the safety function.
— Other auxiliary functionality such as configuration or communication functions.

- Dependability characteristics of the device that ensure continuity of correct service, including reliability and robustness. These may include the absence of classes of faults (e.g. divide by zero), the ability to recover from faults without causing a component failure or to continue to operate in abnormal environmental conditions. Some of these can only be completely justified if the application is taken into account. It is expected that the aspects of the device that will have an impact on these characteristics are defined, either by considering aspects that are application independent, or by considering the absence of vulnerabilities that may make them unattainable and mitigations if those vulnerabilities are present. Such mitigations may include:
    - The avoidance of failures caused by human error;
    - Availability, including failure recovery (e.g. whether failures are annunciated);
    - Implementation of fail-safe implementations that place the device in a safe state;
    - Ability to perform within the specified environment, seismic and other physical conditions;
    - Immunity to failures of auxiliary functions so that they do not affect the primary function;
    - Required maximum failure rates for the device as a whole.
- Computer security measures (features/functions), such as the following:
    - Protecting the application configuration against changes (e.g. via a password);
    - Disabling communication channels that are not used by the specific application, if possible;
    - Checking the integrity of the program (e.g. using cyclic redundancy checks or checksums).

In addition, the description needs to specify the prerequisites of the device to be met by the application in order to guarantee that the described behaviour is achieved. This could include:

- Required resources (e.g. power, communications bandwidth);
- Environmental constraints (e.g. temperature, EMI, humidity, vibration, shock);
- Operational and maintenance requirements (e.g. periodic calibration, correct probe connection).

Documenting these requirements and prerequisites will be the basis of the justification process (see Section 3.1.1.1) to ensure that the justification will provide reasonable assurance that the COTS device can and will perform the safety function over the defined range of use and specific environmental conditions [3].

In addition to the requirements and prerequisites described in this section, the contract may also include, depending on the country specific regulations, the level of documented evidence required, information to support CCF assessment (see Section 2.1.2), computer security measures (functions) (see Sections 3.2.5 and 4.5.1.5), and counterfeit protection measures (see Sections 2.2.3 and 3.1.3.2).

4.2. STEP 2: SELECTING CANDIDATE DEVICES

In this step, assessors:

- 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 arrangements, including the willingness of the manufacturer to engage with the justification process and to give access to information on the development process and design of the product;
- Assess the complexity of each candidate device to evaluate the likelihood of successfully completing the justification;
- Review the existing documentation to determine the likelihood of successfully completing the justification.

The selection of the device is based on the device's functional and behavioural characteristics (such as performance and dependability), 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, processes information, operating history or source code.

For an application specific justification, the candidate devices will need to be able to meet the application requirements, as described in Section 4.1. Similarly, for a generic justification, the device will be selected based on its functionality and the likelihood of it being usable in a number of applications.

Once candidate devices are identified, they are evaluated to determine whether there is sufficient available evidence and built in capabilities to attempt the justification process and proceed with the next steps. It is important to be clear about the digital content of the devices under consideration (see Section 2.2.2). In addition, the complexity of the device's architecture and design will impact the likelihood of success in justifying it. Although the boundary for complexity is difficult to define, it is useful to have an initial assessment to identify the high risk areas in a design (see Section 2.1.1) and reject any devices that are clearly too complex to be able to justify.

Different aspects have to be checked and answered in order to select the candidate device. Requirements of Commercial Grade Products and Criteria for Their Use in the Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, VDI/VDE 3528, Part 1 [32] groups the aspects into those related to documentation, technical properties, quality and obsolescence. The aspects and the corresponding questions are listed in Table 1. The questions have been adapted to COTS devices in the scope of this publication. Typically, this assessment will be performed in parallel with Step 3, as a significant amount of information is necessary to answer these questions. Alternatively, EPRI TR-106439 [19] and EPRI TR-107339 [28] also provide information that can be used in this step.

TABLE 1. QUESTIONS FOR SELECTING A CANDIDATE DEVICE

Area	Questions
Documentation	— Are the principal descriptive documents for the COTS device available (e.g. detailed description of the device, structure of the main components, available functions, characteristics and interfaces to other systems)? — Are documents on quality assured development available for the device, its hardware (schematics, parts numbers, etc.) and software (requirement specifications, documentation of the life cycle, configuration and identification documentation, test certificates, compliance with programming standards)? — Are there comprehensible test documents of the primary functions of the COTS device under the physical and environmental conditions specified (e.g. issued by the manufacturer or a testing organization)? — Are qualification certificates and supporting reports for the COTS device to be selected already available (from which testing organization, and in accordance with which standards)?
Technical properties	— Does the COTS device have the necessary features (e.g. monitoring mechanisms, fault detection, defined/definable failure behaviour)? — Is the COTS device able to operate under the intended/specified environmental and other physical conditions (e.g. manufacturer data on mechanics, climate, electrical equipment, electromagnetic compatibility (EMC))? — Is the COTS device a digital device with software or complex programmable hardware such as FPGAs or ASICs (see Section 2.2.2)?*
Quality aspects	— Is the COTS device suitable and/or robust enough to operate under the specified environmental and physical conditions? — Was the COTS device manufactured in accordance with highly industrial commercial grade production processes with integrated quality management (e.g. Ref. [10])? — Does the manufacturer have a problem reporting process in place that includes the collection and analysis of reported defects metrics and is it considered when eliminating defects in the devices and their production process? — Does the manufacturer have a change process that includes impact analysis and identifies the required V&V activities?

TABLE 1. QUESTIONS FOR SELECTING A CANDIDATE DEVICE (cont.)

Area	Questions
Obsolescence management	— Prior clarification of the requirements for the later determination of the spare parts strategy: ● Does the manufacturer have a spare parts strategy? ● What are the requirements with regard to the long term storage of the hardware components for the provision of spare parts? — Does the equipment engineering include sufficient maintainability features (such as diagnosis and testing options or replaceability) and can maintenance measures be carried out without spurious actuation?

* Methods need to be used to ensure that digital devices/components are identified in the procurement process. EPRI 3002008010 [18] was published in response to several cases of operating experience where undeclared digital content was found, including one product in which the product was installed in the plant without the end user's knowledge. Identification may require actual disassembly of the equipment for inspection.

It is possible that answers to these questions may not provide evidence or that some of the answers will only be obtained in later stages of the justification process. However, it is more likely that the justification will succeed if the majority of these criteria are met. It is important to understand what the risks are of not being able to justify the device before a significant level of investment/resources is spent on the justification. This provides an opportunity to reject a device before a significant amount of effort has been spent in its assessment.

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

4.3. STEP 3: OBTAINING MANUFACTURER INFORMATION AND SUPPORT

In this step, the assessor will:

— Establish a contractual relationship with the manufacturer;
— Agree and sign a non-disclosure agreement if required;
— Ascertain that the evidence and documentation will be made available to carry out the justification;
— Agree to an assessment process and access to information;
— Establish the versions of components (including software and hardware, if applicable) of the device to be justified;
— Agree on the justification report content that users will receive (i.e. what can be shared with the user).

The justification of a COTS device involves gathering evidence to support the assessment. It is important that the versions of the COTS device be established early on (including versions for hardware and software), so that the information is relevant to the versions under consideration. Some of this evidence will come from the development and quality assurance processes of the manufacturer and might include detailed design information, V&V records or even the source code of the device. Therefore, it is necessary to agree with the manufacturer on the level of information that will be made available and what manufacturer resources are necessary to support the justification (e.g. support an audit of the factory or answer any questions that may arise from the analysis performed). An effective way of managing this is to ensure that the following is done during procurement:

— The manufacturer identifies the type, extent and availability of quality assurance, development evidence and evidence of correct behaviour.
— As part of the bid or quote process, the manufacturer includes costs to support the justification process.
— The manufacturer agrees to provide or make available for review any necessary information to support the justification process and specifically identify the types and extent of information needed in the contract.

In order to have access to this information, it is likely that a non-disclosure agreement will need to be put in place.

It can be challenging to identify in advance all of the documents and evidence that the manufacturer will be expected to make available. Although it is important to prepare lists of evidence requirements as far ahead of time as possible before meeting with the manufacturer, information on the manufacturer's terminology and approaches may be needed so that the requirements can be put in language that the manufacturer understands.

Manufacturers are sometimes reluctant to, or will not allow, these documents to leave their premises without strict controls, so negotiation may be required to balance the needs of the manufacturer with the feasibility of performing the assessment and the requirements of a trustworthy assessment report. On-site reviews and assessments may be a necessary compromise.

At the end of Steps 2 and 3, it is possible there will be either none, or one or more devices that have been selected to move on in the assessment.

4.4. STEP 4: PLANNING

In this step, a device justification plan is developed for each of the devices selected for justification.

COTS devices vary in terms of the technologies used to implement them as well as the development process followed and information available to develop them. Any justification approach will need to take into account the requirements defined for the device itself (see Step 1), the application or applications in which they will be used and the information that might be available to justify them. Artefacts of the development process or from application of the manufacturer's quality assurance processes may be used as evidence during the assessment, as well as evidence resulting from any certification that the device might have. The justification strategy will need to take into account:

- The intended use or safety function to be performed by the device, including any categorization/grading consideration, functionality and environmental and other physical constraints;
- The level of cooperation from the vendor, including information made available and the possibility of performing an audit;
- Evidence that exists as a result of the device's certification;
- The technologies used to implement the device (e.g. FPGAs, C code, operating systems, HART, communication protocols);
- The development process followed;
- The operating data available, including quality of collecting and feedback process, number of devices sold of which version, and number of defects found in the field, including analysis of failure data.

The justification follows a device justification plan, which documents the feasibility of the justification and the methods to be used, taking into account the factors listed above. It also explains how the activities planned will meet any considered regulatory approaches, how any areas not covered are identified and a rationale given for their omission. The plan will need to take into account any restrictions imposed by the manufacturer, and therefore, it is useful if the manufacturer agrees with the plan or develops a parallel consistent plan for themselves. The plan will typically include:

- Justification and assessment methods to be used, including explanation of why these are adequate and sufficient to support the necessary claims about the device and meet regulatory requirements;
- Evidence to be collected or generated to support the assessment;
- Identification of the team to perform the assessment based on the design of the device and justification of their competency (e.g. C code review, ASIC design);
- Schedule and milestones;
- Decision points and whether to complete the assessment or conclude the device is not suitable (e.g. has too many deficiencies to be worthwhile addressing).

The evidence expected and its detail are proportionate to the target safety class of the justification.

4.5. STEP 5: ASSESSING

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 (Section 4.5.1);
- The functional, performance and dependability behaviour meet the requirements (Section 4.5.2);
- Potential vulnerabilities and systematic faults have been managed to deliver a product that meets the safety and functional requirements (Section 4.5.3);
- The environmental qualification data exist that are representative of the in-service conditions and demonstrate that the device will meet the functional requirements for all credible variations in the in-service external environment (e.g. temperature, EMI/RFI, seismic events) (Section 4.5.4);
- Additional confidence is achieved through independent complementary activities (Section 4.5.5).

The different aspects of the assessment can be seen in Fig. 4, where the grey boxes relate to assessment of the device behaviour and the white box to the assessment of development and manufacturing processes. The independent complementary assessment focuses on specific areas of function, performance and dependability of the device or its vulnerabilities or failure modes. Each of the different assessment aspects can be graded according to the safety role the device is to perform.

4.5.1. Quality assurance, development and manufacturing processes

This part of the assessment looks at the processes implemented by the manufacturer for the development and production of the COTS device and identifies any gaps in the requirements for a nuclear grade product (e.g. against IEEE 603 [4], IEEE 7-4.3.2 [5], IEC 62671 [9] or IEC 61508 [10]). It includes evidence of the use of appropriate processes, methods, techniques and tools, tools qualification, personnel experience and competence and configuration control.

Evidence that a sound development process and quality assurance principles have been followed increases confidence that a good design approach was implemented (which decreases the chance of introducing faults during development and increases the chance of finding bugs during V&V). It also provides assurance about the pedigree and relevance of product evidence. For example, it can be used to show that the V&V evidence was generated independently, using qualified tools, by competent personnel, and that the evidence is relevant to the version of the firmware/hardware being justified. Evidence may be a result of review or audit of the manufacturer's quality management system, approach to development or safety management approach.

4.5.1.1. Development process

This part of the assessment considers the device's development quality. Quality cannot be achieved unless a commitment is made to it in every phase of the design, implementation and production and any supporting processes. This may be achieved using an adequately defined life cycle. A life cycle is a structured approach to development projects that groups activities into phases. For each phase, the life cycle defines what is required

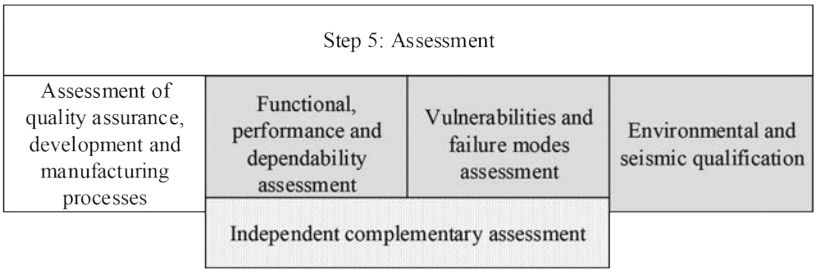

Step 5: Assessment
Assessment of quality assurance, development and manufacturing processes
Functional, performance and dependability assessment
Vulnerabilities and failure modes assessment
Environmental and seismic qualification
Independent complementary assessment

FIG. 4. Different aspects of the assessment.

(the phase inputs) and what must be accomplished or produced (the outputs). The life cycle shows a chronological sequence for each of these phases.

The assessment of the development process also needs to consider design practices and V&V activities performed.

Evidence of good development procedures and, particularly, configuration management can increase confidence that the requirements are met, that there is good traceability from requirements to tests, and that the versions of the hardware and software and the changes made are correctly managed. Overall, a high quality development process inspires confidence in the quality of the device, as it is indicative of effective management of the project, and it is likely to minimize fault creation and maximize fault detection. This is particularly important for software or complex hardware (such as FPGAs), where inspection or testing alone cannot confirm the behaviour of the device.

The development process assessment also determines whether third party components were included in the device and the process for selecting and validating those. It also needs to consider how the supply chain is managed and the quality checks performed to accept third party components.

The life cycle can be assessed against a relevant standard (e.g. IEEE 603 [4], IEEE 7-4.3.2 [5], IEC 62671 [9] or IEC 61508 [10]), but for older or non-standards compliant developments, it may be difficult to find all of this information. Whether this is acceptable depends on the graded approach used. At a minimum, it needs to be possible to reconstruct the life cycle that was followed in practice, even if no formal life cycle was planned.

4.5.1.2. Quality assurance

Controls applied throughout development and production of the device ensure that it is well defined and can be reproduced in a repeatable way. This covers aspects of:

- Configuration management, which helps to ensure that the components and design are controlled;
- Supply chain management, which helps to ensure that third party elements of the device are controlled and verified through an acceptance process;
- Staff competency and qualification and training schemes;
- Change management.

Configuration management is the process of identifying and documenting the characteristics of systems or components and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and documented. This is achieved by applying adequate configuration controls that will ensure that the overall consistency of the development process is maintained throughout the development life cycle. Change management relies on configuration management and describes the process followed to implement changes, which may include performing impact analysis of the changes and identification of required verification activities.

Confidence in the design is much higher when it can be shown that the personnel involved were competent to perform the tasks that were assigned to them (see also Section 3.2.2.1).

4.5.1.3. Design

Design principles, developed through experience and the accumulation of good practice need to be applied in development of the COTS device. In general, these are expected to contribute to the reliability of the device.

Design principles may include the following broad classes:

- Well structured with low complexity (e.g. modularity, avoidance of complex data flows and structures);
- Engineering margins (e.g. de-rating);
- Design for reliability (e.g. fail-safe design, fault tolerance, self-monitoring, avoidance of sources of unpredictability such as concurrency in computer based systems);
- Design for testability;
- Reuse of prevalidated components.

4.5.1.4. Tools

The tools used in the development and V&V of the device have an impact on its quality. A considered decision needs to have been made to ensure that the tools have appropriate provenance, certification where applicable, and support arrangements where required. There needs to be a strategy for maintaining tools and evaluating and accepting changes to the tools.

The devices considered in this report typically do not come with additional maintenance tools such as monitoring and diagnostic/test tools (and these are usually separate from the configuration tools and run as a separate executable), although some devices may include tools to perform calibration and configuration of the device. In addition to this, the most important tools are those used for software or FPGA development, including V&V. Guidance on these can be found in IEEE 7-4.3.2 [5], IEC 60880 [7], IEC 61508 [10] or Nuclear Power Plants — Instrumentation and Control Important to Safety — Development of HDL-Programmed Integrated Circuits for Systems Performing Category A Functions, IEC 62566 [33].

4.5.1.5. Security

The assessment of the manufacturer's processes needs to include security considerations. In particular, it has to take into account the security at the manufacturer's site, the security of the development and manufacturing environment and the manufacturer's approach to managing its supply chain.

4.5.1.6. Obsolescence management

If the manufacturer's obsolescence management was not discussed in Step 2, it is useful to understand the obsolescence approach used by the manufacturer for the device being assessed. This approach may include:

- Plans for making the device obsolete;
- Willingness to enter contractual agreements to supply the device for a certain number of years;
- Notification period for last buys;
- Notification process for obsolescence.

4.5.1.7. Manufacturing

Quality assurance in manufacturing is important in that it inspires confidence that devices produced and delivered for use in the NPP will be identical to the product that has been assessed (although the availability of components may affect the device's design and therefore component changes might be required — see Section 5.5). The supplier is expected to maintain manufacturing processes comparable to the quality assurance requirements found in Quality Management Systems — Requirements, ISO 9001 [34]. Example aspects of manufacturing processes that may be considered include:

- Incoming inspection of components;
- Change control of components;
- Calibration of testing equipment against appropriate standards;
- Serial number of devices manufactured and traceability to versions of components through their BOM;
- Identification of versions of the produced/shipped devices;
- Production testing or manufacturing testing (on each device).

4.5.1.8. Evidence of quality assurance, development and manufacturing processes

Typically, evidence of quality assurance and the use of appropriate development and manufacturing processes by the manufacturer is obtained by performing a site visit, audit or survey of the manufacturer's site and quality controls. The scope of this activity focuses on the particular device being assessed, although some procedures might be applied to a number of different devices from the same manufacturer.

Criteria for the audit may vary; in the United Kingdom (UK), for example, audits are done following the emphasis assessment, which is an approach developed by UK nuclear licensees to assess the quality assurance, design and development processes used by manufacturers of smart devices. In the United States of America (USA), the criteria are defined by the critical characteristics intended to be verified using EPRI method 2; they will typically include the areas discussed in this section (see also EPRI 1011710 [27] and 10 Code of Federal Regulations (CFR) Part 50, Appendix B [35]).

4.5.1.9. Gaps and compensation

The processes followed by the manufacturer are usually assessed by checking compliance with relevant nuclear standards. However, COTS devices are not commonly developed to these standards; instead they may be developed according to other standards such as those in IEC 61508 [11] or standards relevant to the function they perform (e.g. Measuring Relays and Protection Equipment, IEC 60255 [36] for relays and protection equipment).

A standard compliance evaluation to assess the development and manufacturing processes will aim to cover a variety of different components and will make assumptions about technologies used that reflect good practice at the time the approach was developed.

Given the variety of devices, processes and technologies covered, it is likely that the manufacturer may not be able to provide evidence to demonstrate a certain requirement was met. It is also possible that a supplier may develop a COTS device to an older industry standard. This will also introduce gaps that need to be assessed.

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 mitigations need to be specific to identified process deficiencies.

These are cases where a flexible approach to justify devices is particularly useful. For example, a justification can be structured around gathering requirements of the device's intended behaviour and comparing it with available evidence supporting its actual behaviour by using an approach such as Cogs (see Ref. [37]).

There are a number of techniques that can be used as compensatory measures, such as the following:

- Applicable and credible operational experience, which may be used where justified to compensate for weaknesses in other elements;
- Evidence of stability (i.e. low rate of changes) of the product during a meaningful amount of manufacture and use of the product;
- Device specific complementary tests performed to fill gaps in pre-existing documentation of tests, or to extend test coverage as appropriate to the intended application and the other elements of evidence of correctness;
- Compensation at the system level to mitigate device failures or convert them to safe failures;
- Improvements in the documentation initially provided by the manufacturer;
- FMEA or FMEDA;
- Additional special procedures to address quality assurance gaps.

Other examples of evidence sources are given in Section 3.2.1.

4.5.2. Functional, performance and dependability assessment

The functional, performance and dependability assessment focuses on showing that the device meets the requirements described in Step 1, provided that any prerequisites are met.

Different types of evidence are described in Table 2: evidence that 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 that may be produced for the assessment.

The specific attributes of interest will vary with the device and the possible application that will use it. Example attributes and types of evidence are given in Table 3. Some of the evidence may be related to the hardware (e.g. FMEDA, safe failure fraction, use of de-rating), some may be related to the software (e.g. use of coding standards, unit tests, static analysis), and some will be about the integration (e.g. hardware watchdogs, response of the software to random hardware faults) or the component as a whole.

TABLE 2. TYPES OF PRODUCT EVIDENCE

Type of evidence	Description
Testing evidence	Testing evidence is generated by exercising the device in a representative or actual environment using a range of data (test cases). The output or behaviour is compared against expected results. Software based systems and complex hardware are difficult to test completely because simple functionality can hide an enormous amount of internal complexity and number of internal device states. This means that the extent to which the correct behaviour of software can be proved by testing is severely limited. There are several types of testing, for example: — Testing done during development, including prototype testing, hardware and software testing, integration testing, regression testing of changes, etc.; — Functional testing; — Negative testing (e.g. where the device is subject to invalid inputs); — Environmental testing (temperature type testing, EMC testing, etc.).
Analytical evidence	Analytical evidence is generated through analyses of design artefacts carried out at various stages of system development. In contrast to testing, no actual exercising of the system takes place. Instead, analytical evidence comes from analysis of specifications, design documents, source code and other artefacts of the development process. These analyses can be focused on particular properties (i.e. demonstrating that a proposed design will always fulfil particular safety criteria) or on general behaviours (such as the absence of deadlock in a concurrent system). Analytical evidence in support of a software assessment can come from static analysis: analysis of the software source code without executing it. Static analysis techniques range from checking conformance to coding standards, to advanced techniques such as correctness proofs. Depending on the technique, static analysis might support a process argument, demonstrate absence of vulnerabilities or directly support a claim that the software meets its specification.
Quantitative evidence	Quantitative evidence includes both hardware and software failure rates generated through reliability modelling and/or failure rate data. Producing quantitative evidence often involves software reliability models such as reliability growth models, or statistically informed testing. Previous testing and operational data are often the primary sources used by such a model. For digital COTS devices with extensive operational usage, the in-service data may be statistically analysed to give predictions on the units' failure rates. However, such predictions depend on the quality of the data, the similarity between the eventual usage of the device, operating population, data collection methods and the way they have been used in service. Nevertheless, the proven in use data may provide a general/qualitative indication of the reliability of a smart device. The credibility of such reliability indication depends upon the extensiveness of the proven in use data and the process followed in collecting them.

TABLE 3. EXAMPLES OF EVIDENCE TO DEMONSTRATE BEHAVIOUR PROPERTIES

Attribute	Explanation	Example evidence
Functionality	This may include: — Inputs and outputs — Alarms — Algorithms required — Configuration — Communication — Interfaces	— Functional testing — Black box testing — Traceability from requirements to tests — Non-interference of the functions not necessary to the safety function with the safety function
Timing	— Response time — Throughput	— Performance testing — Static timing analysis — Worst case execution time — Predictability analysis of the design

TABLE 3. EXAMPLES OF EVIDENCE TO DEMONSTRATE BEHAVIOUR PROPERTIES (cont.)

Attribute	Explanation	Example evidence
Accuracy	Required precision	— Testing — Analysis of conversion tables — Rounding errors
Dependability	This may include: — Fail-safe behaviour — Reliability — Failure recovery Dependability would also be demonstrated while considering the vulnerabilities assessed (see Section 4.5.3)	— Failure analysis — Fail-safe design — FMEDA — Self-monitoring — Diagnostic coverage — Testing of diagnostic features to show they do not adversely affect the safety function — Analysis of operating history — Evidence of customer problem reporting and analysis — Statistical testing — Fault insertion testing — Power supply interruption testing — Static analysis
Operability	Avoidance of failures caused by human error	— Task analysis — Interface analysis (see Ref. [38])

4.5.3. Vulnerabilities and failure modes assessment

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. These could be, for example, division by zero or buffer overflows if not caught by error handling, use of unspecified or undefined software constructs such as when using C, or timing errors in FPGAs.

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). Examples are given in Table 4. The list is not intended to be complete; it only illustrates the type of issues to be considered in this type of assessment. It also provides examples of evidence that might be produced to show that these vulnerabilities are absent or unlikely to be present.

Additional guidance on failure analysis techniques is available in Appendix II.

The potential for and impact of vulnerabilities need to be assessed in terms of possible negative impacts in the intended application.

Hardware, software and component vulnerabilities need to be evaluated to determine postulated impacts (indeterminate, unexpected behaviours or actions, failure) 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 impacts must then be evaluated to identify preventative and mitigating measures that may be used to offset these vulnerabilities. For example, given particular postulated internal or externally induced fault, will the device fail to a safe or unsafe state? Will or can the failure be detected? How quickly and reliably? And, what are the potential adverse consequences?

Confidence in the correctness and robustness of the design is obtained by confirming that the design has considered and taken appropriate precautions for likely sources of design faults. If this has not been done by the manufacturer, it could be performed as part of the independent assessment described in Section 4.5.5.

TABLE 4. EXAMPLES OF POSSIBLE VULNERABILITIES

Technology/implementation	Example of vulnerabilities	Possible evidence
Programming languages (e.g. C, Java)	— Division by zero — Buffer overflow — Pointer arithmetic — Compiler errors	— Coding standards (e.g. NUREG/CR-6463 [39]) — Static analysis — Compiler validation
Interrupts	— Data tearing and deadlock/live lock	— Static analysis/code review
FPGAs	— Timing — Tool chain vulnerabilities and equivalence between design and implementation	— Coding standards — Tool justification
General	— System overload	— Load testing — Watchdog timers
	— Inappropriate use of time dependent data	— Review of design and white box testing
	— Inappropriate/undefined modes of operation	— Clear definition, code review and testing
	— Communication faults	— Communication testing — Digital communication isolation (e.g. US NRC DI&C-ISG-04 [40]) — No external communications
	— Security vulnerabilities	— Security informed HAZOPs — Identity and analysis of any unaccounted for code that cannot be traced to requirements — Assessment of vulnerabilities in communication capabilities such as Ethernet, HART, wireless, etc. — Static analysis

4.5.4. Environmental and seismic qualification

As part of the justification program, a test programme needs to be executed to demonstrate that the COTS device will perform its safety function during all seismic and environmental parameters specified. The qualification programme can be addressed by test, analysis or a combination of the two methods. For example, this may be done in accordance with Nuclear Power Plants — Electrical Equipment of the Safety System — Qualification, IEC 60780 [41]; IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, IEEE 323 [42] and Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants, RG 1.209 [43] (digital); Electromagnetic Compatibility (EMC), IEC 61000 [44] (EMI/RFI); Guidelines for Electromagnetic Interference Testing in Power Plants, EPRI TR-102323 [45] or Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems, RG 1.180 [46] (EMC); and IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, IEEE 344 [47] (seismic). Following are typical qualification parameters:

- Hardware ageing;
- Susceptibility to EMI/RFI and power surges;
- Ionizing radiation;
- Temperature and humidity extremes;

- Voltage/frequency variations;
- Seismic and non-seismic vibration;
- Operational cycles.

For application specific justifications, the qualification programme will be performed in a defined sequence and in conditions that simulate the actual in-plant environment, simulating all interfaces/connections and in-service mounting. The qualification test programme has to be designed with bounding test envelopes (i.e. min. and max. temperatures, pressures, humidity, bounding seismic spectrum, worst case mounting details) and clear acceptance criteria with tolerances. Any limitations that result from a test programme need to be clearly documented and encompassed in all installations. Test specimens must be functional during testing and monitored to identify degraded performance and failures during the testing. Exercising the safety function during the testing is the preferred method during testing to identify performance changes.

Other methods for seismic qualification in lieu of testing may be deemed acceptable based on the regulator's requirements such as qualification by analysis or operational experience.

Per IEEE 323 [42], the manufacturer may need to identify subcomponents with ageing mechanisms in order to establish a qualified (harsh) or service (mild) life.

The user has to review and accept test results and any anomalies for compliance with requirements, implement any limitations and/or conditions (i.e. periodic maintenance, replacement of age sensitive components) and update uncertainty calculations based on test data.

Caution: For generic qualifications, the user has to verify that the device functions required for the specific safety function are within the scope of the testing. For example: Were all input types tested? Was communication port functionality a part of the qualification? Were requirements relaxed, such as reduced seismic profile for relay chatter?

4.5.5. Independent complementary assessment

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 safety classification of the device and vary from State to State.

The general principle is that the end user will perform (or commission) an assessment to challenge the evidence produced by the manufacturer, and this will include some of the aspects described in Sections 4.5.2 and 4.5.3 (focusing on the behaviour of the device rather than on its development process). Depending on the grading of the component and the State's practices, this may include:

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

An example of a country specific graded approach to independent complementary assessment can be seen in Annex IV.

4.6. STEP 6: IDENTIFYING LIFETIME ISSUES

In this step, the limitations and conditions necessary to preserve the behaviour properties of the component during its lifetime need to be identified.

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

It is necessary to consider that changes will occur over time that will affect the device itself (the technical changes, for example, resulting from ageing) and also the people that use it and the organizational structure in which they operate (the non-technical changes). These aspects interact in various ways. For example, the ongoing maintenance of a device depends on its capacity to be maintained and the reliability of its components as well as the availability of adequately skilled engineers and appropriate documentation. Most of the social aspects require consideration at the application level and depend on the quality systems and safety culture of the end user. These form part of the interface to the application safety justification.

Consistent behaviour over the component's lifetime depends on four factors:

(1) The application continuing to fulfil the device's prerequisites, as defined in Step 1.
(2) Maintaining qualified over the service life. Changes due to age being rendered benign by corrective or preventative maintenance or other processes.
(3) Deliberate changes such as calibration or reconfiguration being benign.
(4) Unintended changes such as damage or vandalism being prevented as far as possible and rendered benign by corrective maintenance if they occur.

It is convenient to understand these aspects from the point of view of the component, the manufacturer and the application.

From the component's point of view, evidence is primarily concerned with aspects of the design of the product. An analysis of design documentation may result in verifying that the design of the device can adequately handle predefined changes, such as changes due to age or calibration. Additional testing can be performed to provide more confidence in the product to maintain its behaviour over time.

Examples of sources of information from the component's design and development are listed in Table 5.

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. This would be documented and agreed with the user.

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 claim may involve the product's operating and maintenance procedures and system design documentation to demonstrate that appropriate security provisions are in place.

Table 6 lists examples of activities required at the application level to support the argument that the instrument's behaviour continues to match up with its documentation.

4.7. STEP 7: PREPARING THE JUSTIFICATION DOCUMENTATION PACKAGE

In this step the device justification report (DJR) needs to be completed and issued and the user documentation and safety manual identifed and updated.

TABLE 5. SOURCES OF INFORMATION FROM COMPONENT DESIGN

Type of changes	Sources of information
Changes due to age	— Design features that tolerate ageing, such as component de-rating — Design features to work around ageing, such as the ability to calibrate or to replace life limited components
Deliberate changes	— Well designed user interface and documentation of connection panel layouts — The ability to test the device
Unintended changes	— Designed-in protection against misconnection — Security provisions

TABLE 6. SOURCES OF INFORMATION FROM APPLICATION

Type of changes	Sources of information
Changes due to age	— Analysis (no ageing mechanisms) — Preventative maintenance (replacement of time sensitive components)
Deliberate changes	— Manufacturer support arrangements — Skilled staff — Available documentation, both of the device and its application — Correctly performing any required change
Unintended changes	— Provision of physical security controls — Procedural controls to avoid changes — Configuration controls during maintenance activities — Proper interconnection and use of the device to avoid damage

The DJR has to be completed and issued following a process of review, comments and challenges. It may include:

- Scope and definition of the safety function as it relates to the device.
- Overview description of the device's architecture and operation with key design features.
- List of the device's baseline software and hardware versions that are being justified.
- Explanation of how the justification plan was implemented.
- Suitability requirements considered.
- Detailed methodology and the specific methods used.
- Argument and references to evidence that supports or otherwise claims that:
  - The development and manufacturing processes are adequate;
  - The functional, performance and dependability requirements are met;
  - The vulnerabilities and failure modes have been considered and mitigated;
  - The component performs adequately within a defined qualification envelope.
- Evidence to support CCF analysis.
- Any user requirements, restrictions on use or limitations identified to address weaknesses and gaps.
- Any required supplementary user documentation for safety. This may be captured in a new or updated safety manual (see IEC 61508 [10]) or incorporated into the user documents for a project (e.g. user manual or maintenance manual).

The DJR will refer to a number of reports produced during the justification as well as to documents that existed before the justification started (including manufacturer's documents and any existing certification). Evidence to support the DJR claims may include supplier specifications, design documentation, V&V plans, FMEA report or reports describing any additional analyses and tests performed. In addition to the DJR, in some cases, a summary report might be written that does not contain any of the manufacturer's intellectual property so that it can be more widely distributed, enabling other end users to explore the use of the device.

The user documentation needed for operation and maintenance, which includes a safety manual adapted to address conditions and constraints identified during the justification (see IEC 61508 [10]), may be assessed against the following considerations, as applicable in the context of their possible impact on safety:

- Recommended guides for normal operation and maintenance, including proof testing, routine actions for testing and inspection, and surveillance.
- Recommended maintenance guides after fault detection and annunciation.
- Identification of and instructions for use of tools required for maintenance.
- Guides and restrictions on firmware upgrades.
- Identification of expected skill levels or training of maintenance personnel.
- Identification of known CCFs and avoidance requirements.

- Identification of safety relevant maintenance issues.
- Identification of known lifetime limiting components and hardware service or qualified life, including, for example, battery replacement or re-flash requirements.
- Consideration of the future need to replicate any customization or modification required (whether by the manufacturer prior to shipment or after receipt), including:
  - Identification of any user configured safety functions;
  - Identification of all required parameter settings that may impact safety;
  - Identification of the achievable system class, if known;
  - Identification of any other constraints under which defined operation can be expected.

Supplementary user documentation for the component needs to be prepared to address any deficiencies identified above. This documentation may be incorporated into justification reports, a user or operating manual, training or maintenance manual or other project documentation, as appropriate.

5. MAINTENANCE OF JUSTIFICATION

5.1. OVERVIEW

Before starting a justification, the configuration of the COTS device needs to be captured by identifying make, model, software and hardware version (see Ref. [23]) and BOM. The justification is specific for the COTS device and cannot be extended to any successive version without an impact assessment, which may require additional activities depending on the nature and extent of the change.

Once a device has been successfully justified, care must be taken to maintain the integrity and validity of that justification with respect to the future items that are procured and installed in the same end use applications. Changes to the hardware, software or manufacturing process all have the potential to invalidate the previous justification and require additional actions to re-establish it. The following sections contain recommended practices and suggestions for maintaining the integrity of the justification.

5.2. CHANGE AND DEFECT REPORTING

To ensure awareness of all potentially significant safety concerns, it is important that the end user of a COTS device be notified of any defects or changes. 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 the notification to the end user.

5.2.1. Item certification maintenance

When a certification (e.g. IEC 61508 [10] SIL) is part of the basis for the justification, maintaining the certification becomes an effective motivation for manufacturers to notify the assessor (or certifier) of issues and changes to the design. This can be particularly helpful when making additional purchases of that item at a later point in time.

Certified COTS devices may possess certificates with time limited validity. At the end of the validity period, the third party certifier re-evaluates the certificate. Changes to COTS devices or their components that impact device certification are to be analysed and assessed. If the effects of the changes are minor then the certification may be sustained, but changes will still need to be identified to the end user. For example, a minor change could be a circuit board layout modification without any effects on the component. The modifications need to be evaluated with respect to the components' function and interfaces. The accumulation of many minor changes on the same part

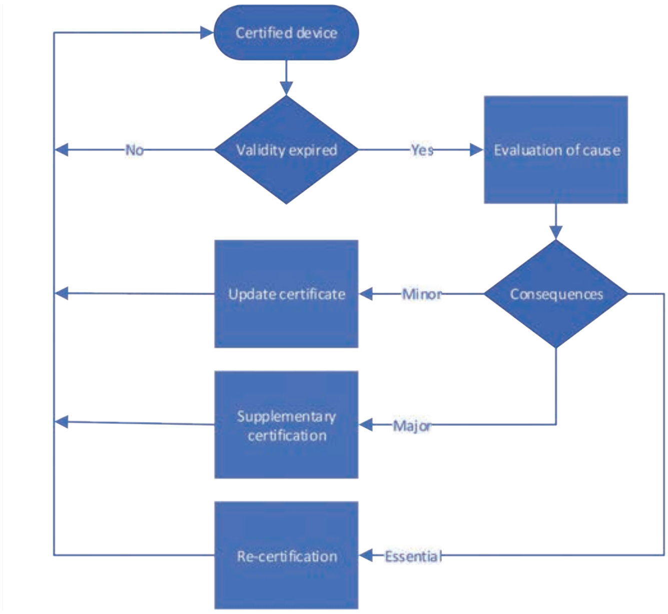


FIG. 5. Typical process for maintaining the certification status.

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 need to result in a supplementary certification being initiated. Essential changes to hardware or software design criteria or properties, or a new processing unit, will probably result in the need for a new certification. Figure 5 illustrates a typical process for maintaining the certification status.

There might be other reasons to reassess the COTS device certification, such as changes in manufacturer or supplier competence affecting 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.

There could be an agreement between the third party certifier and the COTS device manufacturer to maintain the validity of the certification. The agreement could cover, for example, yearly inspections of the development documentation and the manufacturing facility. During the inspection, the COTS device manufacturer could identify planned changes and/or already performed ones. The third party certifier and the COTS device manufacturer could clarify the effects of the changes and agree on the documents to be provided to evaluate them. In principle, it is the obligation and responsibility of the certificate owner to inform the certification body about any changes to the certified COTS device. A third party certifier could survey the standards and regulations and inform the certificate owner of any changes.

This relationship between the certificate owner and certifier can facilitate a dependable reporting mechanism for the assessor to also be notified of changes made to the COTS device.

5.2.2. Regulatory defect reporting responsibility

Some regulatory frameworks require suppliers of nuclear grade items (e.g. basic components as defined by Reporting of Defects and Noncompliance, US Title 10 CFR Part 21 [48]) to report the identification of defects that have the potential to cause significant safety concerns. It is essential to communicate to 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 audit to share that new defect information. It is best to not 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 (i.e. the dedicator). It is best to arrange for the manufacturer to notify the assessor (i.e. dedicator) of all defects and design changes.

When working with manufacturers to set up such contractual agreements and processes, one line of communication that includes the reporting of defects and design changes is sufficient. Also, note that even when such agreements are established, periodic questioning of the manufacturer to request updates on defects and design changes is recommended. Since the nuclear market is often a small percentage of a manufacturer's business, notification is not always among their top priorities.

5.3. PERIODIC QUALITY ASSURANCE MEASURES

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

5.4. SECURITY MANAGEMENT

It is recommended that the end user and assessor maintain an awareness of the identification, assessment and management of new security vulnerabilities and threats related to the basis of the justification of the COTS device. These issues will also be within the scope of notifications from manufacturers as discussed in Section 5.2. The identification of new vulnerabilities and threats is expected to occur. A methodology for evaluating and responding to them will be planned in advance.

5.5. CONFIGURATION MANAGEMENT

The assessor tracks the software and hardware versions that have been justified. Newly manufactured items must be traceable back to the original configuration. Typically, efforts are made to encourage manufacturers to maintain the previously justified versions (unless defects are identified), but changes are expected. A methodology for evaluating the changes will be established. A common driver of change is obsolescence of subcomponents, and periodic communication with the manufacturer can be helpful to anticipate such issues.

It is common for manufacturers to identify multiple subcomponents as acceptable for use within their hardware designs and include all those subcomponents in their BOM. The environmental conditions of the end use application, targeted by the justification, may impose tighter requirements on the BOM than what the manufacturer originally considered. Radiation exposure is a common aspect that can result in such tighter requirements since semiconductor based devices can be broadly considered suitable for exposure levels of 10 Gy (total integrated dose) while many end use applications are expected to include exposure levels of 100 Gy. For these scenarios, qualification testing may need to include the multiple hardware variations, or tighter BOM controls must be arranged with the manufacturer.

5.5.1. Changes to hardware

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 disciplined with configuration management and change reporting, then it may be relied on 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. Changes can be thought of as either change of design (e.g. different solution to deliver the same function) or change of components (maintaining the same design). The impact assessment of the latter might be easier.

When evaluating hardware changes there are four types to consider:

(1) *Original/equivalent:* The manufacturer of the hardware component lists original/equivalent component parts in the BOM. The works inspector[24] verifies the suitability of the component part in the context of the quality management system of the manufacturer. The validation of the original/equivalent component part with respect to the intended use is conducted in the type testing process of the hardware component.

(2) *Same type as original/equivalent but different component part manufacturer:* The works inspector verifies and validates the suitability of the component part in the context of the quality management system. It is confirmed by the hardware component certificate. The type testing organization has to be informed of the use of the component part.

(3) *Different type of component part with equivalent properties:* The type identifier can deviate from the BOM of the original/equivalent. However, the technical data of the component part are equivalent to the original or equivalent component part, in particular with respect to the following criteria:

- Electrical data;
- Geometry;
- Functional principle;
- Structure/technology;
- Material;
- Response behaviour;
- Newly added functionality, such as new interrupts, different speeds, etc.

The use of component parts that fit into this type of hardware change do not yield effects on the technical data and properties of the device. The works inspector verifies and validates the suitability of the component part in the context of the quality management system. It is confirmed by the hardware component certificate. The type testing organization must be informed about the validation process for the suitability of the component part.

(4) *Different type of component part with different properties:* The type identifier and the technical data of the component differ from the BOM. The works inspector verifies the suitability of the component part in the context of the quality management system. It is confirmed by the hardware component certificate. Validating the suitability of the component part with respect to the intended use is conducted as type testing or supplementary type testing of the device.

These four types are based on the German nuclear guideline KTA 3507 [49], which provides a classification of changes of hardware components in manufacturing and the resulting test activities. According to the type, different measures (e.g. supplementary type testing) may be required to re-validate the justification.

5.5.2. Changes to software

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 is initiated. Software changes usually require reworking 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.

For example, the software version number can sometimes be a helpful indicator into the extent of the change. The standard software version numbering scheme is formatted as ‘111.222.333’. A change to the ‘111’ portion signifies a major change, and a change to the ‘222’ portion signifies a minor change. The ‘333’ typically is just a build version tracking the iterations of code compiling while implementing the change. When a major change is indicated, the impact assessment can conclude that some additional work will be needed to re-establish the justification of the COTS device. If a minor change is indicated, then the potential exists that the original justification could still be valid and more information is needed to further investigate the extent of the change.

[24] The works inspector is an expert authorized by the manufacturer and who is independent of the fabrication in the manufacturing plant.

Major changes (i.e. changes to the ‘111’ portion of the software version numbering scheme) are understood to have no boundary on the extent of the change. Typically, major changes include the addition of new features and functions or even complete restructuring of the entire code. It is normally assumed that major changes will result in significant rework of the justification.

Minor changes (i.e. to the ‘222’ portion of the software version numbering scheme) are usually modifications of existing code. They are not expected to include complete deletions or additions of entire code sections (e.g. subroutines, modules). A few factors can be considered to determine the impact of this type of change on the existing justification. These factors include, but are not limited to, the following:

- What was the issue with the previous version that this modification intends to correct?
- Can it be clearly shown that the modification does not impact the device’s ability to perform its safety function?
- Does the change significantly impact the output of the compiler? Does the compiler optimize the code in a significantly different manner because of the modification?
- What regression testing did the manufacturer perform on the new version?
- What additional V&V work was undertaken?

The answers to these types of questions are used to determine if the validity of the justification has remained intact or if some re-evaluations are needed.

A different build (i.e. affecting the ‘333’ portion of the software version numbering scheme) of the same software version is not typically released, but if it is, it will be evaluated in the same manner as that for a minor change (i.e. to ‘222’ portion of the software version numbering scheme).

5.6. COMMERCIAL OFF THE SHELF DEVICE JUSTIFICATION MAINTENANCE

When any of these recommended practices and/or suggestions identify a condition that may impact the integrity of the justification, steps need to be taken to evaluate it and re-perform any activities that are determined to be appropriate. Figure 6 illustrates what this process typically consists of.

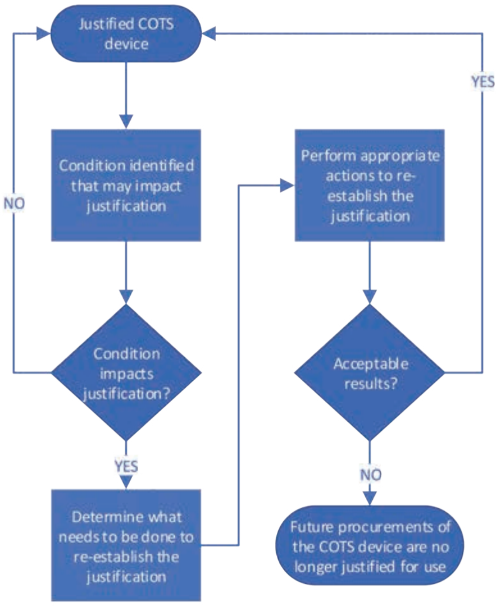

Justified COTS device
Condition identified that may impact justification
Condition impacts justification?
NO
YES
Determine what needs to be done to re-establish the justification
Perform appropriate actions to re-establish the justification
Acceptable results?
YES
NO
Future procurements of the COTS device are no longer justified for use

FIG. 6. Typical process for maintaining the justification.

6. REGULATORY ASPECTS

In order to provide suitable and independent regulatory oversight, the regulator needs to be independent of the justification process. In some Member States, however, the regulator may establish or endorse a specific method or set of methods to support a justification. As an example, in 1996 the US Nuclear Regulatory Commission endorsed EPRI TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants [50]. In other Member States, the approach is less prescriptive and the regulator sets the expectations for risk management; it is up to the licensee to develop a suitable design and justification process. As another example, in the UK, the Office for Nuclear Regulation has published expectations for the justification process (e.g. see guidance for inspectors provided in Technical Assessment Guide — Computer Based Safety Systems, NS-TAST-GD-046 [51]) and the licensees have developed approaches to meet these expectations.

Considering the significant differences in the regulatory context and specific practices in different countries, this section is not intended to provide an exhaustive list of items of regulatory interest in the digital COTS device justification, but mainly to outline common expectations and challenges identified during the review of digital COTS justifications. More detailed examples of the regulatory frameworks are provided in the country specific annexes of this publication.

Some common positions regarding the expectations of regulators on digital COTS are identified in Ref. [21]. However, because of the differences in regulatory framework and expectations between Member States, the justifications for the same application may need to be adapted from State to State. Generally, the regulator will expect the justification to demonstrate a level of quality/reliability/performance as a device developed using guidance and standards specific to the nuclear industry.[25]

Although the regulators' primary concern is the adequate quality, reliability and performance of COTS devices, their primary method for ensuring this is a review of the COTS devices' justification is to establish that:

- The licensees have in place a process for justification of COTS devices that meets the particular requirements or expectations of the Member State;
- The licensees are using the process appropriately;
- The process is not resulting in a deficient COTS device being used in an NPP.

The final responsibility for the justification of a COTS device for a nuclear power plant application is on the end user, who is usually the operator of the NPP who holds the licence (i.e. the licensee). While the justification requires the involvement of the device manufacturer and may involve other specialists (e.g. for software analysis or testing), the adequacy of the design needs to be determined by the assessor(s) and owned by the licensee. For this purpose, the licensee needs to implement a justification process as an intelligent customer even when external assessors are used in part of the process (e.g. assessment in Section 4.5). The overall justification is expected to show a level of independence from the manufacturer (see Refs [21] and [23]). This is primarily aimed at ensuring that the final decision on the suitability of the digital COTS device is sufficiently independent from the manufacturer's commercial interests (see Ref. [23]).

In evaluating the adequacy of a digital COTS device justification, the regulator may request access to the same level of detail associated with the justification as the assessor, so that the depth and applicability of the assessor's reviews can be validated. Although in most cases the regulator will not evaluate every part of the assessment process, it would be typical for the regulator to sample or audit the assessment process and, to do this effectively, the information may need to be made available. Depending on the situation, external contractors may support the regulator in this assessment. For this purpose, a suitable non-disclosure agreement may need to be discussed with the manufacturer to allow the regulator and any technical support contractor access to the same information made available to the assessors. The licensee has to be cognisant of this when initially engaging with the manufacturer.

[25] In some States, a similar justification exercise is also expected for devices developed to nuclear standards (although the justification may be less onerous in this case because of the claim of conformance with nuclear standards and the evidence already available).

A common regulatory concern is the lack of understanding of the importance of documenting what evidence is provided by previous evaluations, the limitations associated with those and how this evidence is created in the justification. In developing the suitability assessment for integrating the device justification into the overall I&C safety justification (Section 3.1.3.1), the assessor or licensee will need to verify whether the claims made on the device are supported by the justification and complemented with additional activities, where necessary. The regulator needs to be able to effectively understand how the body of evidence demonstrates that all requirements are satisfied. The level of detail (or depth of the justification) is also important. A common shortfall identified by regulators in assessing justifications is in recording the assessor's engineering judgement. The assessor is expected to provide an adequate level of information to be able to come to a reasoned conclusion. In some cases, the justifications point to evidence without providing the reasoning as to how this evidence is suitable to support a certain judgement.

Because COTS devices are generally not developed to nuclear standards, it is likely that quite a number of gaps will be initially identified, which then need to be justified. The regulator will usually focus on the identification of failure modes of the device and on the safe failure modes, where appropriate (Section 3.1.3).

One of the most challenging regulatory aspects is determining whether the COTS device is suitable for the target application. There is often an interpretation that, when a device has been justified, it is suitable for any application. However, this is generally not the case because of the limitations of the existing justification (e.g. functions not justified — see Section 3.1.1) and/or the specific aspects of the application (e.g. effect of failures on the plant — see Section 3.1.3).

Lastly, there is an expectation that the depth of the justification is commensurate with the safety classification of the device as it is intended to be used (see discussion in Section 3.2.3). While the practice of justification for higher safety class as per SSG-30 [11] (Class 1) and lower safety class (Class 3) is generally understood, the justification of the intermediate level (e.g. Class 2) is typically more challenging and may depend on the application. Applying a graded approach to the justification process needs to consider the item's importance to safety and other factors specific to the item being used in the NPP. Depending on the gaps associated with a particular COTS device, a number of factors can be considered in determining the extent of grading that needs to be applied, including how important malfunction or failure of the COTS device is to plant safety, the complexity or uniqueness of the device, the degree to which functional compliance can be demonstrated by inspection and testing, and the operational history and degree of standardization of the device. This last part is of particular concern to the regulator (even when the process is not graded or is graded at the highest level) as manufacturers' claims of standardization of digital COTS devices and extremely low failure rates in operational history (e.g. proven in use arguments) have frequently been overstated and are difficult to substantiate.

7. SUMMARY

Digital COTS components are increasingly being used in NPPs, as they provide several advantages compared with bespoke devices developed to nuclear standards (e.g. cost, time to market, operational experience) and because of obsolescence issues with their analogue counterparts. However, the justification of their use in nuclear safety applications can be challenging owing 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 from the manufacturer (e.g. development processes and design documentation).

The aim of this publication is to guide Member States in developing or improving their justification process for digital COTS devices of limited functionality for nuclear application. The proposed framework builds on the current practices of several Member States (some of which are presented in the annexes) by describing some of the challenges with justifying digital COTS devices and suggesting an approach and a process to implement it.

This publication identifies typical challenges associated with the use of digital COTS devices in nuclear applications, outlining the specific vulnerabilities and problems generally identified when justifying their application in NPPs.

Although the justification for the use of a digital COTS device needs to consider the specific application in an NPP, this publication presents an approach for developing a generic device justification of the device, and explains the additional steps needed to evaluate its suitability for each target application. This approach is considered efficient as it allows the reuse of a significant number of the justification activities for several applications.

The proposed strategy consists of three phases:

(1) The definition of the justification envelope, which identifies the requirements for the assessment and any restrictions of use or assumptions that limit the justification;
(2) The assessment itself, which evaluates the suitability of the device and its design and development processes;
(3) The integration of the justification into the overall I&C architecture for the specific application.

While the integration phase is very much dependent on the application and the country specific practices, and is hence not covered in detail in this publication, the first two phases are expanded, outlining a device justification process that consists of the following typical steps:

(1) Defining requirements and prerequisites;
(2) Selecting candidate devices;
(3) Obtaining manufacturer information and support;
(4) Planning;
(5) Assessing;
(6) Identifying lifetime issues;
(7) Preparing the justification documentation package.

The assessment considers the behavioural properties of the device, its possible vulnerabilities and lessons captured in relevant standards. It also includes activities that are performed independently of the manufacturer with the objective of evaluating the assessment activities performed by the manufacturer or confirming the suitability of the COTS device with additional analyses, where appropriate.

The publication provides examples of evidence that may be used to support a justification and technical competencies generally needed in the assessment. A graded approach based on the safety classification of the target application is also discussed, providing examples in the annexes of how this is reflected in the Member States' practices.

The publication also describes how to maintain a justification following modifications to the hardware or software versions of a device, ensuring that any supporting certificates continue to be current and any defects that have been identified have been taken into account.

Finally, the publication discusses regulatory expectations on digital COTS devices and how to ensure that they are of adequate quality, reliability and performance through a review of the justification process.

Appendix I

SPECIFIC ASPECTS OF CERTIFICATION

I.1. USE OF CERTIFICATION

I.1.1. Overview

Many COTS devices developed for safety market applications are certified as meeting IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems (several parts) [10]. Certifications are typically performed by an independent accredited certification body. In general, this standard is not referenced directly as a nuclear design standard. However, it is widely used and well accepted as a product manufacturing standard for programmable electronic systems or equipment used in a functional safety context in many industries. Many I&C products are available today that have been certified to this standard by authorized independent safety assessors. This standard is also intended to be the 'parent' or 'umbrella' standard for the family of nuclear I&C standards in Ref. [6] and provides comprehensive and detailed guidance. For this reason, it is a valuable reference used in the nuclear industry and is recognized by most nuclear regulators. It is used both to assist in interpreting the requirements of the family of nuclear I&C standards in Ref. [6] and as a procurement standard.

In general, certified COTS devices meeting the requirements in IEC 61508 [10] are usually appropriate for use in applications performing IEC 61226 [13] functions respectively (i.e. they may usually be successfully qualified, provided they can be shown to meet the functional safety suitability requirements of a given application). Products that have a generic pre-qualification still require application specific justification to ensure they meet the application requirements. For example, there are often limitations or conditions on a safety certificate that may not be acceptable for the intended use. However, it will usually be much easier to complete a justification with a SIL certified product.

Third party certificates could represent a useful part of the justification if the whole body of documentation developed to support the decision is made available to the end user and the assessor.

It is recognized that the relevance of the certification in the context of the COTS justification can be influenced by the standard against which the analysis is carried out (e.g. IEC 61508 [10] or nuclear standards) and by the contractual arrangements (e.g. scope of the certification requested and independence from the manufacturer/supplier).

Depending on the regulatory practice, the certification may not be accepted instead of the COTS justification (although they may be used as part of the justification) (see Ref. [21]).

I.1.2. Standardization and accreditation aspects

According to Conformity Assessment — Vocabulary and General Principles, EN ISO/IEC 17000:2004 [52], certification[26] is the third party attestation related to products, processes, systems or persons. The third party could apply the certification to different objects such as:

- Corporate quality system certifications;
- Product safety certifications;
- Hardware test standards compliance;
- Software development process certifications.

[26] Certification according to EN ISO/IEC 17000:2004 [52] differs from the definition provided in the IAEA Safety Glossary [15]. In Ref. [15] certification is related to the regulatory body.

Conformity assessment aims to demonstrate the fulfilment of a set of specified requirements. The requirements are usually taken from standards but could also be specified by the manufacturer/supplier, for example specific characteristics of the COTS device. The conformity assessment process is organized in three main stages:

(1) Selection;
(2) Determination;
(3) Review and attestation.

The selection activity comprises the planning of the conformity assessment activities according to the rules of the corresponding certification programme. The result of the first stage is documented in the conformity assessment plan. This plan defines the input needed for assessment and describes the assessment activities, including the schedule. Typical input could be development process descriptions, quality assurance records, development documents, V&V documentation and a test item of the COTS device. The assessment itself is part of the 'determination' stage. Within this stage, the COTS device is assessed to determine evidence proving conformance with the specified requirements. The assessment is often supported by audits at the manufacturer/supplier. Before attesting the object (i.e. deciding whether or not the COTS device has passed the conformity assessment) a review is conducted. The stage 3 review verifies the completeness, correctness and consistency of the activities and results of stages 1 and 2 with respect to the certification program. An expert who has not been involved in the activities of stages 1 and 2 carries out the stage 3 review. Based on the review result, the expert recommends (or not) the issue/reissue of the certificate.

Pursuant to ISO/IEC 17067 [26], product certification is the provision of assessment and impartial third party attestation that fulfilment of specified requirements has been demonstrated. Product certification is carried out by product certification bodies, which would conform to ISO/IEC 17065 [25]. Specified requirements for products are generally contained in standards or other normative documents. Product certification is an established conformity assessment activity that provides confidence to consumers, regulators, industry and other interested parties that products conform to specified requirements, including, for example, product performance, safety, interoperability and sustainability.

National accreditation bodies can grant the authorization or accreditation of the third party certifier as an essential means of providing evidence of the competency of conformity assessment organizations. Within the European Union, national accreditation bodies are legally responsible for the accreditation of conformity assessment bodies (laboratories, inspection and certification bodies). The accreditation bodies assess and monitor the conformity assessment bodies (e.g. by regular audits) in order to demonstrate their competence, impartiality and performance capability.

The application for certification has to be accompanied by documents stating clearly the type and scope of the certification to be carried out. Such documents include, for example, process/product descriptions and indication of the safety class to be achieved. Based on the documents, the certification body checks whether the certification can be performed with regard to the scope of the requested certification and prepares the quotation for the evaluation and certification activities. All expenses for the evaluation and certification will be invoiced to the manufacturer in accordance with the quotation. All information received from the client as a result of the application will be treated confidentially.

Usually the initial inspection of a product is carried out in the test laboratory or inspection body of the certification body. After assessing the submitted documents, the certification body may request the test object(s) from the client or agree to carry out tests in the customer/manufacturer's laboratory. The customer/manufacturer must adapt, prepare or supplement the test sample(s) at the request of the certification body in such a way that the necessary tests can be carried out.

If the certificate holder agrees, the certificates are published. The certificates are published in a database managed by the certification body. The certification body will withdraw the published certificate if it detects, for example, that information relevant for safety is wrong, leading to misinterpretation, or if the certificate is misused by the holder. The public is informed about this fact by the certificate status. The validity of the certificate can be limited and even surveilled. Surveillance activities could be triggered by complaints submitted by the certificate holder himself or by third parties to the certification body.

I.2. TYPES OF CERTIFICATIONS

I.2.1. Corporate quality system certifications

It is becoming common for major product suppliers to obtain industry quality management certifications (e.g. ISO 9001 [34] and Quality Assurance Programme, CSA Z299.2 [53]. This method involves obtaining evidence of appropriate certifications. The vendor must be able to demonstrate that the certification is current and applies to the programmable electronic system product being qualified.

I.2.2. Product safety certifications

COTS device safety certifications (e.g. third party certification to IEC 61508 [10] from a recognized organization like TÜV) are recognized third party assessments of product compliance to an appropriate safety standard, a form of generic justification.

The vendor must be able to demonstrate that the certification is current and applies to both the hardware and software versions of the COTS device being qualified. Product safety certifications come with a ‘safety (assessment) report’ that contains the assessment results and can be reviewed in detail. The safety report may be useful in identifying the device’s safety or fail-safe features, as well as its failure modes, known product limitations or weaknesses. However, the product safety certification typically covers only the failure modes and effects internal to the COTS device. For a proper product safety justification in a given context, the failures or hazards associated with the specific configuration of the COTS device, including both hardware and software, would be carefully reviewed to determine the impact of failures on the plant system and safety functions.

Product safety certifications, though useful, are not equivalent to application specific product justifications. It cannot be assumed that a COTS device certified to an appropriate SIL will be suitable to a given system class. Products designed and certified for Class 1 applications are designed with ‘enforced simplicity’ to ensure that their design and functional behaviour can be easily understood and systematically verified. A product with a SIL 3 certification may not be suitable if the intended application is outside of the safety envelope defined by the safety manual (e.g. reliance on a communications link might not be certified) yet might be required for the application.

The safety report will identify strict limitations or a range of configurations for which the COTS device is certified. In order to justify the COTS device, the certification report is reviewed in detail to determine the bounds of application. Any/all limitations, exclusions or constraints are identified for use of the COTS device. Some considerations for the justification of the device include the following questions:

- What was the extent of the certification and does it apply to the proposed application and the intended configuration, hardware and software? Do any of the safety certification’s limitations, exclusions or constraints apply and what is their impact? Hardware test reports should be reviewed to verify that testing conformed to all the requirements of the applicable test standard and that acceptance criteria are applicable in the system context.
- Does the actual COTS device supplied meet the certification specifications in terms of version of hardware and/or firmware for all components/modules supplied, and is the vendor guaranteeing the version shipped fully meets the original certification? Has the COTS device design been ‘frozen’ by the vendor or has the design changed since the certification was issued? What is the impact of the change?
- If the application of the COTS device is known to be outside of the bounds of the certification, is it possible for the vendor to take additional steps to validate these exceptions (e.g. an uncertified version of a module could be certified, an unapproved function block could be verified)?
- Is the COTS device to be used outside of its certified operating limits? Is additional testing required to confirm qualification (e.g. vibration, temperature, humidity, seismic)? This may not be advisable if it is likely the vendor may substitute parts in future orders of the COTS device that may not meet the exceeded test specifications. In such cases, the constraint to repeat the additional testing if replacement units are procured in future needs to be documented.

Third party certifications and approvals usually come with an appropriate assessment report, in addition to the safety report. It is recommended to obtain and review the assessment report. The effectiveness of the methods and tools used for the certification would be justified.

Additional guidance on the use of third party certifications may be found in IEC 61513 [6], clause 6.4.1.3, and IEC 62138 [8], clause 6.2.2.4.

I.2.3. Equipment qualification

There are numerous standards for hardware certifications and approvals, especially in the areas of EMI immunity and environmental and seismic resistance.

As part of hardware qualification, the assessment of functional characteristics has to be reviewed — such as EMI immunity and resistance to environmental and seismic disturbances (see IEC 60780 [41] and IEEE-323 [42] for further guidance).

Testing is the preferred method to demonstrate qualification, although other methods based on analysis may be acceptable. Test and analysis reports supporting hardware certifications need to be reviewed carefully and their suitability as part of the application specific qualification confirmed.

I.2.4. Software development process certifications

This method focuses on taking credit for software development process quality assurance certifications. This method may be used to supplement or replace all or parts of the software development process assessment. Several recognized software process assessment frameworks exist, as well as guides and standards that address specific aspects of the software development process. This guide recognizes credible third party assessments and certifications done in compliance with IEC 61513 [6] and IEC 60880 [7] or IEC 62138 [8], as well as any of the following (as appropriate to the class as specified):

— IEEE 828 [54] (Class 2 or 3);
— IEEE 830 [55] (appropriate for Class 2 or 3);
— IEEE 1012-2016 [22] (Class 2 or 3);
— IEEE 7-4.3.2 [5] (appropriate for Class 1);
— ISO 90003:2018 [56] (appropriate for Class 3 when used in conjunction with an ISO 9001 software);
— ISO/IEC 12207 [57] (Class 2 or 3);
— ISO/IEC 25041 [58] (appropriate for Class 2 or 3);
— ISO/IEC 25010 [59] (appropriate for Class 2 or 3);
— Any other recognized and industry accepted standard or assessment guide/methodology that can be shown to be reasonably equivalent to one of the above.

Most of the guides and standards listed above are not intended for the development of software important to safety and therefore do not require the identification, verification, traceability and validation of software safety requirements throughout the development process. Careful consideration of this deficiency is to be taken into account. Additional compensating evidence may be deemed necessary, particularly for Class 1 and 2 applications.

Note further that IEEE 1012-2016 [22] also uses the SIL concept referring to ‘software integrity level,’ but a device may have a different SIL using the criteria in IEEE 1012-2016 [22] instead of IEC 61508 [10]. Care has to be taken with using both IEC 61508 [10] and IEEE 1012-2016 [22] in the same justification because of this concern.

Appendix II

FAILURE ANALYSIS TOOLS AND TECHNIQUES

This appendix serves as a reference to available failure analysis tools and techniques that can be used during the design process to define design requirements associated with defensive measures and diagnostics, to identify hazards and failure mechanisms that could lead to failure of the performance of a safety function and to prevent unintended functions. With digital COTS, the design information may be limited or unavailable. To compensate for this gap, a failure analysis can be used to identify failure mechanisms that could lead to a loss of the device's ability to perform its safety function. A set of critical characteristics need to be developed to address these identified failure mechanisms and how they should be resolved using a verification method.

Failure analysis can be performed qualitatively and/or quantitatively. Quantitative approaches have been used to determine hardware failure rates for years based on calculated subcomponent failure rates and/or using in situ performance failure rate data. With the introduction of software into digital equipment, the quantitative calculation of failure rates has become difficult or impossible to determine owing to the potential of hidden systematic software flaws that, if triggered, could result in system failure.

The following section contains key documents defining methods and techniques that can be used to identify failure mechanisms of digital devices used in a safety related application. There is no preferred method selected by this standard because the benefits are normally specific to the application based on system architecture and level of complexity.

Reference [20] provides guidance for assessing the dependability of software based components and systems and presents several failure analysis techniques that are commonly used in both the nuclear industry and other industries for safety critical systems. Reference [20], section 4.3, provides guidance on several techniques of functional validation:

- Modelling and simulation;
- Failure modes and effects analysis (FMEA);
- Functional FMEA;
- Design FMEA;
- Fault tree analysis (FTA) — additional information available in IEC 61025[27] [61];
- Hazards and operability analysis (HAZOP) — additional information available in IEC 61882 [62];
- System theoretic process analysis.

Additional techniques discussed in IEC 62671 [9], clause 6.7, include reliability, maintainability and testability, the use of both FMEDA and failure modes, effects and criticality analysis (FMECA) for systematic methods for determining hardware failure modes, their frequency and their impact.

In addition to the IAEA identified failure analysis techniques, the following failure analysis techniques are used throughout the nuclear and process industry in safety system development:

- FMEDA — IEC 62671 [9] endorses the use of FMEDA to provide a higher level of reliability by evaluating both failure mechanisms and the identification of these mechanisms through self-diagnostics. Software failure rates still have to be accessed using operational performance data to provide additional support for the hardware based numbers. Note that systematic failures/common cause software failures still have to be addressed qualitatively.
- FMECA — IEC 60812:2018 [63] says that a failure modes, effects and criticality analysis is an extension to the FMEA to include a means of ranking the severity of the failure modes to allow prioritization of countermeasures. This is done by combining the severity measure and frequency of occurrence to produce a metric called criticality. Procedures for Performing a Failure Mode, Effects and Criticality Analysis,

[27] Nuclear Power Plants — Instrumentation and Control Important to Safety — Hardware Design Requirements for Computer-Based Systems, IEC 60987:2007+AMD1:2013 CSV [60] endorses the use of FTA and FMEA.

MIL-STD-1629A [64] establishes requirements and procedures for performing an FMECA to systematically evaluate and document, by item failure mode analysis, the potential impact of each functional or hardware failure on mission success, personnel and system safety, system performance, maintainability and maintenance requirements. Each potential failure is ranked by the severity of its effect in order that appropriate corrective actions may be taken to eliminate or control the high risk items.

II.1. APPLYING TECHNIQUES

II.1.1. Which technique to use?

As noted above, there are various techniques that can be used to perform failure analysis. Some techniques are better than others for identifying potential vulnerabilities. Selection of the technique(s) needs to be based on the COTS device and application along with the available expertise in performing these analyses.

EPRI Report 3002000509, Hazard Analysis Methods for Digital Instrumentation and Control Systems [17], is a guideline that provides comprehensive, practical, cost effective methods for identifying hazards in digital systems before the systems are put into operation. This EPRI report also provides guidance on the weaknesses and strengths of different techniques and closely aligns with the techniques described in Ref. [20].

The following methods are evaluated in that EPRI report [17]:

- Functional failure modes and effect analysis;
- Design failure modes and effect analysis;
- Top down method using FTA;
- HAZOP method;
- Systems theoretic process analysis method;
- Purpose graph analysis method.

The objectives of the EPRI report, as stated in its section 1.2, are as follows:

“— Evaluate the capability of each method for identifying potential vulnerabilities in a digital I&C system, including hazardous interactions with plant components and plant systems;
— Demonstrate the workability of each method on practical examples based on experiences reported by EPRI members;
— Provide a step-by-step procedure for each method so that users can adapt them into a procedure format;
— Provide worked examples to demonstrate each method in a step-by-step manner;
— Use the results to identify the comparative strengths and limitations of each method;
— Provide guidance on how to blend multiple methods to gain efficiencies in the analysis, limit the analytical effort, or limit corrective actions such as design changes or the application of administrative controls to the identified hazards.”

For IEC 61508 [10] SIL certification, the FMEDA technique is widely used.

II.1.2. Bounding the analysis

When a failure analysis is performed, the boundaries need to be defined to ensure adequate coverage of critical system specific application interfaces such as power, inputs and outputs and operator interfaces.

II.1.3. Combination of techniques

The user is not limited to using a single technique but can use multiple techniques based on whatever works better or more effectively for a particular area. An example of this is using ‘bottom up’ and ‘top down’ techniques such as an FMEA (bottom up approach) to identify critical failure areas followed up with an FTA (top down approach) to identify cut sets of potential failure mechanisms that need to be evaluated.

II.1.4. Integration of failure analysis into the design and development process

To provide direction on how failure analysis is integrated into the design and development process, the following are some examples from existing industry processes:

- In IEEE 1012-2016 [22] for V&V, hazards analysis is used throughout the different phases of the lifecycle process.
- In the IEC 61508 [10] SIL certification process, the FMEDA technique is used to quantify hardware failure probabilities and address needed diagnostics for identified faults.
- In the US commercial grade dedication process (see EPRI 3002002982 [65]), FMEAs are used to define critical characteristics.
- In IEEE 7-4.3.2 [5], qualification of COTS devices for use in safety related applications require the performance of a supporting hazard analysis.

II.2. ADDRESSING COMMON CAUSE FAILURE

This section identifies methods on how to address systematic failures or CCFs. The IAEA definition for CCF in the IAEA Safety Glossary [15] is: "*common cause failure*. *Failures* of two or more *structures, systems or components* due to a single specific *event* or cause."

An additional definition in IEEE 603 [5] is: "Common cause failure (CCF) — Loss of function to multiple structures, systems, or components due to a shared root cause."

With respect to addressing CCF, IEC 60880 [8] and IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems, IEEE 379 [66] provide direction for safety related systems, such that CCF has to be assessed for susceptibility and if there is a susceptibility identified, the effects of the CCF have to be addressed at the system level.

Another approach for addressing CCF is the implementation of diversity. For additional information, see Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, NUREG/CR-6303 [67].

Additional documents that address systematic or common cause failures in digital systems include the following:

- IEC 62340 [1], Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Requirements for Coping with Common Cause Failure (CCF), provides principles and requirements for overcoming CCF.
- The abstract of EPRI Report 3002005326, Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems [68], states:

  "This report provides practical guidance that will help utility engineers, equipment suppliers, and system integrators address a full range of potential digital failure and CCF contexts. It includes steps for identifying and qualitatively assessing susceptibilities in terms of their likelihood, failure effects, and the measures in place to protect against them. The report also includes guidance on using susceptibility and coping analyses to screen and prioritize potential vulnerabilities. The guidance also includes the application of risk insights."

- IEC 61508-5, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems [69], provides direction for systematic failure or CCFs not by quantification of a probability but by the reduction of these risks.

— IEEE 379, IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems [66], states:

> “The requirement for a safety system to function in the presence of common-cause failures (CCFs) is beyond the scope of the application of single-failure criterion and, therefore, this standard. However, it is important to screen out the potential CCFs when performing a single-failure analysis. As part of evaluating the overall reliability of safety systems, IEEE Std 352 extends the qualitative analysis beyond that which is done for failure modes and effects analysis (FMEA), or fault tree analysis, by considering CCFs. Therefore, an extended qualitative analysis described in IEEE Std 352 should be used to identify and screen out common-cause failure mechanisms not normally considered in an analysis of independent component failures.”

— IEC 60880, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Software Aspects for Computer-Based Systems Performing Category A Functions [7], states:

> “This standard provides requirements for the purpose of achieving highly reliable software. It addresses each stage of software generation and documentation, including requirements specification, design, implementation, verification, validation and operation. The principles applied in developing these requirements include:
>
> - Best available practices;
> - Top-down design methods;
> - Modularity;
> - Verification of each phase;
> - Clear documentation;
> - Auditable documents;
> - Validation testing.”

Depending on the regulatory context in which a particular digital device is implemented, the exact definition and the implications of the definition need to be considered. For example, in some Member States, cascading failures (failures of several systems due to a single specific support system) are not considered CCFs but rather are considered as single failures.

REFERENCES

[1] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Requirements for Coping with Common Cause Failure (CCF), IEC 62340, IEC, Geneva (2007).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).

[3] NUCLEAR REGULATORY COMMISSION, Dedication of Commercial-Grade Items for Use in Nuclear Power Plants, Regulatory Guide 1.164, US NRC, Washington, DC (2017).

[4] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE 603, IEEE, New York (2018).

[5] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations, IEEE 7-4.3.2-2016, IEEE, New York (2016).

[6] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — General Requirements for Systems, IEC 61513, IEC, Geneva (2011).

[7] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Software Aspects for Computer-Based Systems Performing Category A Functions, IEC 60880, IEC, Geneva (2006).

[8] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Software Aspects for Computer-Based Systems Performing Category B or C Functions, IEC 62138, IEC, Geneva (2018).

[9] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Selection and Use of Industrial Digital Devices of Limited Functionality, IEC 62671, IEC, Geneva (2013).

[10] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, IEC 61508, IEC, Geneva (2010).

[11] 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).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Technical Challenges in the Application and Licensing of Digital Instrumentation and Control Systems in Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-1.13, IAEA, Vienna (2015).

[13] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation, Control and Electrical Power Systems Important to Safety — Categorization of Functions and Classification of Systems, IEC 61226, IEC, Geneva (2020).

[14] NUCLEAR REGULATORY COMMISSION, Embedded Digital Devices in Safety-Related Systems, RIS 2016-05, US NRC, Washington, DC (2016).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary, Terminology Used in Nuclear Safety and Radiation Protection, 2018 edn, IAEA, Vienna (2018).

[16] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems — Part 1: General Requirements, IEC 61508-1, IEC, Geneva (2010).

[17] ELECTRIC POWER RESEARCH INSTITUTE, Hazard Analysis Methods for Digital Instrumentation and Control Systems, Rep. 3002000509, EPRI, Palo Alto, CA (2013).

[18] ELECTRIC POWER RESEARCH INSTITUTE, Guideline on Prevention and Detection of Undeclared Digital Content, Rep. 3002008010, EPRI, Palo Alto, CA (2016).

[19] ELECTRIC POWER RESEARCH INSTITUTE, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, EPRI TR-106439, EPRI, Palo Alto, CA (1996).

[20] 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).

[21] MULTINATIONAL DESIGN EVALUATION PROGRAMME, Common Position on Selection and Use of Industrial Digital Devices of Limited Functionality, CP-DICWG-07, OECD/NEA, Paris (2014).

[22] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard for System, Software, and Hardware Verification and Validation, IEEE 1012-2016, IEEE, New York (2016).

[23] OFFICE FOR NUCLEAR REGULATION, Licensing of Safety Critical Software for Nuclear Reactors: Common Position of International Nuclear Regulators and Authorised Technical Support Organisations — Rev. 2018 (2018),
http://www.onr.org.uk/software.pdf

[24] MULTINATIONAL DESIGN EVALUATION PROGRAMME, Common Position on the Treatment of Common Cause Failure Caused by Software within Digital Safety Systems, CP-DICWG-01, OECD, Paris (2013).

[25] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION/INTERNATIONAL ELECTROTECHNICAL

COMMISSION, Conformity Assessment — Requirements for Bodies Certifying Products, Processes and Services, Standard 17065:2012, ISO/IEC, Geneva (2012).

[26] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION/INTERNATIONAL ELECTROTECHNICAL COMMISSION, Conformity Assessment — Fundamentals of Product Certification and Guidelines for Product Certification Schemes, Standard 17067:2013, ISO/IEC, Geneva (2013).

[27] ELECTRIC POWER RESEARCH INSTITUTE, Handbook for Evaluating Critical Digital Equipment and Systems, EPRI 1011710, EPRI, Palo Alto, CA (2005).

[28] ELECTRIC POWER RESEARCH INSTITUTE, Evaluating Commercial Digital Equipment for High-Integrity Applications, EPRI TR-107339, EPRI, Palo Alto, CA (1997).

[29] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

[30] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation Control and Electrical Power Systems — Cybersecurity Requirements, IEC 62645:2019, IEC, Geneva (2019).

[31] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems — Requirements for Coordinating Safety and Cybersecurity, IEC 62859, IEC, Geneva (2016).

[32] 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 (06/2017), VDI/VDE, Düsseldorf/Frankfurt am Main (2017).

[33] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Important to Safety — Development of HDL-Programmed Integrated Circuits for Systems Performing Category A Functions, IEC 62566, IEC, Geneva (2012).

[34] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Quality Management Systems — Requirements, ISO 9001:2015, ISO, Geneva (2015).

[35] NUCLEAR REGULATORY COMMISSION, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants, Appendix B to 10 CFR Part 50, US NRC, Washington, DC (2017).

[36] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Measuring Relays and Protection Equipment, IEC 60255, IEC, Geneva (2014).

[37] GUERRA, S., CHOZOS, N., SHERIDAN, D., Justifying Digital COTS Components when Compliance Cannot be Demonstrated — The Cogs Approach (Proc. 9th Int. Topical Mtg on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC&HMIT), Charlotte, NC, 2015), ANS, La Grange Park, IL (2015).

[38] NUCLEAR REGULATORY COMMISSION, Human-System Interface Design Review Guidelines, Rep. NUREG-0700 (Rev. 2), US NRC, Washington, DC (2002).

[39] NUCLEAR REGULATORY COMMISSION, Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems — Final Report, Rep. NUREG/CR-6463, US NRC, Washington, DC (1996).

[40] NUCLEAR REGULATORY COMMISSION, Highly-Integrated Control Rooms — Communications Issues (HICRc), Interim Staff Guidance DI&C-ISG-04, Rev. 1, US NRC, Washington, DC (2009).

[41] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Electrical Equipment of the Safety System — Qualification, IEC 60780, 2nd edn, IEC, Geneva (1998).

[42] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, IEEE 323-2003, IEEE, New York (2003).

[43] 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).

[44] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Electromagnetic Compatibility (EMC), Standard 61000 Series, IEC, Geneva (2002–2018).

[45] ELECTRIC POWER RESEARCH INSTITUTE, Guidelines for Electromagnetic Interference Testing in Power Plants, EPRI TR-102323, EPRI, Palo Alto, CA (1994).

[46] NUCLEAR REGULATORY COMMISSION, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems, Regulatory Guide 1.180, Rev. 1, US NRC, Washington, DC (2003).

[47] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, IEEE 344-2004, IEEE, New York (2004).

[48] NUCLEAR REGULATORY COMMISSION, Reporting of Defects and Noncompliance, 10 CFR Part 21, US NRC, Washington, DC (2015).

[49] 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).

[50] ELECTRIC POWER RESEARCH INSTITUTE, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, EPRI TR-107330, EPRI, Palo Alto, CA (1996).

[51] OFFICE FOR NUCLEAR REGULATION, Technical Assessment Guide — Computer Based Safety Systems, NS-TAST-GD-046 (Rev. 5), ONR, Liverpool (2019).

[52] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION/INTERNATIONAL ELECTROTECHNICAL COMMISSION, Conformity Assessment — Vocabulary and General Principles, Standard 17000:2004, ISO/IEC, Geneva (2004).

[53] THE CSA GROUP, Quality Assurance Programme, CSA Z299.2, CSA, Toronto, ON (2007).

[54] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard for Software Configuration Management Plans, IEEE 828, IEEE, New York (2012).

[55] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Recommended Practice for Software Requirements Specifications, IEEE 830, IEEE, New York (1998).

[56] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION/INTERNATIONAL ELECTROTECHNICAL COMMISSION, Software Engineering — Guidelines for the Application of ISO 9001:2015 to Computer Software, ISO/IEC 90003:2018, ISO, Geneva (2018).

[57] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION/INTERNATIONAL ELECTROTECHNICAL COMMISSION, Systems and Software Engineering — Software Life Cycle Processes, ISO/IEC 12207:2017, ISO, Geneva (2017).

[58] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION/INTERNATIONAL ELECTROTECHNICAL COMMISSION, Systems and Software Engineering — Systems and Software Quality Requirements and Evaluation (SQuaRE) — Evaluation Guide for Developers, Acquirers and Independent Evaluators, Standard 25041:2012, ISO/IEC, Geneva (2012).

[59] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION/INTERNATIONAL ELECTROTECHNICAL COMMISSION, Systems and Software Engineering — Systems and Software Quality Requirements and Evaluation (SQuaRE) — System and Software Quality Models, Standard 25010:2011, ISO/IEC, Geneva (2011).

[60] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Important to Safety — Hardware Design Requirements for Computer-Based Systems, IEC 60987:2007+AMD1:2013 CSV, IEC, Geneva (2013).

[61] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Fault Tree Analysis (FTA), IEC 61025, 2nd edn, IEC, Geneva (2006).

[62] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Hazard and Operability Studies (HAZOP Studies) — Application Guide, IEC 61882, IEC, Geneva (2016).

[63] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Failure Modes and Effects Analysis (FMEA and FMECA), IEC 60812:2018, 3rd edn, IEC, Geneva (2018).

[64] DEPARTMENT OF DEFENSE, Procedures for Performing a Failure Mode, Effects and Criticality Analysis, MIL-STD-1629A, DOD, Washington, DC (1980).

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

[66] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems, IEEE 379-2014, IEEE, New York (2014).

[67] NUCLEAR REGULATORY COMMISSION, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, NUREG/CR-6303, Office of Nuclear Regulatory Research, Washington, DC (1994).

[68] ELECTRIC POWER RESEARCH INSTITUTE, Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems, Rep. 3002005326, EPRI, Palo Alto, CA (2016).

[69] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems — Part 5: Examples of Methods for the Determination of Safety Integrity Levels, IEC 61508-5, IEC, Geneva (2010).

[70] INTERNATIONAL ATOMIC ENERGY AGENCY, Workforce Planning for New Nuclear Power Programmes, IAEA Nuclear Energy Series No. NG-T-3.10, IAEA, Vienna (2011).

Annex I

PRACTICE IN CANADA

I–1. REGULATORY ASPECTS

The Canadian Nuclear Safety Commission (CNSC) is responsible for regulating the use of nuclear energy and materials. The CNSC permits nuclear power utilities to operate nuclear power plants (NPPs) in Canada under a power reactor operating licence (PROL). A PROL specifies applicable standards for operation. Canadian nuclear power utilities are licensed in accordance with applicable standards in their PROL. The CNSC's licensing regime includes the licence conditions handbook (LCH), which is a companion piece to interpret a licence. The general purpose of the LCH is, for each licence condition, to clarify the regulatory requirements and other relevant parts of the licensing basis.

The LCH requires the licensee to ensure that the instrumentation and control (I&C) system is designed to satisfy requirements of the plant level system classification, ensure that system safety features for enhancing system reliability and integrity are identified and implemented in the design, and ensure that the system is not vulnerable to common cause failure (CCF). In particular, the LCH references CSA standard N290.14-07, Qualification of Pre-Developed Software for Use in Safety-Related Instrumentation and Control Applications in Nuclear Power Plants [I–1], for justification in using digital predevelopment software. This is the standard used by licensed utilities in Canada to qualify commercial grade software for use in safety related applications. This standard was written by the CSA Group through a consensus standards development process approved by the Standards Council of Canada. This process brings together volunteers representing varied viewpoints and interests to achieve alignment and balance between stakeholders.

N290.14-15, Qualification of Digital Hardware and Software for Use in Instrumentation and Control Applications for Nuclear Power Plants [I–2], is the second edition of the standard, which has been or will be considered for adoption by licensees (when those utilities apply for re-licensing). This second edition has been greatly expanded, to include hardware qualification requirements and an expanded scope of software. This standard also references several other publications, including, but not limited to those by the Electric Power Research Institute (EPRI), International Electrotechnical Commission (IEC), Institute of Electrical and Electronics Engineers (IEEE) and the International Organization for Standardization (ISO). It was developed by the Canadian Standards Association (operating as 'CSA Group') and provides an interlinked set of requirements for the management of nuclear facilities and activities.

I–2. SCOPE

The intent of N290.14-07 [I–1] is to establish a software qualification process for predeveloped software used in safety related equipment in NPPs. Candidate software products are assessed within the context of their application. The output of the software qualification process results in a software qualification report that provides concise documentation of all the qualification evidence used to justify the use of the candidate software in the given application. The software qualification report provides a clear definition of all the components of the system software, describes the corresponding functionality, identifies any interfacing systems, and imposes limits, restrictions and conditions upon the use of the target software in the application.

The scope of N290.14-07 [I–1] applies to software used in real time process computing Category I, II and III applications. N290.14-07 [I–1] recognizes that Category IV is deemed non–safety related and thus does not require any justification for use. Moreover, N290.14-07 [I–1] does not apply to business systems or analysis software.

The standard is primarily used to justify the use of commercial grade software that has very minor (if any) changes. This is commonly characterized as ‘predeveloped,’ which is defined as software available for use, either commercially or otherwise, prior to design processes. This is different from custom software, which is instead developed under a software quality assurance programme (associated with software category) to meet specific functional and performance requirements in a target application. It is common to qualify the underlying custom software platform as predeveloped software. However, if the predeveloped software product does require some level of modification for the target application, it is then considered ‘custom’ software.

I–3. METHODOLOGY

An assessment of predeveloped software considers the reliance placed on the candidate product to perform its functions important to safety over its in-service life. Considerations include the required behaviour or characteristics of the product with respect to:

- Fail-safe or fail detected behaviour;
- Deterministic response;
- Performance;
- Maintainability;
- Security;
- Reliability;
- Testability (especially where frequent proof testing or occasional software changes are necessary).

The qualification of predeveloped software in accordance with N290.14-07 [I–1] includes the following activities:

- Identifying the candidate product. This includes identifying the candidate product’s functions and description(s) of system interfaces.
- Categorizing safety function(s) of the candidate product.
- Assessing a list of software related qualification concerns. These qualification concerns are a set of postulated failure aspects of a product that have the potential to impede the functions important to safety performed by the product or interfere with the safety related functions performed by other systems and components.
- Qualifying methods:
    - Recognized programme method;
    - Mature product method;
    - Preponderance of evidence method.
- Documenting qualification evidence in a report.
- Concluding qualification of the predeveloped software and candidate product.
- Maintaining the qualification by identifying the impact of any changes that could render the qualification report invalid and requalify the candidate product (if necessary).

It should be noted that N290.14-07 [I–1] does not dedicate any activities associated with verifying the suitability of the candidate product. N290.14-07 [I–1] assumes that the candidate product has been selected for use based on practical project management activities (e.g. cost benefit analysis).

I–4. EXPERIENCE

The Canadian experience with digital computer control systems dates back to the original construction of CANDU reactors in Canada. A CANDU reactor relies on a digital control computer’s control programs to control the reactor. In addition, Darlington Nuclear Generation Station and Point Lepreau use a digital shutdown system computer that monitors various signals to trip the reactor in the event of any initiating conditions (i.e. high boiler pressure, low heat transport flow rate).

As a result, Canadian utilities and design agencies have collaborated to create a rigorous suite of software development frameworks for safety related applications. This suite of standards is known as the 'CANDU Computer Systems Engineering Centre of Excellence.' A separate standard exists for Category I, Category II and Category III (CE-1001-STD [I–3], CE-1002-STD [I–4] and CE-1003-STD [I–5], respectively). These standards provide requirements on software development processes and outputs for use in safety related applications in NPPs. In addition, these standards have been used to develop and maintain the digital control computers and digital shutdown systems over the past two decades. However, as plants age, replacement equipment often comes with digital software and firmware embedded, which pose challenges in applying the CANDU Centre of Excellence standards.

N290.14-07 [I–1] has aided utilities in Canada greatly by providing a systematic approach to qualifying predeveloped software for use in safety related applications. There is extensive experience with using the N290.14-07 [I–1] standard. Very complicated projects can be qualified on a component by component basis in accordance with each component's nuclear safety category. Critical components are categorized as Category I or II and qualified accordingly. Generally, designers strive to segregate the design functions of complex computer systems to help distinguish Category I functions from Category II and III functions. This simplifies the design and also helps the qualification process overall. Utilities in Canada consider the N290.14-07 [I–1] process to be an effective way to evaluate predeveloped digital systems for use in safety related applications. It is a balanced approach between industry standards (i.e. safety integrity level certifications) and evaluating detailed software development activities on prospective suppliers. Unqualified software is either not used or mitigated sufficiently through design such that the application's categorization can be revised down appropriately.

REFERENCES TO ANNEX I

[I–1] THE CSA GROUP, Qualification of Pre-Developed Software for Use in Safety-Related Instrumentation and Control Applications in Nuclear Power Plants, N290.14-07, CSA, Toronto, ON (2007).

[I–2] THE CSA GROUP, Qualification of Digital Hardware and Software for Use in Instrumentation and Control Applications for Nuclear Power Plants, N290.14-15, CSA, Toronto, ON (2015).

[I–3] ATOMIC ENERGY OF CANADA LIMITED, Standard for Software Engineering of Safety Critical Software, CE-1001-STD (Rev. 2), AECL, Chalk River, ON (1999).

[I–4] ATOMIC ENERGY OF CANADA LIMITED, Software Engineering of Category II Software, CE-1002-STD, AECL, Chalk River, ON (2007).

[I–5] ATOMIC ENERGY OF CANADA LIMITED, Software Engineering of Category III Software, CE-1003-STD, AECL, Chalk River, ON (2007).

Annex II

PRACTICE IN GERMANY AND SWITZERLAND

II–1. REGULATORY CONTEXT

The approach used in Germany and Switzerland to qualify digital commercial off the shelf (COTS) devices is based on the requirements given in Safety Requirements for Nuclear Power Plants (SiAnf) [II–1], the KTA safety standard 3501 [II–2] for Germany, and the guideline HSK-R-46 [II–3] for Switzerland.

These rules represent the system level for qualification of digital COTS devices for Category A, B and C safety functions (per Nuclear Power Plants — Instrumentation and Control Important to Safety — Classification of Instrumentation and Control Functions, DIN EN 61226 [II–4]).

The differences between the approaches for the categories (A, B and C) are given in the 'I-3 interpretation' of the German "Safety Requirements for Nuclear Power Plants" (SiAnf) [II–5] and in KTA requirements. The KTA standards also specify the involvement of §20 of the German Atomic Law [II–6] — using an independent expert for the qualification task.

II–2. APPROACH

Regarding nuclear safety, Nuclear Power Plants — Instrumentation and Control Important to Safety — General Requirements for Systems, DIN EN 61513 [II–7] provides an interpretation of the general requirements of Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, DIN EN 61508-1 [II–8]. Regarding software aspects, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Software Aspects for Computer-Based Systems, DIN EN 60880 [II–9], for systems performing Category A functions, and Nuclear Power Plants — Instrumentation and Control Important to Safety — Software Aspects for Computer-Based Systems, DIN EN 62138 [II–10], for systems performing Category B and C functions, correspond to Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems Performing Category B or C, DIN EN 61508-3 [II–11], for nuclear applications.

Equipment qualification in Germany and Switzerland utilizes the approach prescribed in Requirements of Commercial Grade Products and Criteria for Their Use in the Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, VDI/VDE 3528 [II–12]. This guideline describes the basic approach and boundary conditions for equipment qualification of commercial grade products, by intended use in nuclear instrumentation and control (I&C) technology. The aim of VDI/VDE 3528 [II–12] is to realize or preserve an I&C system with required reliability by use of components that are qualified according to industrial standards.

II–3. METHODOLOGY

The approach for evidence demonstrating digital COTS devices for nuclear use is oriented on the national nuclear rules (German SiAnf [II–1], KTA 3501 [II–2]), which refer to the dedicated national standards relevant for hardware and software qualification.

Based on this, the KTA rules represent the boundary conditions and include the phases for qualification. In this case, the software qualification will be defined as part of the theoretical assessment phase, which is specified before the start of a practical test and is to be approved by §20 of the German Atomic Law [II–6] — use of an independent expert for Categories A and B.

The overview in Table II–1 shows the link between the standards.

The aim of the VDI/VDE 3528 [II–12] standard is to fill in the gaps of evidence regarding measures to avoid faults by employing a higher level of qualification measures to cope with failures in the I&C system design and achieve the necessary functional reliability level. The standard describes design variants for the qualification of COTS devices based on industrial precertification, including suitability assessments. The guideline also requires a suitability assessment, performed by §20 of the German Atomic Law [II–6] — use of an independent expert for equipment qualification. Furthermore, DIN EN 61508-1 [II–8] establishes a life cycle framework that will be credited to cover these aspects.

TABLE II–1. SAFETY FUNCTION CATEGORY LINKED WITH RELATED STANDARDS

	Category A (DIN EN 61226 [II–4])	Category B (DIN EN 61226 [II–4])	Category C (DIN EN 61226 [II–4])
Qualification	KTA 3503 [II–13] Type Testing of Electrical Modules for the Instrumentation and Control System Important to Safety (§20 of the German Atomic Law — requiring an independent expert)	KTA 3503 [II–13] Type Testing of Electrical Modules for the Instrumentation and Control System Important to Safety (§20 of the German Atomic Law —requiring an independent expert)	DIN EN 62138 [II–10] Nuclear Power Plants — Instrumentation and Control Important to Safety — Software Aspects for Computer Based Systems Performing Category B or C Functions
	KTA 3505 [II–14] Type Testing of Measuring Sensors and Transducers of the Instrumentation and Control System Important to Safety (§20 of the German Atomic Law — requiring an independent expert)	KTA 3505 [II–14] Type Testing of Measuring Sensors and Transducers of the Instrumentation and Control System Important to Safety (§20 of the German Atomic Law — requiring an independent expert)	
	DIN EN 60780 323 [II–15] Nuclear Facilities — Electrical Equipment Important to Safety — Qualification	DIN EN 60780-323 [II–15] Nuclear Facilities — Electrical Equipment Important to Safety — Qualification	VDI/VDE 3528 [II–12] Requirements of Commercial Grade Products and Criteria for Their Use in the Instrumentation and Control Systems Important to Safety in Nuclear Power Plants
	DIN EN 60987 [II–16] Nuclear Power Plants — Instrumentation and Control Important to Safety — Hardware Design Requirements for Computer-Based Systems	DIN EN 60987 [II–16] Nuclear Power Plants — Instrumentation and Control Important to Safety — Hardware Design Requirements for Computer-Based Systems	
	DIN EN 60880 [II–9] Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Software Aspects for Computer-Based Systems Performing Category A Functions	DIN EN 62138 [II–10] Nuclear Power Plants — Instrumentation and Control Important to Safety — Software Aspects for Computer-Based Systems Performing Category B or C Functions	
	DIN EN 62566 [II–17] Nuclear Power Plants — Instrumentation and Control Important to Safety — Development of HDL-Programmed Integrated Circuits for Systems Performing Category A Functions	VDI/VDE 3528 [II–12] Requirements of Commercial Grade Products and Criteria for Their Use in the Instrumentation and Control Systems Important to Safety in Nuclear Power Plant	

TABLE II–1. SAFETY FUNCTION CATEGORY LINKED WITH RELATED STANDARDS (cont.)

	Category A (DIN EN 61226 [II–4])	Category B (DIN EN 61226 [II–4])	Category C (DIN EN 61226 [II–4])
Qualification	VDI/VDE 3528 [II–12] Requirements of Commercial Grade Products and Criteria for Their Use in the Instrumentation and Control Systems Important to Safety in Nuclear Power Plants		
Quality	KTA 1401 [II–18] General Requirements Regarding Quality Assurance	KTA 1401 [II–18] General Requirements Regarding Quality Assurance	DIN EN ISO 9001 [II–19] Quality Management Systems — Requirements
	ISO 19443 [II–20] Quality Management Systems — Specific Requirements for the Application of ISO 9001:2015 by Organizations in the Supply Chain of the Nuclear Energy Sector Supplying Products and Services Important to Nuclear Safety (ITNS)	ISO 19443 [II–20] Quality Management Systems — Specific Requirements for the Application of ISO 9001:2015 by Organizations in the Supply Chain of the Nuclear Energy Sector Supplying Products and Services Important to Nuclear Safety (ITNS)	
Manufacturing	KTA 3507 [II–21] Factory Tests, Post-Repair Tests and the Certification of Proven Performance of Modules and Devices of the Instrumentation and Control System Important to Safety	KTA 3507 [II–21] Factory Tests, Post-Repair Tests and the Certification of Proven Performance of Modules and Devices of the Instrumentation and Control System Important to Safety	DIN EN ISO 9001 [II–19] Quality Management systems — Requirements
	DIN EN 60987 [II–16] Nuclear Power Plants — Instrumentation and Control Important to Safety — Hardware Design Requirements for Computer-Based Systems	DIN EN 60987 [II–16] Nuclear Power Plants — Instrumentation and Control Important to Safety — Hardware Design Requirements for Computer-Based Systems	DIN EN 10204 [II–22] Metallic Products — Types of Inspection Documents
	DIN EN 10204 [II–22] Metallic Products — Types of Inspection Documents	DIN EN 10204 [II–22] Metallic Products — Types of Inspection Documents	

II–4. PRACTICAL EXPERIENCE

II–4.1. Types of digital commercial off the shelf devices used in various countries

The qualification for digital COTS devices, according to the above described methodology, is already performed for the following kinds of equipment:

- Programmable logic controller (PLC) platforms in Categories B and C[1];
- Transducers installed in cabinets for Category A[2];

[1] The use of PLC platforms in Category A is strongly linked to a process in which the development phases are also checked by §20 of the German Atomic Law, which requires an independent expert. Similarly, the nuclear requirements are respected during the development, which is normally not possible to cover if the development is finalized.

[2] The required function of the devices is limited.

- Digital recorders used for documenting Category A function signals;
- Engineering software for Category A, B and C functions;
- Network communication features for Category A, B and C functions.

II–4.2. Challenges and lessons learned

During qualification of digital COTS devices, some relevant topics have to be considered:

- Close interaction with the manufacturer of the digital COTS device is mandatory;
- Start of practical tests only after a positive software assessment is recommended to reduce the risk of tests with unsuccessful results;
- Documentation of the change management process (life cycle of the COTS device), including the trigger for increasing software and hardware versions;
- Respect for computer security aspects.

II–4.3. Approaches adopted in the equipment qualification

A phase model for performing specific digital COTS device qualification that is covered by a dedicated equipment qualification plan is recommended to ensure the traceability of activities for interaction between the responsible organization that performs the qualification and the independent expert required by §20 of the German Atomic Law [II–6].

REFERENCES TO ANNEX II

[II–1] FEDERAL MINISTRY FOR THE ENVIRONMENT, NATURE CONSERVATION AND NUCLEAR SAFETY, Safety Requirements for Nuclear Power Plants, SiAnf, BMU, Berlin (2015).

[II–2] KERNTECHNISCHER AUSSCHUSS, Reactor Protection System and Monitoring Equipment of the Safety System, Safety Standard 3501, KTA, Salzgitter (2015).

[II–3] HAUPTABTEILUNG FÜR DIE SICHERHEIT DER KERNANLAGEN, Anforderungen für die Anwendung von sicherheitsrelevanter rechnerbasierter Leittechnik in Kernkraftwerken, Guideline HSK-R-46 (04/2005), HSK, Villigen (2005).

[II–4] GERMAN INSTITUTE FOR STANDARDIZATION, Nuclear Power Plants — Instrumentation and Control Important to Safety — Classification of Instrumentation and Control Functions, DIN EN 61226, DIN, Berlin (2010).

[II–5] FEDERAL OFFICE FOR THE SAFETY OF NUCLEAR WASTE MANAGEMENT, Interpretations of the “Safety Requirements for Nuclear Power Plants,” RS-Handbuch 3-0.2, BfE, Berlin (2015).

[II–6] FEDERAL MINISTRY OF JUSTICE AND CONSUMER PROTECTION, Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz), German Atomic Law, BMJV, Berlin (2018).

[II–7] GERMAN INSTITUTE FOR STANDARDIZATION, Nuclear Power Plants — Instrumentation and Control Important to Safety — General Requirements for Systems, DIN EN 61513, DIN, Berlin (2013).

[II–8] GERMAN INSTITUTE FOR STANDARDIZATION, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems — Part 1: General Requirements, DIN EN 61508-1, DIN, Berlin (2011).

[II–9] GERMAN INSTITUTE FOR STANDARDIZATION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Software Aspects for Computer-Based Systems Performing Category A Functions, DIN EN 60880, DIN, Berlin (2010).

[II–10] GERMAN INSTITUTE FOR STANDARDIZATION, Nuclear Power Plants — Instrumentation and Control Important to Safety — Software Aspects for Computer-Based Systems Performing Category B or C Functions, DIN EN 62138, DIN, Berlin (2010).

[II–11] GERMAN INSTITUTE FOR STANDARDIZATION, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems — Part 3: Software Requirements, DIN EN 61508-3, DIN, Berlin (2011).

[II–12] 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).

[II–13] KERNTECHNISCHER AUSSCHUSS, Type Testing of Electrical Modules for the Instrumentation and Control System Important to Safety, Safety Standard 3503, KTA, Salzgitter (2015).

[II–14] KERNTECHNISCHER AUSSCHUSS, Type Testing of Measuring Sensors and Transducers of the Instrumentation and Control System Important to Safety, Safety Standard 3505, KTA, Salzgitter (2015).

[II–15] GERMAN INSTITUTE FOR STANDARDIZATION, Nuclear Facilities — Electrical Equipment Important to Safety — Qualification, DIN EN 60780-323, DIN, Berlin (2018).

[II–16] GERMAN INSTITUTE FOR STANDARDIZATION, Nuclear Power Plants — Instrumentation and Control Important to Safety — Hardware Design Requirements for Computer-Based Systems, DIN EN 60987, DIN, Berlin (2015).

[II–17] GERMAN INSTITUTE FOR STANDARDIZATION, Nuclear Power Plants — Instrumentation and Control Important to Safety — Development of HDL-Programmed Integrated Circuits for Systems Performing Category A Functions, DIN EN 62566, DIN, Berlin (2015).

[II–18] KERNTECHNISCHER AUSSCHUSS, General Requirements Regarding Quality Assurance, Safety Standard 1401, KTA, Salzgitter (2017).

[II–19] GERMAN INSTITUTE FOR STANDARDIZATION, Quality Management Systems – Requirements, DIN EN/ISO 9001, DIN, Berlin (2015).

[II–20] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Quality Management Systems — Specific Requirements for the Application of ISO 9001:2015 by Organizations in the Supply Chain of the Nuclear Energy Sector Supplying Products and Services Important to Nuclear Safety (ITNS), ISO 19443, ISO, Geneva (2018).

[II–21] 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).

[II–22] GERMAN INSTITUTE FOR STANDARDIZATION, Metallic Products — Types of Inspection Documents, DIN EN 10204, DIN, Berlin (2005).

Annex III

PRACTICE IN THE UNITED STATES OF AMERICA

III–1. SCOPE

The following content describes the regulatory structure in the United States of America (USA) that drives the requirements for justifying the use of commercial off the shelf (COTS) devices in nuclear safety applications. The methodology for developing the justification is also described and is illustrated in Fig. III–1. In alignment with the body of this guide, this content is written with a focus on individual components and not on systems or platforms.

III–2. REGULATORY STRUCTURE

The US Code of Federal Regulations (CFR) lays the foundation for requirements for items installed in nuclear safety applications through the definition of the term 'basic component' found in Reporting of Defects and Noncompliance, 10 CFR Part 21 [III–1]:

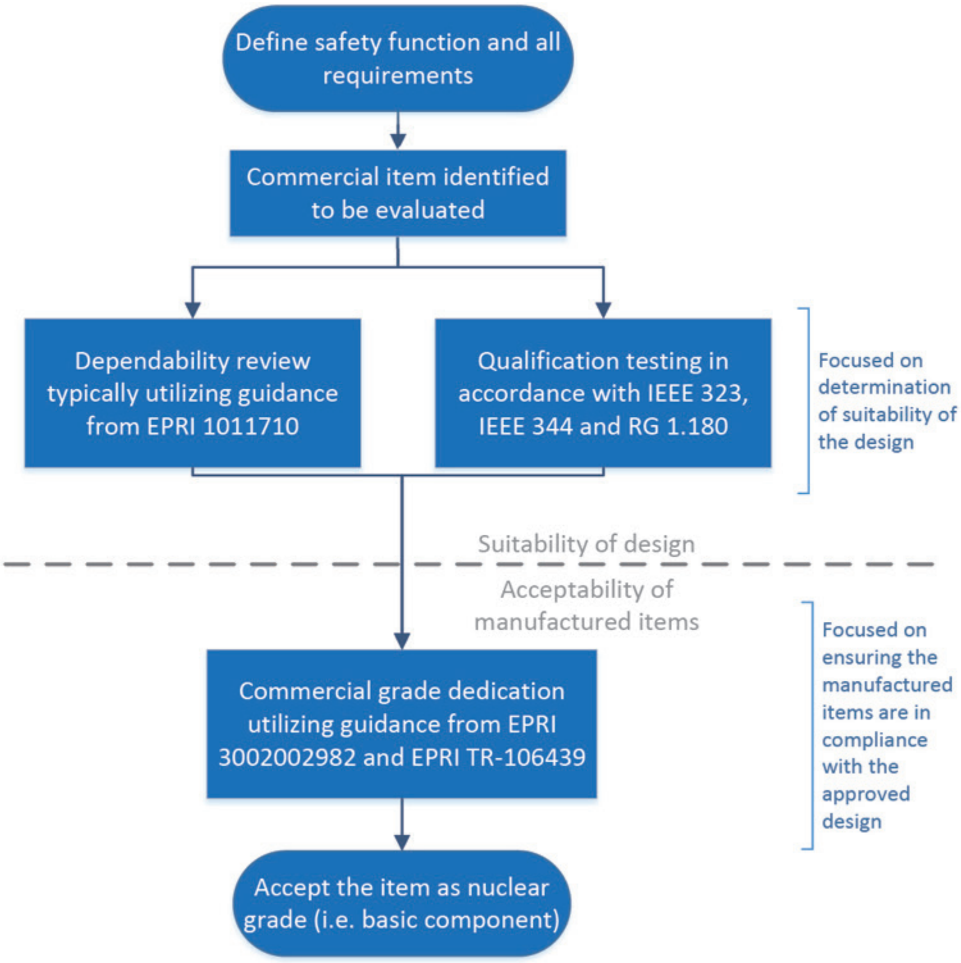

Define safety function and all requirements
Commercial item identified to be evaluated
Dependability review typically utilizing guidance from EPRI 1011710
Qualification testing in accordance with IEEE 323, IEEE 344 and RG 1.180
Focused on determination of suitability of the design
Suitability of design
Acceptability of manufactured items
Commercial grade dedication utilizing guidance from EPRI 3002002982 and EPRI TR-106439
Focused on ensuring the manufactured items are in compliance with the approved design
Accept the item as nuclear grade (i.e. basic component)

FIG. III–1. The justification process for commercial off the shelf devices in the USA.

> “Basic component. (1)(i) When applied to nuclear power plants licensed under 10 CFR Part 50 or Part 52 of this chapter, basic component means a structure, system, or component, or part thereof that affects its safety function necessary to assure:
>
> (A) The integrity of the reactor coolant pressure boundary;
> (B) The capability to shut down the reactor and maintain it in a safe shutdown condition; or
> (C) The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to those referred to in § 50.34(a)(1), § 50.67(b)(2), or § 100.11 of this chapter, as applicable.
>
> (ii) Basic components are items designed and manufactured under a quality assurance program complying with appendix B to part 50 of this chapter, or commercial grade items which have successfully completed the dedication process. …”

The framework for the process used to justify the use of commercial grade (COTS) devices as basic components (i.e. successful completion of a dedication process or dedication) is described by United States Nuclear Regulatory Commission (US NRC) Regulatory Guide (RG) 1.164 [III-2], as follows:

> “10 CFR Part 21, ‘Reporting of Defects and Noncompliance,’ establishes the framework for an acceptance process under the definition for ‘dedication’ and this process is undertaken to provide reasonable assurance that a commercial-grade item to be used as a basic component will perform its intended safety function. Specifically, the definition for ‘dedication’ requires that the dedication process be conducted in accordance with the applicable provisions of Appendix B, ‘Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants,’ to 10 CFR Part 50, ‘Domestic Licensing of Production and Utilization Facilities’”.

RG 1.164 [III–2] also “endorses, in part, the Electric Power Research Institute (EPRI) 3002002982, Revision 1 to EPRI NP-5652 and TR-102260, ‘Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications,’ with respect to acceptance of commercial-grade dedication of items and services to be used as basic components for nuclear power plants.”

For digital equipment, RG 1.164 [III–2] states that:

> “EPRI 3002002982, Revision 1 of EPRI NP-5652 and TR-102260, Section 14.1, ‘Digital Equipment and Computer Programs Integral to Plant SSCs,’ lists six EPRI guidance documents for accepting digital devices. Only TR-106439 ‘Guideline on Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications’ and TR-107330 ‘Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants,’ have been reviewed and endorsed by the NRC in letters dated July 17, 1997 (Ref. 17) and July 30, 1998 (Ref. 18), respectively, as an acceptable approach for meeting an NRC requirement.”

The other aspect of justifying items for use in nuclear safety applications is environmental qualification. This requirement is driven by Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants, 10 CFR Part 50.49 [III–3]. This regulation requires qualification of safety related equipment, and specifies that temperature, pressure, humidity, chemical effects, radiation, ageing, submergence, synergistic effects and margin have all to be addressed. It also states that “Safety-related electric equipment is referred to as ‘Class 1E’ equipment in IEEE 323-1974.” Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants, RG 1.89 [III–4] endorses IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, IEEE 323-1974 [III–5], as an acceptable approach to addressing the requirements of 10 CFR Part 50.49 [III–3]. Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants, RG 1.209 [III–6] also provides guidance within the context that digital items are typically located in mild environments.

The term ‘Class 1E’ comes from IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE 603 [III–7] and is defined as:

> “The safety classification of the electric equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment.”

In addition to the environmental qualification aspects cited in 10 CFR Part 50.49 [III–3], there are seismic qualification requirements summarized in Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants, RG 1.100 [III–8] as:

> “The general requirements for the seismic design of electrical and active mechanical equipment appear in Title 10 of the Code of Federal Regulations (10 CFR) Part 50, ‘Domestic Licensing of Production and Utilization Facilities’ (Ref. 1), and 10 CFR Part 52, ‘Licenses, Certifications, and Approvals for Nuclear Power Plants’ (Ref. 2). The primary sections include General Design Criterion (GDC) 1, ‘Quality Standards and Records’; GDC 2, ‘Design Bases for Protection Against Natural Phenomena’; of Appendix A, ‘General Design Criteria for Nuclear Power Plants,’ to 10 CFR Part 50’.”

RG 1.100 [III–8] goes on to endorse IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, IEEE 344-2004 [III–9], as an acceptable approach to addressing seismic requirements.

The final type of qualification required to be addressed is electromagnetic compatibility (EMC). Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems, RG 1.180 [III–10] specifies acceptable methods for qualifying the equipment accordingly.

III–3. METHODOLOGY (INCLUDING PRACTICAL EXPERIENCES)

When a need for a basic component (i.e. Class 1E item) is identified, the first step is to gather the information necessary to create a complete specification. This information includes the safety function, environmental conditions and all other component specific requirements. This step also includes deciding whether this effort will be focused on a specific application or if it will have a broad and generic focus. Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, EPRI TR-106439 [III–11] and Evaluating Commercial Digital Equipment for High-Integrity Applications, EPRI TR-107339 [III–12] provide helpful guidance for this initial activity to ensure that the requirements specification is accurate and complete.

Once the safety function and supporting technical requirements are defined by the licensee, potential devices can be identified. The rest of this methodology assumes that the potential device is commercial grade (e.g. COTS). This includes a review of the functionality and features of the COTS device and probing of the manufacturer to understand how willing they are to allow access to their design documentation, development process and manufacturing process. Again, EPRI TR-106439 [III–11] and EPRI TR-107339 [III–12] provide helpful guidance in this area.

With the requirements defined and the item selected, the next step is to perform reviews and testing of the design to confirm it is suitable for the application(s). This includes a dependability review, environmental testing, seismic testing and EMC testing.

The environmental testing, seismic testing and EMC testing aspects are straightforward and well defined by standards such as IEEE 323-1974 [III–5] and IEEE 323-1983 [III–13], RG 1.209 [III–6], IEEE 344-2004 [III–9] and RG 1.180 [III–10]. A test programme is prepared in accordance with the applicable standards and a specimen is configured in a conservative representation of the intended application(s). Then the specimen is taken through the test programme (sometimes iteratively) to prove that it can perform its safety function during and after experiencing all the required conditions. In some cases, aspects of this testing can be replaced by analysis. The analysis approach is described in IEEE 344-2004 [III–9].

The dependability review is focused on determining whether the design has adequate evidence of systematic integrity (i.e. built in quality) and a sufficiently low probability of random failures (i.e. reliability). EPRI TR-106439 [III–11], section 4.2, addresses this activity in its discussion of dependability characteristics: "[t]he dependability attributes, which include items such as reliability and built in quality, are generally influenced strongly by the process and personnel used by the manufacturer in the design, development, verification, and validation of the software-based equipment." The manner and scope of this review varies based on the specific item and the intended application. It also varies based on the availability of and access to the manufacturer's (often proprietary) information. The less information that is available, the more testing of the item must be relied upon. EPRI TR-106439 [III–11] includes a list of example activities that could be included in this review, but ultimately states that "[t]he dedicator must determine which activities are appropriate for each application. In general, the choice and extent of activities undertaken to verify adequate quality, and the specific criteria applied in making the assessment, depend on the safety significance and complexity of the device." Since the evaluation of safety significance and complexity is not clearly defined in the US nuclear industry, this guidance leads to some ambiguity as to how this review should be performed. EPRI TR-106439 [III–11] does include four examples of how the process can be used for various situations, and the US NRC's safety evaluation of the EPRI report adds that "[d]epending upon application and product specifics, some of the recommended evaluations may not be needed. Conversely, there may be additional verification activities needed that are not mentioned in the example" (see Ref. [III–14]).

Although it is not endorsed by the US NRC, Handbook for Evaluating Critical Digital Equipment and Systems, EPRI 1011710 [III–15], is often used as guidance for performing the dependability review. The activity described by EPRI 1011710 [III–15] is a critical digital review (CDR) and consists of a system orientation, a process orientation, a thread analysis and a risk analysis. This process typically involves reviews of the manufacturer's development and manufacturing processes, hardware and software architecture, functional features, self-diagnostics, fault detection and operating history.

Once the dependability review and qualification testing are complete, the design can be considered suitable for the intended application. At this point, the methodology moves into the traditional realm of commercial grade dedication (CGD). The focus turns from determining the suitability of the design to determining the acceptability of the actual items that have been manufactured. CGD is traditionally an acceptance process based on confirming that a manufactured item is in compliance with the approved design. Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications, EPRI 3002002982 [III–16] states that "Commercial-grade item dedication is an acceptance method used to obtain reasonable assurance that an item will be capable of performing its intended safety-related function(s). Commercial-grade item dedication occurs after the design and qualification activities are complete."

The primary reference for the CGD process is EPRI 3002002982 [III–16]; this is supplemented by EPRI TR-106439 [III–11] for inclusion of dependability characteristics. The process consists of the technical evaluation and acceptance activities. The technical evaluation is based on the identified safety function(s) and typically uses a failure modes and effects analysis (FMEA) to determine critical characteristics. Each critical characteristic is given a specific acceptance criterion and an acceptance method. There are four acceptance methods available: (1) special tests and inspections, (2) commercial grade surveys (CGS), (3) source verification, and (4) item/supplier performance record. EPRI TR-106439 [III–11] provides guidance that dependability characteristics usually cannot be verified using method 1; it is typical for methods 1, 2 and 4 to all be used in the CGD process for digital equipment. Note that method 4 cannot be used on its own.

Often, the dependability review is considered synonymous with the use of method 2, and this can sometimes cause confusion. While the CDR and CGS both involve seemingly similar vendor audit activities, the goals of these two activities are very different. A CDR is a very technically focused activity that includes some quality assurance oriented reviews, which results in a determination of the suitability of the design for the application. A CGS is a very quality assurance focused activity that includes some technical reviews resulting in a determination of whether items are being manufactured in compliance with the already approved design.

The final step is the acceptance activity in which the acceptance methods are performed to verify the critical characteristics of the manufactured items. Once complete, the items are considered basic components and are justified for use in the intended nuclear safety application.

REFERENCES TO ANNEX III

[III–1] NUCLEAR REGULATORY COMMISSION, Reporting of Defects and Noncompliance, 10 CFR Part 21, US NRC, Washington, DC (2015).

[III–2] NUCLEAR REGULATORY COMMISSION, Dedication of Commercial-Grade Items for Use in Nuclear Power Plants, Regulatory Guide 1.164, US NRC, Washington, DC (2017).

[III–3] NUCLEAR REGULATORY COMMISSION, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants, 10 CFR 50.49, US NRC, Washington, DC (2017).

[III–4] NUCLEAR REGULATORY COMMISSION, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants, Regulatory Guide 1.89 (Rev. 1), US NRC, Washington, DC (1984).

[III–5] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, IEEE 323-1974, IEEE, New York (1974).

[III–6] 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 (2007).

[III–7] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE 603, IEEE, New York (2018).

[III–8] NUCLEAR REGULATORY COMMISSION, Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants, Regulatory Guide 1.100 (Rev. 3), US NRC, Washington, DC (2009).

[III–9] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, IEEE 344-2004, IEEE, New York (2004).

[III–10] NUCLEAR REGULATORY COMMISSION, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems, Regulatory Guide 1.180 (Rev. 1), US NRC, Washington, DC (2003).

[III–11] ELECTRIC POWER RESEARCH INSTITUTE, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, EPRI TR-106439, EPRI, Palo Alto, CA (1996).

[III–12] ELECTRIC POWER RESEARCH INSTITUTE, Evaluating Commercial Digital Equipment for High-Integrity Applications, EPRI TR-107339, EPRI, Palo Alto, CA (1997).

[III–13] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, IEEE 323-1983, IEEE, New York (1983).

[III–14] NUCLEAR REGULATORY COMMISSION, Review of EPRI Topical Report TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” TAC No. M94127, US NRC, Washington, DC (1997).

[III–15] ELECTRIC POWER RESEARCH INSTITUTE, Handbook for Evaluating Critical Digital Equipment and Systems, EPRI 1011710, EPRI, Palo Alto, CA (2005).

[III–16] ELECTRIC POWER RESEARCH INSTITUTE, Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications: Revision 1 to EPRI NP-5652 and TR-102260, Rep. 3002002982, EPRI, Palo Alto, CA (2014).

Annex IV

PRACTICE IN THE UNITED KINGDOM

IV–1. REGULATORY ASPECTS

The Office for Nuclear Regulation (ONR) is responsible for regulating nuclear safety and security across the United Kingdom (UK). The ONR's purpose is to provide efficient and effective regulation of the nuclear industry, holding it to account on behalf of the public. The UK generally operates a goal setting regime rather than the more prescriptive, standards based regime applied in some other Member States. This means that the ONR sets out broad regulatory requirements, and it is for licensees to determine and justify how best to achieve them, referencing relevant good practice (see Ref. [IV–1]).

The key principles considered by ONR inspectors in reviewing safety submissions are set out in the safety assessment principles (SAPs) (see Ref. [IV–2]). The concepts outlined in the key SAPs are then expanded on in more detailed technical assessment guides (TAGs).

The underlying concept behind any safety justification is for the licensee (or duty holder) to show that, with the proposed design and safety measure, the risk is reduced as low as reasonably practicable (ALARP). As a sampling organization, ONR may choose to sample a safety submission (or part of it) but does not approve it formally. It is the responsibility of the licensee to ensure that the risk continues to be as low as reasonably practicable during continued operation of the facility.

The safety justification in the UK is generally expected to be presented in a claims, argument and evidence (CAE) format, to ensure that there is a traceable path between the claim on the device in the overall I&C safety case and the supporting document justifying it (i.e. evidence). The link between claim and evidence has to be explicitly established through the argument element in the CAE justification.

IV–2. STRATEGY

Digital commercial off the shelf (COTS) devices are generally referred to as 'smart devices' in the UK. These devices are assimilated to computer based safety systems.[1] The key SAP applicable to computer based safety systems is clause ESS.27 of the SAPs, which states: "Where the system reliability is significantly dependent upon the performance of computer software, compliance with appropriate standards and practices throughout the software development lifecycle should be established in order to provide assurance of the final design."

The additional guidance supporting clause ESS.27 of the SAPs [IV–2] in Technical Assessment Guide — Computer Based Safety Systems, NS-TAST-GD-046 [IV–3] clarifies that, because of the complexity of these systems, traditional methods of reliability assessment are typically not sufficient to manage the risk of systematic failures, and additional activities are expected as part of their justification. Clause ESS.27 in Ref. [IV–2] and TAG046 [IV–3] also note that a two legged approach is expected in demonstrating the suitability of a smart device for a UK nuclear application. The two legs consist of the following:

— Production excellence, which is a demonstration of excellence in all aspects of production from the initial specification through to the finally commissioned system;

— Independent confidence building measures (ICBMs), which provide an independent and thorough assessment of the safety system's fitness for purpose.

[1] In some instances, smart devices may use field programmable gate arrays or application specific integrated circuits. Because of their inherent complexity, they are generally treated as computer based safety systems and are expected to be justified as such.

As stated in clause ESS.27, “[i]f weaknesses are identified in the production process, compensating measures should be applied to address these. The choice of compensating measures and their effectiveness should be justified in the safety case.” It is possible that the gaps in production excellence cannot be reasonably compensated for and the justification may need to be aborted for that specific integrity level.

ICBMs are generally carried out by the licensee independently from the manufacturer, with specialized technical support where needed. To maximize the value added, they are generally expected to be diverse from the compensating measure used in the production excellence leg.

The expectation in the UK is that the extent of the justification required is in line with the safety significance of the device, according to its safety class. Three safety classes are recognized in accordance with the relevant SAP [IV–2] (i.e. Class 1 to 3). At a minimum (e.g. Class 3), demonstrated good commercial quality of the production excellence of the device may be sufficient, with commissioning test results and prior use as ICBMs. At the higher safety class (e.g. Class 1), it is necessary to assess a wide range of manufacturer’s documentation, including source code. An extensive set of ICBMs are also expected for Class 1 compared with Class 3, sufficient to make an adequate case for safety in the intended application.

TAG046 [IV–3] identifies limits to the reliability claims that can be placed for a single smart device at different safety classes. Modifications at the I&C architecture level may be an effective way to reduce the claim on each smart device, provided that this is supported by a suitable common cause failure (CCF) analysis.

IV–3. METHODOLOGY

The justification of smart devices will include the following areas:

- Identification of characteristics and behaviour required for the device;
- Production Excellence evaluation and implementation of ICBMs;
- Hardware qualification;
- Environmental qualification (including electromagnetic compatibility, EMC);
- Suitability analysis, to confirm that the smart device is suitable for the application given the results of the evaluations listed above.

In the following, the UK practice for addressing production excellence and ICBMs is presented.

IV–3.1. Production excellence

Production excellence is typically assessed using emphasis in the UK (see Ref. [IV–4]), which is both an approach and a tool developed in the UK by the C&I Nuclear Industry Forum (CINIF) based on Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, IEC 61508 [IV–5]. Emphasis consists of approximately 300 questions structured in four phases:

- Phase 1: quality assurance and safety management.
- Phase 2: generic programmable electronic aspects and development process for the device as a whole.
- Phase 3: hardware development process and verification.
- Phase 4: software development process and verification.

The questions are answered by the manufacturer, who provides evidence to support the answers given. The assessor reviews the answers and associated evidence to make judgements of their adequacy to support the implied emphasis requirement. If any deficiencies (or gaps) are identified, they need to be compensated for.

Emphasis is typically performed by considering the device independently of the application for which it will be used. This allows for reuse of the justification in a number of applications, provided that the behaviour of the device and any restrictions identified during the assessment are suitable for each application.

Emphasis covers most IEC 61508 [IV–5] techniques and measures, which are graded to safety integrity levels (SILs). An indication of SIL to class mapping is provided in TAG046 [IV–3].

A CAE based approach may be beneficial. Cogs, also developed by CINIF (see Ref. [IV–6]), is a structured CAE justification approach that was developed with the aim of being generic (i.e. independent of how the COTS component is going to be used) so that it could be reused in a number of applications after suitable verification of its validity in the target application. It is structured around gathering evidence of the intended behaviour of the component and comparing it with available evidence supporting its actual behaviour.

IV–3.2. Independent confidence building measures

The ICBMs are also graded according to class. Examples of ICBMs at the highest class (Class 1/pfd = 10^{-3}) are:

- Instrument type tests;
- Examination, inspection, maintenance and test records;
- Proof test records;
- Commissioning tests;
- Hardware reliability analysis;
- Prior use;
- Supplier pedigree;
- Independent certification;
- Independent review of supplier's standards and procedures;
- Independent functional safety assessment;
- Independent review of tools;
- Static analysis;
- Dynamic analysis;
- Statistical testing.

Examples of ICBMs at Class 3 are:

- Examination, inspection, maintenance and test records;
- Commissioning tests;
- Prior use;
- Supplier pedigree.

IV–4. EXPERIENCE

The approach to justifying smart devices in the UK nuclear industry is a mature process. Several devices (in the order of a few dozen, at the time of this publication) have been assessed following this methodology, and many more are due to be assessed in the next few years. Examples of smart devices justified for nuclear application in the UK include:

- Temperature transmitters;
- Pressure transmitters;
- Radiation monitors;
- Protection relays;
- Gas analysers;
- Voltage regulators.

The majority of this assessment has been done at Class 3. Only a limited number of devices have been assessed to Class 1 and 2.

The justification process requires access to numerous documents, which include development process artefacts such as verification documents and results of analysis and testing performed by the manufacturer. Experience shows that it is important to agree to access to documentation early in the engagement process with the manufacturer, which may require non-disclosure agreements.

For smart device justification in the UK, there is generally limited reliance on certifications, especially at the higher safety classes. While the review of an independent qualified certification body can be used as evidence, its relevance depends on the scope of the certification and the availability of the supporting analyses. Often, the certifications are commissioned by a manufacturer and hence need a level of independent review (including of the supporting documents and analyses). Examples of certifications that can be credited as evidence as part of the justifications in the UK are related to quality assurance (e.g. ISO 9001) and hardware certification (e.g. environmental qualification).

Similarly, a proven in use argument is generally a weak justification for a smart device. In fact, the relevance of the operational experience significantly depends on the quality of data collection (e.g. including the version number, the number of demands, the failure mode) and the contractual arrangement for defect notifications. Operational experience is also limited in identifying systematic failures and hence needs to be complemented, for example with additional assessment of the design process and further analyses.

REFERENCES TO ANNEX IV

[IV–1] OFFICE FOR NUCLEAR REGULATION, A Guide to Nuclear Regulation in the UK, 2016 update, ONR, Liverpool (2016).

[IV–2] OFFICE FOR NUCLEAR REGULATION, Safety Assessment Principles for Nuclear Facilities, 2014 edn, ONR, Liverpool (2014).

[IV–3] OFFICE FOR NUCLEAR REGULATION, Technical Assessment Guide — Computer Based Safety Systems, NS-TAST-GD-046 (Rev. 5), ONR, Liverpool (2019).

[IV–4] STOCKHAM, R., Emphasis on safety, E&T, Issue 2 (2009).

[IV–5] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, IEC 61508, IEC, Geneva (2010).

[IV–6] GUERRA, S., CHOZOS, N., SHERIDAN, D., “Justifying Digital COTS Components when Compliance Cannot be Demonstrated — The Cogs Approach”, Proc. 9th Int. Topical Mtg on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC&HMIT), Charlotte, NC, 2015, ANS, La Grange Park, IL (2015).

GLOSSARY

device of limited functionality. A device that has the following characteristics (quoted from IAEA SSG-39 [2], p. 106):

- It contains predeveloped software or programmed logic;
- It is autonomous and performs only one conceptually simple principal function, which is defined by the manufacturer and which is not modifiable by the user;
- It is not designed to be reprogrammable;
- If it is reconfigurable, the configurability is limited to parameters relating to compatibility with the process being monitored or controlled, or interfaces with connected equipment.

digital device. A device whose implementation is based on operations performed using signals with defined, discrete levels or that contains defined, discrete internal states and makes transitions between those states (IEC 62671:2013 [10]). Additionally:

- The functions of such devices are usually defined by processes that include development and testing involving software or hardware description languages. Such devices may be internally controlled by software or may consist of application specific integrated circuits (ASICs), complex programmable logic devices (CPLDs) or field programmable gate arrays (FPGAs), etc., that have been configured through the use of software.
- Devices, equipment or systems that are controlled by software are described as ‘computer based’, whereas ‘digital’ is a broader term that encompasses any device using digital circuits to implement logic.
- Digital devices developed for non-nuclear industries are called industrial digital devices.

intelligent customer. “An organization (or individual) that has the competence to specify the scope and standard of a required product or service and subsequently assess whether the supplied product or service meets the specified requirements.” (See IAEA NG-T-3.10 [70]).

justification. In this publication, justification means the process by which a commercial off the shelf (COTS) digital device is proved to be suitable for application in a nuclear power plant. In other contexts, ‘justification’ is also referred to as ‘qualification’ or ‘dedication.’

qualification. In this publication, the term is mainly used in relation with environmental certifications (e.g. seismic, temperature, electromagnetic interference/radiofrequency interference, EMI/RFI).

restricted configurability. Applies to devices that can be configured in only very limited ways to select from among relatively few options the manner in which a device will function in its intended application (IEC 62671:2013 [10]).

ABBREVIATIONS

BOM	bill of materials
CCF	common cause failure
COTS	commercial off the shelf
DJR	device justification report
EMC	electromagnetic compatibility
EMI/RFI	electromagnetic interference/radiofrequency interference
FMEA	failure modes and effect analysis
FMEDA	failure modes, effects and diagnostics analysis
FPGA	field programmable gate array
FTA	fault tree analysis
HART	highway addressable remote transducer
I&C	instrumentation and control
ICBM	independent confidence building measure
NPP	nuclear power plant
SAP	safety assessment principle
SDOE	secure development and operational environment
SIL	safety integrity level
V&V	verification and validation

CONTRIBUTORS TO DRAFTING AND REVIEW

Altkind, F.	Swiss Federal Nuclear Safety Inspectorate, Switzerland
Arndt, S.	Nuclear Regulatory Commission, United States of America
Chertov, A.	Rusatom Automated Systems, Russian Federation
de Grosbois, J.	International Atomic Energy Agency
Eiler, J.	International Atomic Energy Agency
El Hadhri, Z.	Bel V, Belgium
Glöckler, O.	International Atomic Energy Agency
Guerra, S.	Adelard, United Kingdom
Jarrett, R.	Tennessee Valley Authority, United States of America
McKay, K.	Ontario Power Generation, Canada
Miedl, H.	TÜV Rheinland ISTec, Germany
Nack, A.	Paragon, United States of America
Nemier, M.S.	Curtiss-Wright, United States of America
Picca, P.	Office for Nuclear Regulation, United Kingdom
Sohn, K.Y.	Mirae Engineering, Republic of Korea
Tienes, M.	Framatome, Germany
Vandewalle, A.	Nuclear Safety Support Services, Belgium

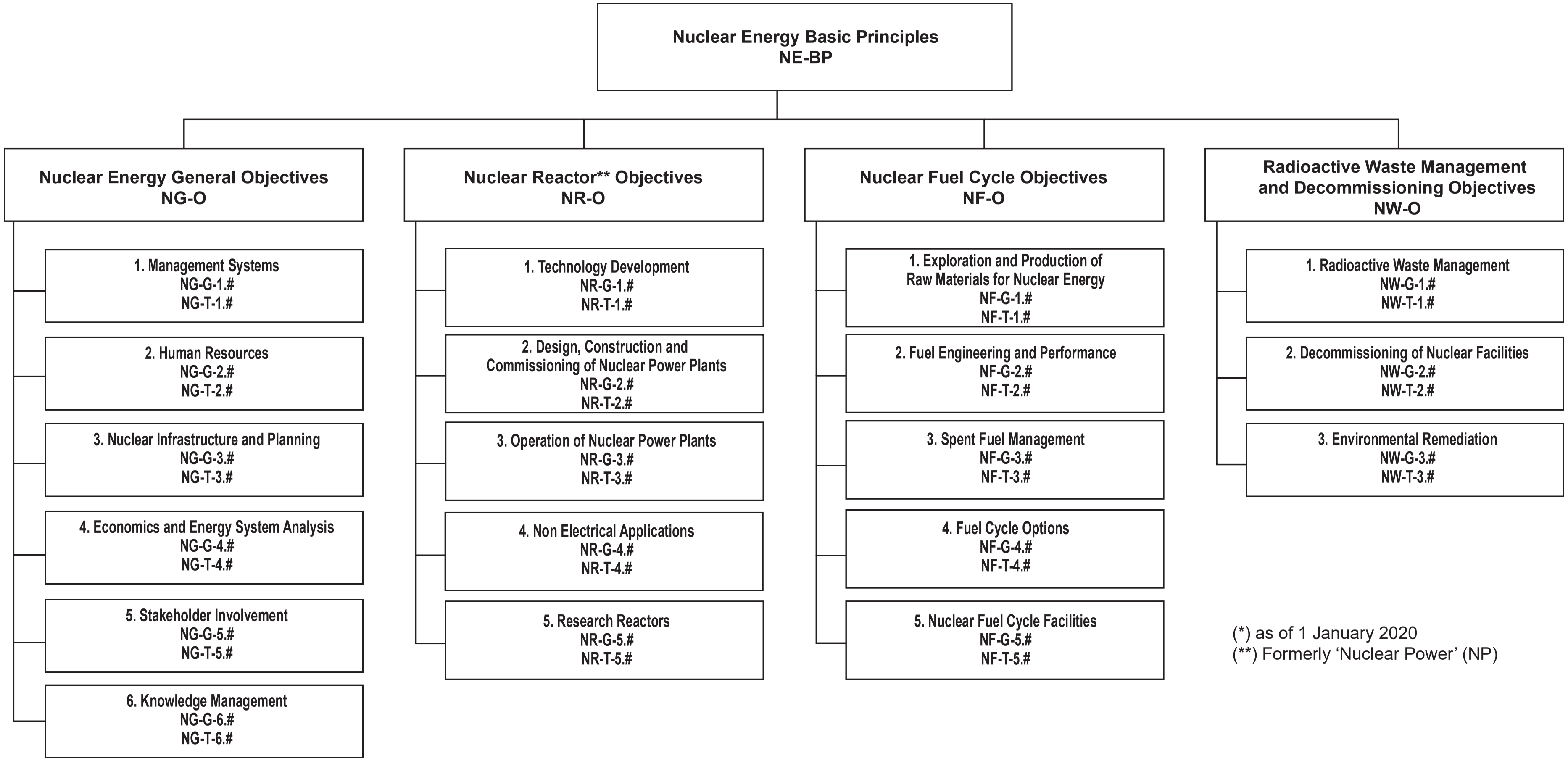
Technical Meeting

Toronto, Canada, 19–22 June 2018

Consultants Meetings

Vienna, Austria, 6–10 November 2017, 19–23 February 2018, 15–19 October 2018

Structure of the IAEA Nuclear Energy Series*



Nuclear Energy Basic Principles
NE-BP

Nuclear Energy General Objectives
NG-O

1. Management Systems
NG-G-1.#
NG-T-1.#

2. Human Resources
NG-G-2.#
NG-T-2.#

3. Nuclear Infrastructure and Planning
NG-G-3.#
NG-T-3.#

4. Economics and Energy System Analysis
NG-G-4.#
NG-T-4.#

5. Stakeholder Involvement
NG-G-5.#
NG-T-5.#

6. Knowledge Management
NG-G-6.#
NG-T-6.#

Nuclear Reactor** Objectives
NR-O

1. Technology Development
NR-G-1.#
NR-T-1.#

2. Design, Construction and Commissioning of Nuclear Power Plants
NR-G-2.#
NR-T-2.#

3. Operation of Nuclear Power Plants
NR-G-3.#
NR-T-3.#

4. Non Electrical Applications
NR-G-4.#
NR-T-4.#

5. Research Reactors
NR-G-5.#
NR-T-5.#

Nuclear Fuel Cycle Objectives
NF-O

1. Exploration and Production of Raw Materials for Nuclear Energy
NF-G-1.#
NF-T-1.#

2. Fuel Engineering and Performance
NF-G-2.#
NF-T-2.#

3. Spent Fuel Management
NF-G-3.#
NF-T-3.#

4. Fuel Cycle Options
NF-G-4.#
NF-T-4.#

5. Nuclear Fuel Cycle Facilities
NF-G-5.#
NF-T-5.#

Radioactive Waste Management and Decommissioning Objectives
NW-O

1. Radioactive Waste Management
NW-G-1.#
NW-T-1.#

2. Decommissioning of Nuclear Facilities
NW-G-2.#
NW-T-2.#

3. Environmental Remediation
NW-G-3.#
NW-T-3.#

(*) as of 1 January 2020
(**) Formerly ‘Nuclear Power’ (NP)

Key

BP:	Basic Principles
O:	Objectives
G:	Guides and Methodologies
T:	Technical Reports
Nos 1–6:	Topic designations
#:	Guide or Report number

Examples

NG-G-3.1:	Nuclear Energy General (**NG**), Guides and Methodologies (**G**), Nuclear Infrastructure and Planning (topic **3**), **#1**
NR-T-5.4:	Nuclear Reactors (**NR**)*, Technical Report (**T**), Research Reactors (topic **5**), **#4**
NF-T-3.6:	Nuclear Fuel (**NF**), Technical Report (**T**), Spent Fuel Management (topic **3**), **#6**
NW-G-1.1:	Radioactive Waste Management and Decommissioning (**NW**), Guides and Methodologies (**G**), Radioactive Waste Management (topic **1**) **#1**

ORDERING LOCALLY

IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

NORTH AMERICA

Bernan / Rowman & Littlefield

15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Telephone: +1 800 462 6420 • Fax: +1 800 338 4550

Email: orders@rowman.com • Web site: www.rowman.com/bernan

REST OF WORLD

Please contact your preferred local supplier, or our lead distributor:

Eurospan Group

Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

Trade orders and enquiries:

Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640
Email: eurospan@turpin-distribution.com

Individual orders:

www.eurospanbookstore.com/iaea

For further information:

Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609
Email: info@eurospangroup.com • Web site: www.eurospangroup.com

Orders for both priced and unpriced publications may be addressed directly to:

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/publications

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA