ADELARD

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

Sofia Guerra

Steven Arndt, Janos Eiler, Ron Jarrett, Horst Miedl, Andrew Nack, Marie Niemer, Paolo Picca

22 October 2019

PT/712/150004/3

Adelard LLP, 24 Waterside, 44-48 Wharf Road, London N1 7UX
T +44 20 7832 5850 E office@adelard.com W www.adelard.com

OUTLINE

- Introduction
- Challenges
- Strategy
- Process
- Maintenance of justification

INTRODUCTION

- Digital COTS components increasingly used in NPPs
  - Analogue counterparts obsolete and often not available
- Improved functionality
  - Better accuracy
  - Better noise filtering
  - In-built linearisation
  - Better on-line calibration
  - Better diagnostic features
- Large user base and corresponding operating history
- Challenges associated with demonstration of adequacy
- This paper summarises a IAEA publication on the justification of digital COTS devices
- Scope – digital COTS with limited functionality, that can be configured but not programmed

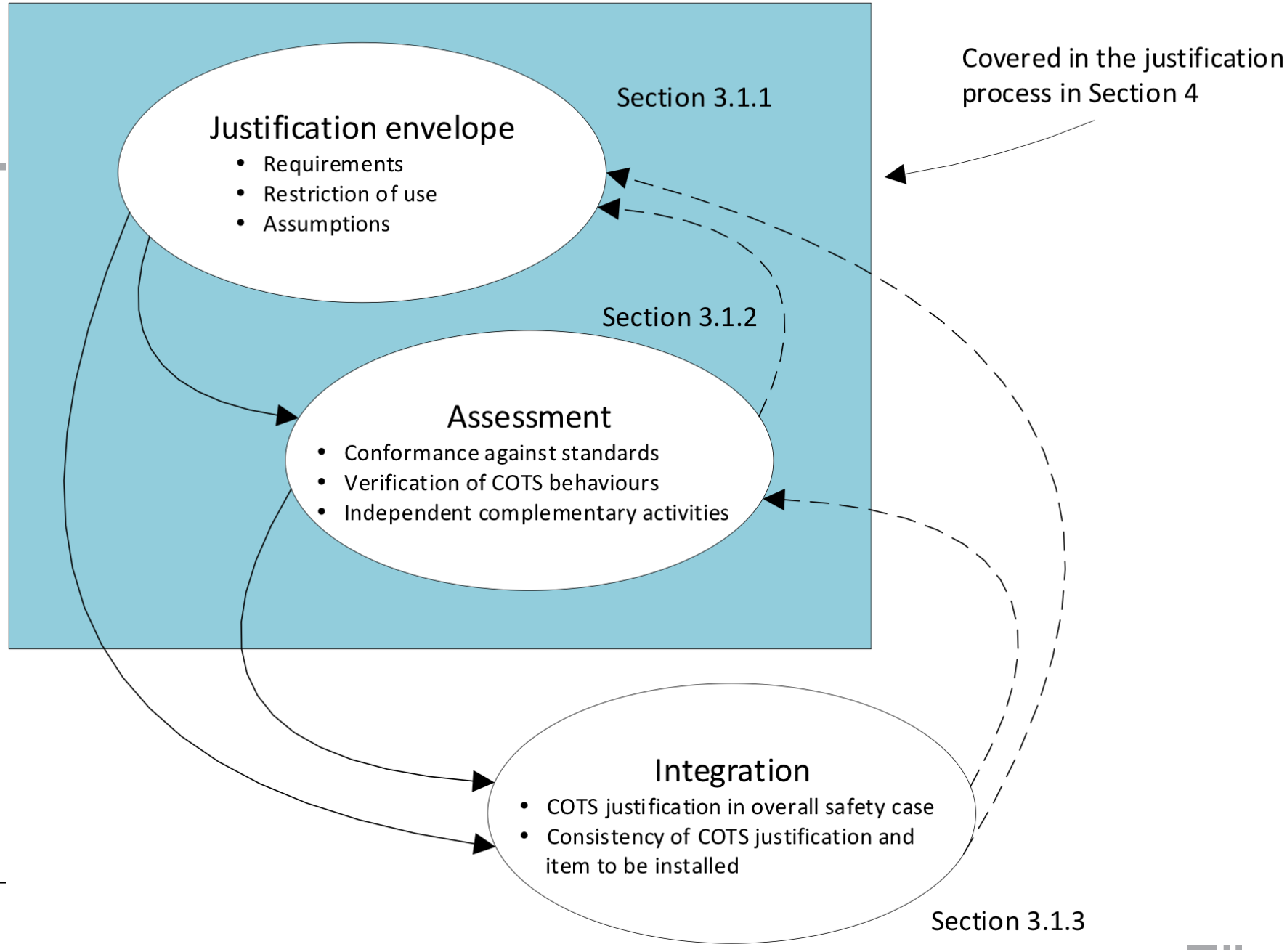
STRUCTURE OF THE DOCUMENT

1. Introduction
2. Challenges associated with commercial industrial I&C equipment
3. Strategy for the justification of commercial industrial I&C equipment
4. Justification process
5. Maintenance of the justification
6. Regulatory aspects
7. Summary

CHALLENGES

- Digital COTS devices
  - Complexity of software-based system/components
  - Common cause failures considerations
- Hardware and software vulnerabilities
  - Potential new failure modes
  - Identification of EDD and undeclared content
  - Counterfeit, fraudulent and suspect items
  - Computer security considerations
- Organisational challenges
  - Identification of safety requirements
  - Device selection
  - Evidence required to justify the COTS device
  - Change management
  - Lack of qualified and experienced personnel

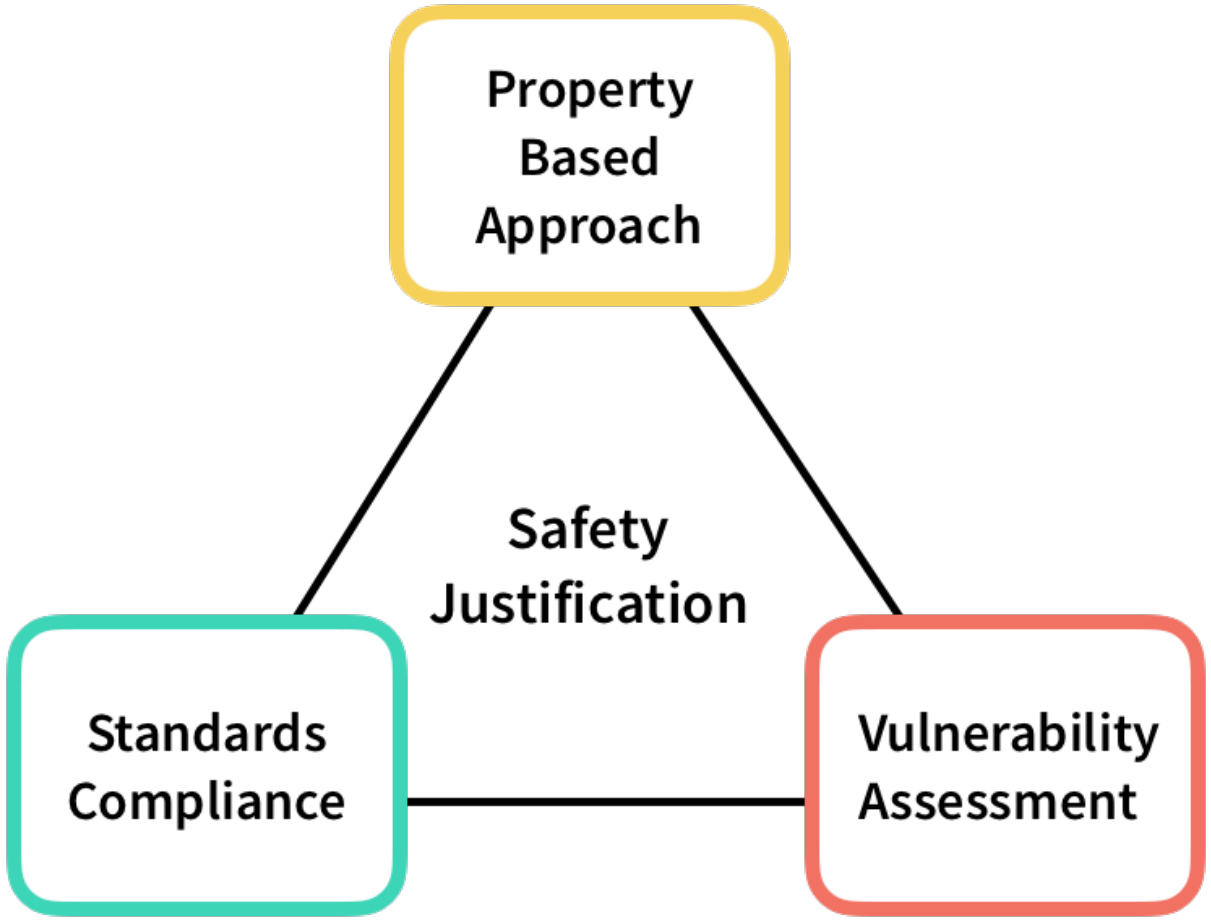
STRATEGY



JUSTIFICATION ENVELOPE

- Advantages of generic assessments
  - Reuse of components in several applications
- Suitability of device and justification for the application crucial part of deployment
- The justification envelope should include
  - The identification of requirements including, for example, target safety classification, functional and non-functional requirements, scope of the environmental and seismic qualification
  - Restrictions of use, which may reduce the scope and the complexity of the justification.
  - Assumptions that may have been made by the assessors and affect the scope of the justification.

ASSESSMENT



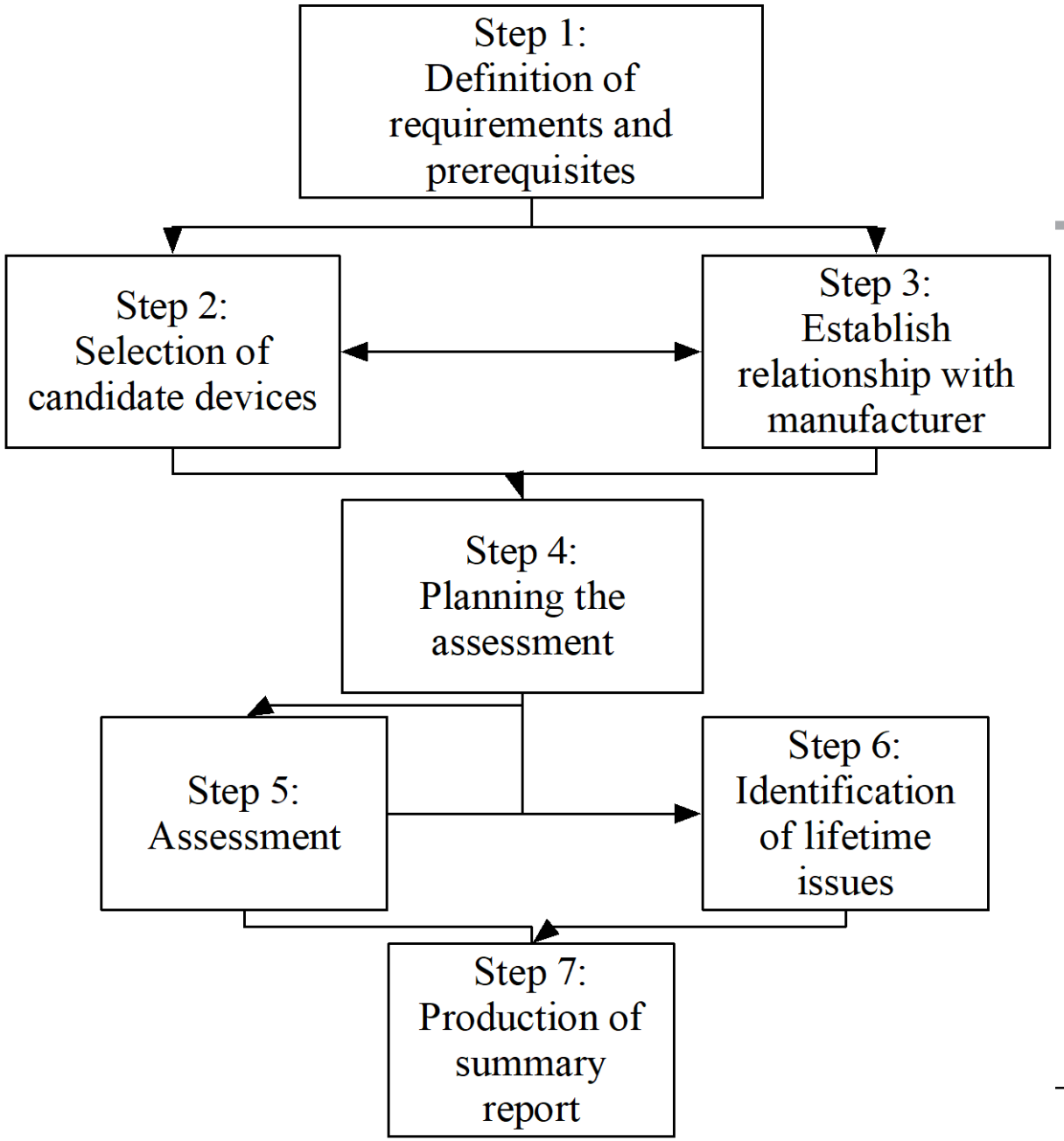
INTEGRATION

- COTS device is implemented in the I&C architecture and its safety justification is integrated in the overall safety justification:
  - A review of the justification in the context of the application: verify if the behaviour, restriction of use and any assumptions considered in the generic justification are suitable for the application.
  - Common cause failure (CCF) analyses: the same device or devices of similar characteristics may be used in other parts of the overall I&C architecture, possibly at a different levels of the defence in depth of the plant. The impact of systematic failures of these devices at plant level should be considered.
  - Application-specific vulnerability assessment: when a specific application is identified for the COTS device, an assessment of the impact of the failure modes identified in the vulnerability assessment on the plant is required.

PROCESS

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

- The steps do not necessarily need to be performed


Step 1:
Definition of requirements and prerequisites
Step 2:
Selection of candidate devices
Step 3:
Establish relationship with manufacturer
Step 4:
Planning the assessment
Step 5:
Assessment
Step 6:
Identification of lifetime issues
Step 7:
Production of summary report

STEP 1: DEFINITION OF REQUIREMENTS AND PREREQUISITES

- In this step:
  - Identify the device requirements that are necessary to be considered during the justification
  - Identify the prerequisites of the device to be met by the application in order to guarantee that the requirements are achieved
- The justification of the device will be based on the requirements identified in this step
- This can be done by
  - defining all the necessary requirements for the application
  - performing a generic assessment by considering the functionality of the component as claimed by the manufacturer (e.g. in data sheets or user manuals)
- The generic justification might consider 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).

STEP 2: SELECTION OF CANDIDATE DEVICES

- In this step:
  - Select candidate devices
  - Review the functionality and other characteristics of the device to decide whether they meet the application requirements or are of sufficient interest to perform a generic qualification
  - Investigate commercial arrangement including the willingness of the manufacturer to engage with the justification process and to give access to information on the development process and design
  - Assess the complexity of the devices to evaluate the likelihood of completing the justification
  - Review the existing documentation to determine the likelihood of completing the justification

STEP 3: MANUFACTURER INFORMATION AND SUPPORT

- In this step:
  - Establish contractual relationship with the manufacturer
  - Agree and sign an NDA, if required
  - Agree the evidence and documentation that will be made available to carry out the justification
  - Agree assessment process and access to information
  - Agree versions of components (including software and hardware) of the device to be justified
  - Agree on justification report content that users will receive (what can be shared with the user)

STEP 4: PLANNING

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

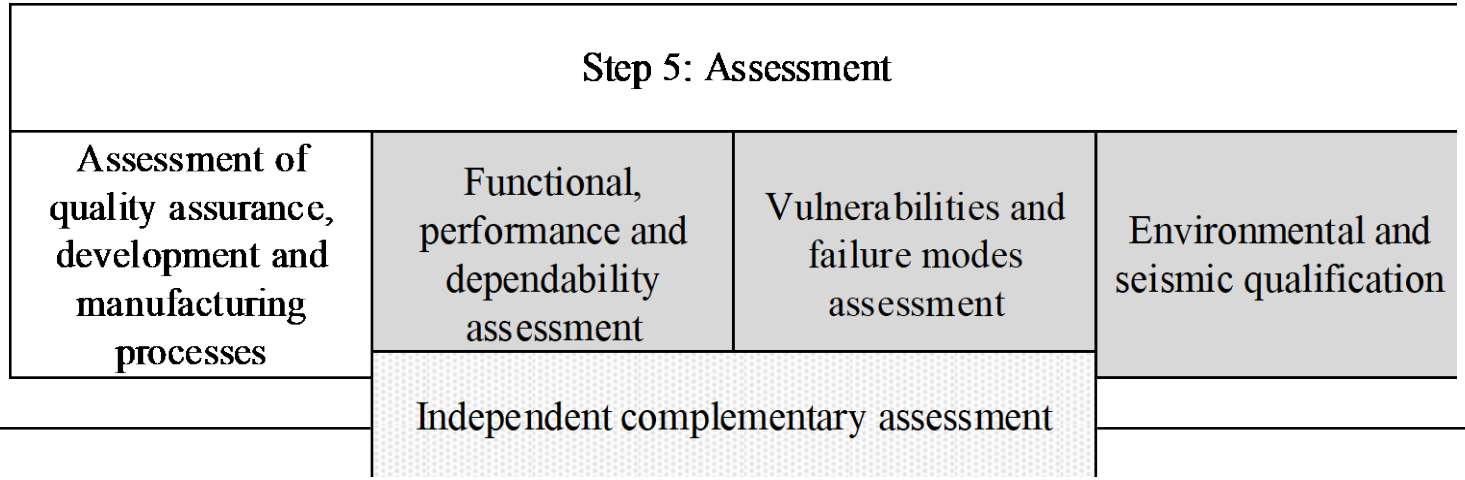
- The justification follows a DJP, which documents the feasibility of the justification and the methods to be used,

- DJP takes into account
  - the technologies used to implement the device
  - development process followed
  - operating data available
  - existing certification

- It also explains how the activities planned will meet any considered national approaches, and any areas not covered are identified and a rationale given for their omission.

STEP 5: ASSESSMENT

- In this step, the assessment is carried out to examine whether
  - The device has been developed and manufactured using appropriate design techniques and processes that are commensurate with the safety role of the device
  - The functional, performance and dependability behaviour meet the requirements
  - Potential vulnerabilities and systematic faults have been managed
  - The environmental qualification data exists that is representative of the in-service conditions
  - Additional confidence is achieved through independent complementary activities.



QUALITY ASSURANCE, DEVELOPMENT AND MANUFACTURING PROCESSES

- Assessment of processes implemented by the manufacturer for the development and production of the COTS product and identifies any gaps in the requirements for a nuclear grade product
- It includes evidence of the use of appropriate processes, methods, techniques and tools, tools qualification, personnel experience and competence and configuration control.
- Includes
  - Development process
  - Quality assurance
  - Design
  - Tools
  - Security
  - Obsolescence management
  - Manufacturing

FUNCTIONAL PERFORMANCE AND DEPENDABILITY ASSESSMENT

Attribute	Explanation	Example evidence
Functionality	This may include: - Inputs and outputs - Algorithms - Configuration	Functional testing Black box testing Traceability from requirements to tests Non-interference
Timing	Response time Throughput	Performance testing Static timing analysis Predictability analysis of the design
Dependability	This may include: - Fail-safe behaviour - Reliability - Failure recovery	Failure analysis Fail-safe design FMEDA Self-monitoring Diagnostic coverage
Operability	…	

VULNERABILITIES AND FAILURE MODES ASSESSMENT

- Possible defects or deficiencies that could lead to a failure
- Consider specific aspects of the design and implementation

Technology/implementation	Example vulnerabilitiy	Possible evidence
Programming languages	Division by zero Buffer overflow Pointer arithmetic	Compliance with coding standard Static analysis
FPGAs	Timing Tool chain vulnerabilities	Coding standards Tool justification
General	System overload	Load testing
…	…	…

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 functional during all seismic and environmental parameters specified.
- Qualification parameters may include
  - Hardware ageing
  - Susceptibility to EMI/RFI and power surges
  - Radiation
  - Temperature and humidity extremes
  - Voltage/frequency variations
  - Seismic and non-seismic vibration
  - Operational cycles

INDEPENDENT COMPLEMENTARY ASSESSMENT

- The justification includes some activities that are performed independently from the manufacturer
- The level of independence and the activities vary with grading and from country to country
- They may include
  - Commissioning tests
  - Source code static analyses
  - Simulation based testing
  - Additional types of testing

STEP 6: IDENTIFICATION OF LIFETIME ISSUES

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

- The suitability assessment considers the behaviour at the time of commissioning.
- Consider the preservation of suitability during the lifetime of the component.
  - Time affects the device itself, e.g., ageing
  - Time affects its context, including the people that use it and the organisational structure in which they operate..
- Evidence may include
  - Processes from the manufacturer demonstrating that they have procedures in place to maintain the technical know-how and adequate support arrangements
  - Operating and maintenance procedures and appropriate security provisions.

EXAMPLE OF SOURCES OF INFORMATION FROM DESIGN

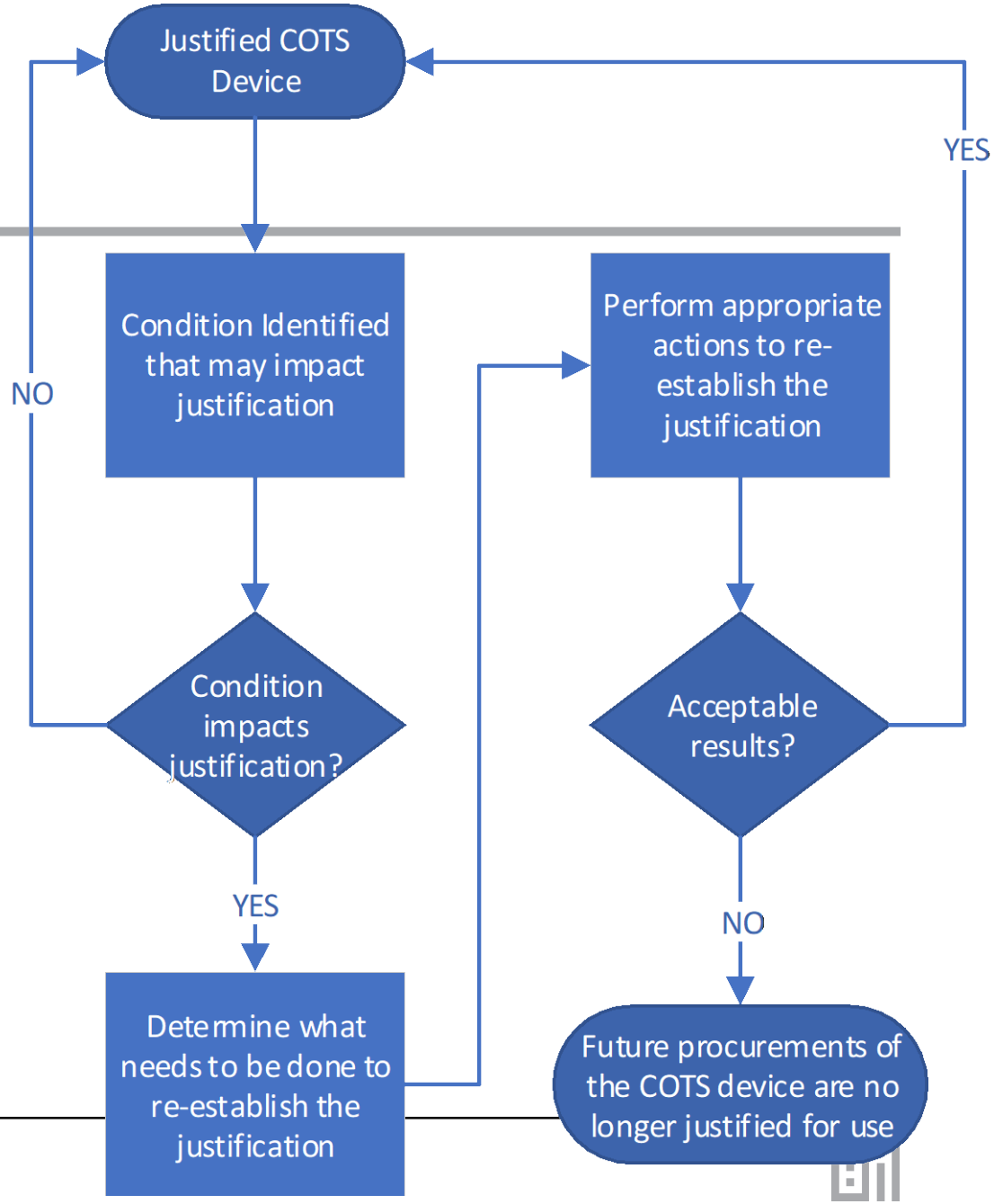
Type of change	Sources of information
Changes due to age	Design features that tolerate ageing, such as component de-rating Design features to work around aging, such as the ability to calibrate or to replace life limited components
Deliberate changes	Well designed user interface and connection panel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

STEP 7: DOCUMENTATION PACKAGE

- In this step:
  - Complete and issue the device justification report (DJR)
  - Identify and update user documentation and safety manual
- The DJR will refer to a number of documents produced during the justification, as well as evidence that existed before the justification started (including manufacturer's documents and any existing certification).

MAINTENANCE OF JUSTIFICATION

- Maintain the integrity and validity of justification
- Issues include
  - Change management and defect reporting
  - Periodic quality assurance measures, e.g., audits
  - Configuration management



CONCLUSIONS

- Digital COTS devices increasingly used in NPPs
- Several challenges with its use
  - Complexity of digital components
  - Not developed to nuclear standards
  - Existing and access to information
- IAEA report discussing these issues
  - Challenges
  - Strategy
  - Justification process to implement the strategy

ADELARD