# THE ROLE OF CERTIFICATION IN THE SAFETY DEMONSTRATION OF COTS EDDS

**Sofia Guerra and Luke Hinde**
Adelard LLP
24 Waterside, 44-48 Wharf Road
London N1 7UX, UK
{aslg,lpeh}@adelard.com

[Digital Object Identifier (DOI) placeholder]

## ABSTRACT (Abstract Head)

Embedded digital COTS devices are increasingly being used in Nuclear Power Plants. Although these devices are often not developed according to nuclear standards, they still need to be justified to be deployed in nuclear applications.

Different countries have been developing their own processes to justify COTS digital devices. In many cases, this justification is based on the assessment of the development process. This is consistent with traditional standard-based approaches to safety justification – compliance to accepted practice was deemed to imply adequate safety. This could be demonstrated either directly through a review of the development artefacts or indirectly through consideration of existing certification, e.g., IEC 61508.

However, over the last 20 years, there has been a trend towards explicit claim-based approaches, where specific safety claims are supported by arguments and evidence at progressively more detailed levels. The standards-based approach and the claim-based approaches are not mutually exclusive, and a combination can be used to support a safety justification. In fact, for the most critical systems, it can be argued that a safety case should consider both aspects.

In this paper, we discuss the use of development process-based approaches to the safety justification of EDDs COTS components, the link between development processes and reliability, how certification may support the justification, and some of the pitfalls of relying on certification.

*Key Words*: Embedded digital devices, certification, safety justification approach

## 1 INTRODUCTION

Embedded digital COTS (commercial off-the-shelf) devices are increasingly being used in Nuclear Power Plants (NPPs). Although these devices are often not developed according to nuclear standards, they still need to be justified to be deployed in safety-related nuclear applications. Their safety justification might require knowledge of the internal structure and development process. However, they are normally sold as a "black box" where there is no knowledge of the internal structure. In addition, their software constitutes a valuable intellectual investment, and the civil nuclear companies purchase sensors in small quantities, and therefore there is limited incentive for the manufacturers to support the assessments that might be necessary to justify their use. Consequently, the nuclear industry is interested in using certification as the main component of the safety justification.

This paper discusses the use of certification to justify embedded digital devices or *smart devices*, i.e., devices that contain a programmable component, such as a microprocessor or an FPGA, and therefore contain both hardware and software. Beyond containing software, the key feature of a smart device is that it is programmed to perform a specialised function, for example measuring a physical quantity or

monitoring another device, and cannot be reprogrammed by the end user in a way that changes this functionality. Limited configuration by the end user may be possible, such as setting alarm thresholds or input and output ranges. Examples of smart devices include radiation monitors, uninterruptible power supplies, or temperature sensors and transmitters.

The focus of this paper is on product safety certifications (and software development process certification), in particular to IEC 61508, or IEC nuclear standards; equipment qualification certification is not explicitly included in the paper, and several of the conclusions would be different if equipment qualification was included.

This paper discusses safety justification approaches, and distinguishes those based on compliance with specified processes with behaviour-based approaches. It considers certification as one particular approach to process-based justification, and explores some of the weaknesses of such an approach. It suggests a strategy combining aspects of process-based and behaviour-based justification, and highlights some of the ways in which these aspects can complement each other to produce a sound justification.

## 2 SAFETY JUSTIFICATION APPROACHES

There are two principal approaches to the construction of a safety justification [1]. The focus of a *process-based* approach is on demonstrating that the design and development approach is in accordance with accepted standards and practices. A *behaviour-based* approach focuses on demonstrating that the produced device exhibits the correct behaviour. We describe each approach in more detail below.

### 2.1 Process-based Approach

A process-based justification of a smart device, or any I&C system, is a demonstration that the device has been designed and verified according to a structured process which meets a rigorous set of requirements. It is argued that a system that has been developed in compliance with these requirements on the development process is acceptably safe. The requirements on the design and development process may be based on a combination of widely used standards for electronic equipment, e.g. IEC 61508 [2], nuclear-specific standards, e.g. IEC 60880 [3], or a set of requirements written specifically for the justification of I&C equipment in a particular context; in many cases the requirements vary according to the level of safety required.

A process-based justification is supported by an assessment of the development of the device to ensure that all requirements are met. This includes documentation of the organisation and quality management of the supplier, and the development processes followed for the device being justified. This assessment may be done directly to support the justification, or it may be performed by a third party who provide certification that the device has met a specified standard.

### 2.2 Behaviour-based Approach

A behaviour-based approach to justification of a device focuses on demonstrating that the final device achieves the required safety properties or behaviour. These properties depend on both the device itself, and its role within the overall I&C system, and are therefore specific to the device being justified. Examples of such properties include accuracy, response time, and fault detection.

A behaviour-based justification will be supported by both development documentation and testing. Device requirements and specification documents confirm that the specified behaviour of the device meets the safety requirements for the application. Tests and other analyses, e.g. static analysis of software, demonstrate that the behaviour of the device conforms to the specification and that there is no undocumented or unintended behaviour. The absence of unintended behaviour may also be supported by demonstrating that a rigorous development process is followed which will identify faults before release.

# 3 CERTIFICATION

Certification typically assesses the development processes of a device against an accepted standard such as IEC 61508, and therefore is a process-based approach, as described above. Given the challenges related to access to manufacturer's IP, the skills required to perform such assessments (including detailed understanding of hardware and software engineering and corresponding verification techniques), the cost associated with the detailed assessment and the number of devices typically used by a particular licensee, certification can be an attractive basis for the safety justification of a product. In fact, certification is used in a number of safety-related areas, as well as for NPPs in a number of countries, as discussed in [4], although the extent to which third party certification is relied on to support the qualification of smart devices varies significantly. In particular, it is rare that third-party certification of COTS products is accepted at the highest integrity levels, although there are a few exceptions.

Certification alone is not enough to provide a complete justification for the use of a smart device. It is also necessary to justify the selection of the chosen device for the chosen application, or provide some other demonstration that the device meets the requirements of the application.

There are number of pitfalls related to relying on certification as the main basis for the safety justification. These are both related to its focus on the process and to the certification practices (see, for example, [5]). These potential problems are discussed in the following sections.

# 4 PITFALLS OF PROCESS-BASED JUSTIFICATION

## 4.1 Validation of standards processes

Standards-based approaches works well in stable environments where best practice is deemed to imply adequate safety and the components were developed according to the relevant standards. However, for software-based systems, the link between compliance with standards and the integrity achieved has not been demonstrated. In fact, as argued in [5], there is counter evidence to the claim that following IEC 61508 demonstrates the corresponding integrity level.

Although IEC 61508 rejects the use of quantified reliability for software, the standard talks about statistical testing and discusses statistical requirements for operating experience. In addition, the quantified SILs imply that the software reliability is quantified.

Previous work [6] has demonstrated the link between the development process and reliability of the product, where process modelling is used to support arguments about the reliability of a product. This work is related to the theory of reliability growth modelling, which shows that, using relatively standard assumptions, a conservative lower limit on the mean time before failure (MTBF) is inversely proportional to the number of faults in the software [7]. In particular, the lower limit is that

$$MTBF \geq \frac{eT}{N},$$

where N is the number of faults, and T is the length of time the device has been in operation. This shifts the problem of reliability prediction from estimating reliability directly to one of estimating the value of N.

One method of estimating N we have developed is to construct a "barrier model" to perform a detailed analysis of the software development process. In the barrier model, a parameterised model is constructed to provide estimation for the number of residual faults N and to assess the quality of the development process with respect to industry norms. In the barrier model each development stage introduces errors of different types (e.g. requirements, design or code) or includes review, analysis or testing to detect errors. This is illustrated in Figure 1.

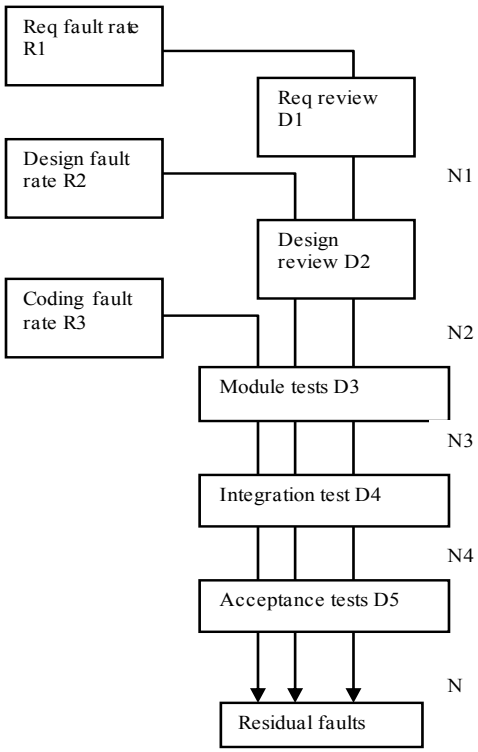


**Figure 1: Barrier model**

The process model can be used to predict the number of residual faults and the faults detected at intermediate stages. The model assumes that the number of faults introduced during development is proportional to the number of lines of code. The application of different verification techniques provides a number of sequential barriers, each of which detects a proportion of the remaining faults in the code. Faults detected are then rectified. However, some faults may be undetected by any verification technique applied, and so remain in the final software. For a fixed process encompassing the design, implementation and verification of a software product, the number of faults expected to be present in the final software is therefore proportional to the length of the code, i.e. more complex code is expected to contain more faults.

The data required for the model are the fault creation rates per 1000 lines of code at each stage (R1, R2,...) and the detection efficiencies of the various barriers (D1, D2,…). In practice the barriers will have different detection efficiencies for the different types of faults. For example, module testing should have high detection efficiency for code faults, lower efficiency for design faults and an even lower efficiency for requirements faults. Therefore, a set of detection efficiencies are used for the different fault sources, e.g. $D1_{req}$, $D2_{req}$ $D3_{req}$..., $D2_{des,}$ $D3_{des,}$ $D4_{des}$.... etc. The number of faults revealed at each stage is the combined output of these fault streams as they pass through the barriers, e.g.:

$$N1 = R1 \times D1_{req}$$

$$N2 = R1 \times (1- D1_{req}) \times D2_{req} + R2 \times D2_{des}$$

$$N3 = R1 \times (1- D1_{req}) \times (1-D2_{req}) \times D3_{req} + R2 \times (1-D2_{des}) \times D3_{des} + R3 \times D3_{code}$$

After the final stage there is no further barrier, so the number of residual faults (per kloc) is the sum of the different fault streams, attenuated by the sequence of barriers:

$$N = \sum R_i \prod (1-D(j)_i) \qquad (j \geq i),$$

where $i$ represents the fault source, $j$ represents a barrier, $R_i$ is the fault rate of source $i$, and $D(j)_i$ is the detection efficiency barrier $j$ for faults of type $i$.

For any new process, the model parameters, $D$ and $R$, have to be determined for all project stages. If work is done to validate the steps mandated by a standard, publicly available industrial process data could be collated to support this aspect of the study. This could be used to understand whether the techniques required by the standard are enough to achieve the required reliability. At the moment, there is no evidence that indeed such a link exists.

## 4.2 Complexity

In addition, as clearly shown above, reliability is related to complexity. In general, process-based approaches founded on certification do not consider the complexity of the device when assessing the development process. For example, neither IEC 61508 nor IEC 60880 requirements on the verification techniques for software performing category A functions depend on the complexity of the software architecture, nor on the number of lines of code.

In particular, the lower limit of a device's reliability is given by $MTBF \geq \frac{eT}{N}$, where N is the number of faults, and T is the length of time the device has been in operation. A process-based approach would typically only require a fixed amount of testing to be performed, and so the value of T is fixed. As a result, for a specified target MTBF, there is a maximum size of code for which a process-based justification can show that this MTBF is achieved without additional testing of the device, or other behaviour-based justification.

Other aspects of development, such as the prevention of systematic hardware failures, also depend on the complexity of the device. Since certification of a device need not consider the complexity of the device, a certification-based justification could be challenged on whether the process provides sufficient assurance of the absence of faults. Conversely, for simple devices containing a small amount of code and a simple architecture, a simpler verification process may be able to provide confidence in the absence of faults. However, such a verification process may not meet all requirements of a standard, and so could not be justified based on certification.

## 4.3 Uncertainty

There is an important role played by uncertainty in dependability cases [8]. When an assessment of compliance with a standard is performed, there will be a confidence associated with the conclusions, and in particular, the reliability that can be claimed for that component. In experimental results, when experts reviewed the assessment of systems and asked to provide a level of confidence that SIL 2 had been achieved, they decided to consider it SIL 1 because of uncertainties.

The confidence required in a SIL for software is not addressed in the standards. For hardware, there is a requirement for the failure rate data to have a confidence level of at least 70%, for example (clause 7.4.9.5 of Part 2). The level of required confidence could push the SIL requirement to a higher level. However, application of standards does not explicitly discuss the rigour of their application, or the impact of any possible non-compliances in the overall confidence or on what may be claimed.

## 4.4 Assumptions and application

A safety justification based on compliance with standards argues that it provides evidence that a device has been developed according to a well-structured process, and that this process meets a suitable standard representing best practice. Evidence to support certification generally consists of quality assurance plans and documentation from different phases of development.

However, certification is only one part of a complete safety justification. A safety justification relying

on certification of the development process must further justify that a device developed according to this standard meets the safety requirements, as the design and verification processes ensure that the design achieves the specifications, and that defects are identified and removed. For example, calculations of safe failure fractions make assumptions of what the safe state is, but this is not clear until the application is known. There may be applications where availability is a safety requirement, and the argument of fail safety does not apply.

Similar assumptions are made about the environment where the device will be used. Such an example is the temperature used for FMEA calculations, but other less obvious assumptions may be made that will have an impact on the suitability of the device and are not clearly visible in a certificate.

## 5 CERTIFICATION: LACK OF VISIBILITY AND CONSISTENCY

Certification documentation typically consists of a certificate stating key information such as device name, version, standard and level of compliance achieved, and supporting reports documenting the assessment that was performed. These reports summarise the activities performed as part of the assessment, and the conclusions reached. However, they typically do not include details of the development process followed by the device manufacturer, testing that was performed during development or how the conclusions have been reached.

This lack of visibility of the assessment performed for the certification can be exacerbated by the use of devices certified to different standards, or by a lack of consistency in the certification methodology. Standards and certification bodies may have different interpretations or expectations for certain parts of the development process, particularly when standards are written for use by different industries, or when certifying organisations are based in different countries or regulatory contexts. For example, we have seen examples where our assessment identified significant weaknesses in the development process, despite the system having been certified for IEC 61508 to SIL 3.

In a previous paper, Rosemount stated that our assessment "was one of the most rigorous and focused audits of our designs and processes that we have ever experienced. This was not a simple process of checking boxes based on a quality manual or process we have in place on our intranet site. The auditors requested to see proof that the processes were followed and that they were effective in achieving the goals they were designed to achieve. There was also extensive inquiry into how the device firmware was written, and many aspects of the performance of the firmware to minimize the possibility of bugs in the implementation. A product that endures this level of scrutiny must have not only a good design but have clear proof and accurate documentation that shows that quality and good design principles were designed in from the beginning." [9]. This feedback is typical of what manufacturers tell us after we have assessed their SIL certified device, which reinforces the perception that certification may be focussed on compliance and often does not explore the possible weaknesses with the devices.

## 6 A COMBINED APPROACH

Process-based/standards-compliance approaches are an important part of any safety justification, as they consider that adequate practices were followed, including design, development, quality assurance, configuration management and manufacturing. However, given the potential limitations of process-based approaches to justification, we suggest a combined approach that explicitly considers demonstration of the correct behaviour of the device in the justification. In this section, we consider process-based approaches in general, and do not restrict ourselves to the specific case where the standards compliance "is given" through certification. In fact, it assumes in several places that information about the quality assurance and development processes are accessible to those performing the justification.

The strategy triangle in Figure 2 [10] identifies three key aspects that are generally relevant in a safety justification.

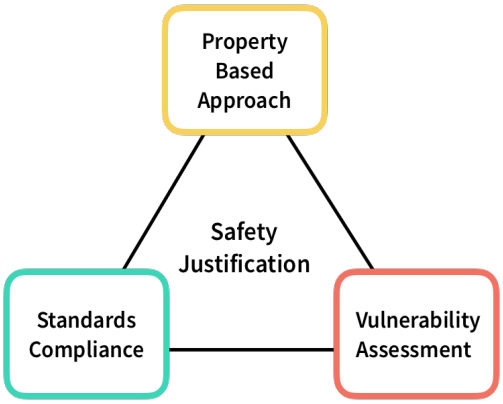

Figure 2. The strategy triangle of justification

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

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

Assessment of the behaviour of the device can provide validation of the development process, as well as evidence for the absence of faults and consequently increased confidence that the device achieves its reliability targets. In the following subsections, we discuss some of the ways in which different aspects of the strategy triangle can complement each other to provide a sound safety justification where an approach based only on one aspect may fall short.

## 6.1 Understanding

The IAEA report on software dependability [11] lists a number of principles for the assessment of software dependability. They include the need to understand the intended and unintended behaviour of the system, “including adverse unintended consequences under conditions of failure”.

Justification that the development process is well-structured and follows relevant good practice provides some confidence that there are no undocumented or unintentional behaviours of the device. However, these behaviours are often not explicitly considered during a compliance assessment, in particular vulnerabilities or potential weaknesses in a device or of the underlying technologies that would need to be mitigated.

Potential weaknesses in the development process that are identified during the assessment can be used to inform testing and behaviour-based justification, by identifying components or aspects of functionality where there is less confidence that the device is fault-free and exhibits the correct behaviour. Focused testing and analysis on these areas can enhance a process-based justification by demonstrating that these weaknesses do not compromise the safety of the device.

COTS devices are not developed specifically for the intended application in a NPP, and so testing during development will be across the full range of inputs and configurations for the device. By detailed analysis of test results, and often by performing further testing covering all configurations and inputs

expected during operation, including failure modes, a complete assessment of the behaviour of the device can provide a more detailed understanding of the hazards and their impact on the plant. This justification also provides validation that the device meets the requirements of the application.

## 6.2 Configuration management

A thorough configuration management process, supported by certification or other assessment of the process, can complement a behaviour-based approach to justification.

The evidence supporting a behaviour-based justification approach consists primarily of tests or other analyses performed on the device to be deployed. Updates to a device, made before deployment as a result of issues detected during qualification, or made throughout the lifetime of the device in response to faults identified during operation, have the potential to alter the behaviour of the device. It is essential that the evidence of the correct behaviour of the device is demonstrated to be applicable to the version being used in the nuclear power plant; a thorough and consistently followed configuration management process can support the relevance of this evidence.

A certified configuration management process will produce detailed change records, including impact analyses, for each modification to the device. These records allow the impact of the changes on the justification to be determined, in particular providing justification for which evidence is still applicable, and which tests may need to be repeated or revised. This is an important part of demonstrating that the device can be shown to continue to meet the safety requirements over time.

## 6.3 Justification of older devices

Certification is more challenging, and sometimes not possible, for older devices and systems, even if the device is believed to be of good quality, and has been used for similar applications for many years. Such devices may not have been developed to modern standards, personnel involved in the development may have left the organisation, or documents produced during development may no longer be available. Even newer devices may contain a significant amount of code from, or have other major design similarities with, older devices, which can significantly increase the challenge and cost of certification or other assessments of the development process.

A combination of process-based and behaviour-based approaches may enable the justification of such a device. This combined approach to justification would include an assessment of the development process of the device. The goal of this assessment would not be to demonstrate compliance with a modern standard, but to provide evidence of good practice during development, and to identify areas of weakness or missing evidence compared to current standards and best practice. This assessment would inform a behaviour-based justification, to ensure that behaviour that could be affected by the weaknesses in the development process is adequately addressed by the justification.

## 6.4 Justification of new devices using new technologies or approaches

Digital technologies and associated techniques and approaches are constantly evolving. Standards, however, have long development timeframes and take several years to include new or updated development practices. The flexibility and rigour provided by assurance frameworks that explicitly consider behaviour are enablers for using technologies that have not yet been adopted by published standards. One such example was the approach taken to justify a FPGA-based system before standards for FPGAs had been published [12], but this flexibility is often required, for example, when development processes follow Agile approaches, new verification techniques and tools are deployed or approaches using machine learning or AI.

## 7 CONCLUSIONS

In this paper we discussed the safety justification of COTS embedded digital devices and, in particular, the role of process-based/standards-compliance approaches including certification in such justification. We identified a number of pitfalls related to such approaches and we suggested a strategy that combines process compliance with explicit consideration of the behaviour of the devices. The approach suggested is consistent with that described in the IAEA document on smart devices [10].

Although the possible issues specifically related to certification (discussed in Section 5) will not be addressed by such a combined approach, the risks related to those issues can partially be mitigated by explicitly seeking evidence to support the behaviour of the device which, in some cases where less onerous integrity is required, may be justified to be sufficient.

## 8 ACKNOWLEDGMENTS

We thank colleagues at Adelard for many discussions on these topics.

## 9 REFERENCES

1. P Bishop, R Bloomfield and S Guerra, "The future of goal-based assurance cases", *Proceedings of Workshop on Assurance Cases, supplemental volume of the 2004 International Conference on Dependable Systems and Networks*, pp. 390-395, Florence, Italy, June 2004.
2. International Electrotechnical Commission, IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, 2010.
3. International Electrotechnical Commission, IEC 60880 Nuclear Power Plants: Instrumentation and Control Systems Important to Safety - Software Aspects for Computer Based Systems Performing Category A Functions, 2006.
4. S Guerra and G Fletcher, "Overview of Approaches to the Use and Licensing of COTS Digital Devices in Safety Critical Industries", *12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2021)*, 2021.
5. A Summers, "IEC 61508 Product Approvals Veering Off Course" https://www.controlglobal.com/articles/2008/187/ (2008)
6. R Bloomfield and S Guerra, "Process Modelling to Support Dependability Arguments", *Proceedings of the International Conference on Dependable Systems and Networks, DSN 2002*, Washington, DC, USA, June 2002.
7. P Bishop and R Bloomfield, "A Conservative Theory for Long Term Reliability Growth Prediction", *IEEE Trans. Reliability*, **vol 45 no. 4**, pp. 550-560 (1996).
8. R Bloomfield, B Littlewood and D Wright. "Confidence: Its Role in Dependability Cases for Risk Assessment", *37th International Conference on Dependable Systems and Networks,* UK, 2007.
9. E Saopraseuth, N Wienhold, E Butler, S Guerra and H Khlaaf, "Emphasis Class 1 and Class 2 Assessment of Rosemount Pressure and Temperature Transmitters", *11th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2019)*, USA, 2019.
10. "Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for Use in Nuclear Power Plant Applications". IAEA Nuclear Energy Series NR-T-3.31, 2020.

11. “Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plants”. IAEA Nuclear Energy Series NR-T-3.27, 2018.
12. S Guerra and D Sheridan, “Justification of an FPGA-based System Performing a Category C Function: Development of the Approach and Application to a Case Study”, *8th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2012)*, 2012.