Office for Nuclear Regulation

Regulatory Expectations for the Justification of COTS Components in the UK

Tim Parkes ONR

19 May 2022

Contents

Background - UK Regulatory Regime

UK Health and Safety Legislation places a legal duty on duty holders to reduce risks to both workers and the public “so far as is reasonably practicable” (SFAIRP).

HSE and ONR guidance generally uses the term ‘as low as reasonably practicable’ (ALARP) as a convenient means to express the legal duty to reduce risks SFAIRP. The terms ALARP and SFAIRP are interchangeable and require the same tests to be applied.

Nuclear regulation in the UK therefore operates under a ‘goal-setting’, as opposed to prescriptive.

UK Regulatory Regime (Cont)

Nuclear Site License Condition 23 requires licensees to “in respect of any operation that may affect safety, produce an adequate safety case to demonstrate the safety of that operation and to identify the conditions and limits necessary in the interests of safety.”

The licensee is required to make the justification that operations, and equipment used in carrying out those operations, are safe and that risks are reduced ALARP.

ONR has established its Safety Assessment Principles (SAPs) for use by ONR inspectors when assessing safety cases for nuclear facilities/activities. These are supported by a suite of Technical Assessment Guides (TAGs), setting out ONR’s expectations to further assist inspectors in their technical assessment work in support of making regulatory judgements and decisions.

Justification of Computer Based Safety Systems

ONR SAP ESS.27:

Engineering principles: safety systems	Computer-based safety systems	ESS.27
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.		

Justification of Computer Based Safety Systems (Cont)

Justification should follow a multi-legged approach comprising the following:

- Production excellence: a demonstration of excellence in all aspects of production from the initial specification through to the finally commissioned system; and
- Independent confidence building measures: confidence gained through the application of independently conducted, diverse from production, techniques and methods used to assess the system software and hardware.

A graded approach to justification, with levels of being rigour proportionate to the safety significance of the system (e.g. based on safety function categorisation) is expected.

Justification of Computer Based Safety Systems (Cont)

Production Excellence

(a) thorough application of technical design practice consistent with current accepted standards for the development of software for computer-based safety systems;

(b) implementation of a modern standards quality management system; and

(c) application of a comprehensive testing programme formulated to check every system function, including:

(i) prior to installation on site, the verification of all phases of the system production process and the validation of the integrated system against its specification by persons not involved in the specification and design activities;

(ii) following installation on site, a demonstration that the safety system, in conjunction with the plant, performs in accordance with its specification. This demonstration should be devised by persons not involved in the system's specification, design or manufacture; and

(iii) a programme of dynamic testing, applied to the complete system to demonstrate that the system is functioning as intended.

Justification of Computer Based Safety Systems (Cont)

Independent Confidence Building

(a) complete, and preferably diverse, checking of the finally validated production software by a team that is independent of the system's suppliers, including:

(i) independent product checking that provides a searching analysis of the final system;

(ii) independent checking of the design and production processes, including the activities undertaken to confirm the realisation of the design intent; and

(b) independent assessment of the comprehensive testing programme covering the full scope of the test activities.

Sources of RGP

Some key sources of guidance informing ONR's expectations (not an exhaustive list):

ONR SAPs https://www.onr.org.uk/saps/saps2014.pdf

TAG046 Computer Based Safety Systems (onr.org.uk)

Licensing of safety critical software for nuclear reactors – Common position of international nuclear regulators and authorised technical support organisations. www.onr.org.uk/software.pdf

IAEA SSG-39 Design of Instrumentation and Control Systems for Nuclear Power Plants | IAEA

Sources of RGP (Cont)

IEC 61508:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems.

IEC 61513:2013. Nuclear power plants - Instrumentation and control systems important to safety – General requirements for systems

IEC 61226:2009. Classification of instrumentation and control functions.

IEC 60880:2009. Software aspects for computer-based systems performing category A functions.

IEC 62138:2009 Software aspects for computer-based systems performing category B or C functions

IEC 62566:2012 Development of HDL-programmed integrated circuits for systems performing category A functions

IEC 60987:2015 Hardware design requirements for computer-based systems

Justification of COTS ‘Smart’ Components

From TAG046:

“Smart devices are instruments, sensors, actuators or other previously electromechanical components (e.g. relays, positioners and controllers), whose functionality is limited and which feature built-in intelligence, in the form of a microprocessor or HDL-programmed device, to help perform its function. An important distinction between smart devices and other computer-based systems is that the end user cannot modify or add device functionality in any way, though they can usually perform limited configuration. Such devices are still considered as computer-based systems and therefore their use in safety or safety related applications should be justified according to SAP ESS.27.”

Justification of COTS ‘Smart’ Components (Cont)

A key difference between the justification of COTS smart devices as opposed to bespoke systems is the fact that much of the evidence required to underpin an assessment is contained in manufacturer’s commercially sensitive intellectual property.

The expectation is that this evidence is available to the licensee’s assessors in order to inform the assessment. This often requires commercial and non-disclosure agreements being established.

In general COTS components are developed for general industrial applications and are unlikely to have been specifically developed to nuclear standards. The established approach in the UK is for production excellence to be assessed against IEC 61508.

Justification of COTS ‘Smart’ Components (Cont)

Any gaps or weaknesses identified during the production excellence assessment need to be addressed in order to maintain confidence in the fitness for purpose of the device.

If the gap is not considered a significant detriment to the overall justification it may be possible to mitigate this through other evidence viewed as part of the assessment. In such cases the mitigation should be supported by a justification of why the gap is not considered to be significant, and how the mitigating evidence is judged to be adequate.

Compensating activities will be required to address more significant gaps in production excellence. These cannot be generically defined as the specific activity will depend on both the nature and significance of the gap. In some cases the compensating activity may require action by the device manufacturer to address the gap.

Justification of COTS ‘Smart’ Components (Cont)

The independent confidence building measures supporting the justification should be selected once technical details of the device (e.g. architecture, language(s), technology, techniques employed during development) are known – this may not be until after production excellence assessment has commenced.

Independent confidence building measures should be diverse to those employed during device development and should be conducted independently of the manufacturer.

For components being justified for use in Class 1 or Class 2 applications the initial expectation is that the source code will be subject to static and or dynamic analysis as part of independent confidence building. This may not be required for Class 3 components.

As ever, the ALARP principle applies and the appropriateness (and ‘reasonable practicability’) of the chosen measures should be justified.

Justification of COTS ‘Smart’ Components (Cont)

The nature of COTS smart devices is that they can often be used in a broad range of applications. It is therefore important that a safety justification contains an assessment of the device’s suitability for the target application.

‘Generic’ justifications that allow devices to be used in a range of applications may be acceptable. In such cases any restrictions, constraints or limitations on use should be clearly specified.

Use of Third- Party Certifications to Support Justification

For low integrity components it may be acceptable for information published by accredited independent test houses to support a justification, either supporting aspects of the production excellence argument or as an independent confidence building measure.

However, licensees would be expected to assess the suitability of the available information and the underpinning evidence.

The process used by the independent test house, including the standards against which the assessment was conducted, should be documented as should any limitations placed on the use of the device.

Specifically, the licensee should determine whether the information is applicable to the proposed application and whether the methods applied are equivalent to established production excellence assessment methods.