Office for
Nuclear Regulation

Challenges of licensing COTS digital components

Mark Bowell, ONR, UK

22 October 2019

Key features

- Increased functionality compared to non-smart equivalent
  - eg signal processing, communications, diagnostics
- Additional complexity
  - Challenges to justification and testability
- Multiple functions
  - Potential to interfere with performance between primary and ancilliary functions
- Introduces need for consideration of systematic failure
  - Additional risk of common cause failure
- Version control
  - Impact on obsolescence management
- Cyber security
  - New vulnerabilities

Key challenges

- Identification in packaged equipment
- Engagement with manufacturer / IP owner
    - Access to documentation, processes and source code can be problematic
- Generic justification vs specific justification
    - The justification needs to consider the specific application

UK approach

- Claims arguments evidence approach for the justification
  - Typical challenges in the articulation of the arguments and availability of suitable evidence
- Limited reliance on certificates as main source of justification
  - May provide some additional confidence
- Graded approach using safety classes (IEC 61226)
  - Linked to IEC 61508 safety integrity levels that align with ONR TAG 3 on safety systems

Use in the UK

- Applications in existing facilities
  - Typically at lower safety classes
  - Some sharing of pre-qualification database of generic justifications between licensees
- Applications for new build
  - Significant number of smart devices proposed during generic design assessments
  - Proposed use at higher safety classes
  - Impact on the security case

UK Relevant Good Practice

- ONR assessment guidance, eg safety assessment principles ESS.27, technical assessment guide 46
- Standards produced by standards making organisations, eg IAEA SSG-39, IAEA NP-T-3.27, IEC 61226, IEC 61508
- Chapters 1.4 (pre-existing software), 1.15 (smart sensors and actuators) and 1.17 (third party certification) of “Licensing of safety critical software for nuclear reactors: Common position of international nuclear regulators and authorised technical support organisations (Revision 2018)”
- Guidance and tools agreed by both ONR and licensees, produced by research funded by the control and instrumentation nuclear industry forum (CINIF)
- Well defined and established standard practice adopted by licensees

Application of ESS.27 to smart devices

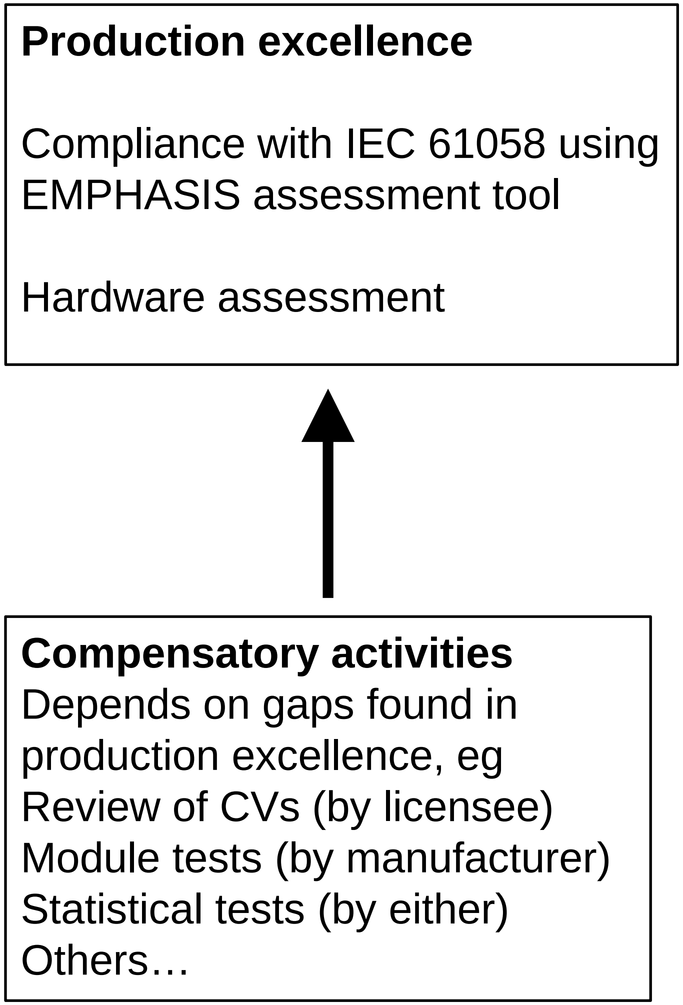
ESS.27 states:

"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."

Associated guidance paragraphs include:

- The rigour of the standards and practices applied should be commensurate with the level of reliability required. The standards and practices should demonstrate 'production excellence' and, through the application of 'confidence-building' measures, provide proportional confidence in the final design.
- 'Production excellence' is a demonstration of excellence in all aspects of production from the initial specification through to the finally commissioned system. If weaknesses are identified in the production process, compensating measures should be applied to address these.
- Independent 'confidence-building' should provide an independent and thorough assessment of the safety system's fitness for purpose.

Application of ESS.27 to smart devices



Production excellence

Compliance with IEC 61058 using EMPHASIS assessment tool

Hardware assessment

Compensatory activities

Depends on gaps found in production excellence, eg

Review of CVs (by licensee)

Module tests (by manufacturer)

Statistical tests (by either)

Others…

Independent confidence building measures

Graded approach based on:

Type testing

Examination, maintenance, inspection and test proposals and records

Commissioning tests

Hardware reliability analysis

Prior use

Supplier pedigree

Certification

Review of manufacturer’s standards and procedures

Functional safety assessment

Review of tools

Static analysis

Dynamic analysis

Statistical testing

Others…

Requirements for class 3 smart devices

Class determined according to IEC 61226 (IAEA terminology: safety-related systems).

Evidence of production excellence, assessed using EMPHASIS against IEC 61508, including SIL1 techniques. Compensatory measures are permitted where gaps are identified.

Independent confidence building measures (ICBMs) shall include:

- Device type tests
- Examination, inspection, maintenance and testing arrangements
- Hardware failure modes and effects analysis or review of the manufacturer’s reliability calculations
- Commissioning tests
- Data on prior use from reputable sources
- Evidence of manufacturer pedigree

The following ICBMs should also be considered:

- Dynamic analysis of the code
- Statistical testing
- Certification by an independent body
- Independent desk top review and static analysis of the code
- Independent tool review

Requirements for class 2 smart devices

Class determined according to IEC 61226 (IAEA terminology: safety-related systems).

Evidence of production excellence, assessed using EMPHASIS against IEC 61508, including SIL2 techniques. Compensatory measures are permitted where gaps are identified.

Independent confidence building measures (ICBMs) shall include:

- Device type tests
- Examination, inspection, maintenance and testing arrangements
- Hardware failure modes and effects analysis
- Commissioning tests
- Data on prior use from reputable sources
- Evidence of manufacturer pedigree

If there is access to the source code:

- Independent desk top review and static analysis of the code, and
- Dynamic analysis of the code, and
- Statistical testing (if possible with “reasonable effort”)

If there is no access to the source code:

- Statistical testing

The following ICBMs should also be considered:

- Certification by an independent body
- Independent functional safety assessment
- Independent tool review

Requirements for class 1 smart devices

Class determined according to IEC 61226 (IAEA terminology: safety systems).

Evidence of production excellence, assessed using EMPHASIS against IEC 61508, including SIL3 or SIL4 techniques, depending on the associated reliability claim. Compensatory measures are permitted where gaps are identified but will be difficult to identify because many techniques are already mandatory ICBMs.

Independent confidence building measures (ICBMs) shall include:

- Device type tests
- Examination, inspection, maintenance and testing arrangements
- Hardware failure modes and effects analysis
- Commissioning tests
- Data on prior use from reputable sources
- Evidence of manufacturer pedigree
- Independent desk top review and static analysis of the code
- Dynamic analysis of the code
- Statistical testing
- Certification by an independent body
- Independent functional safety assessment
- Independent tool review

Third party certification

- A certificate with no supporting detail or evidence can be considered close to useless.
- The licensee and ONR require access to a detailed report providing sufficient evidence of the assertions made.
- There are substantial aspects of the safety demonstration specific to the application that cannot be foreseen and addressed by a generic certification.
- Certification should not replace product evidence and, in general, should not replace process evidence either. Instead it should be an efficient means of ensuring that appropriate evidence is available for assessment. This requires detail and transparency in the certification report.

Certification experience

Certificates can obscure the scope of the assessment, for example

- IEC 61058 compliance is claimed to a particular SIL, but in fact only parts 1 and 2 have been applied and the software ignored
- Software is declared in scope but this is addressed only through an informal proven in use argument
- A range of products is quoted but actually only one particular model within that range was assessed
- The product can carry out different safety functions with different hardware/software configurations but the assessment considered only a subset of the available functionality
- Version updates are ignored, ie an assessment of one version is considered applicable to all versions before or since

Office for
Nuclear Regulation

Certification experience

An assertion of compliance to a particular requirement can have a large variation in the level of scrutiny, for example

- A claim for compliance to quality standards (ISO 9000) applies only to sales and not to development
- The assessor checked that a process existed but didn’t check for the outputs
- The assessor checked that particular documents existed but didn’t sample the contents
- Techniques with broad titles (eg “static analysis) have no benchmark for judging applicability or adequacy
- It is unclear how technique requirements (eg breadth, coverage and rigour) are graded for safety integrity level
- The assessment relied entirely on the manufacturer’s process rather than carrying out independent tests
- Shortfalls or non-compliances are identified but are then ignored or insufficiently justified in higher level conclusions