ONR GUIDE			
Computer Based Safety Systems			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-046 Revision 6		
Date Issued:	April 2019	**Review Date:**	Oct 2023
Approved by:	Steve Frost	E,C&I Professional Lead	
Record Reference:	CM9 Folder 1.1.3.978. (2020/261582)		
Revision commentary:	Rev 5: Routine Update Rev 6: Updated Review Period		

TABLE OF CONTENTS

1. INTRODUCTION 2
2. PURPOSE AND SCOPE 2
3. RELATIONSHIP TO SAPS, WENRA REFERENCE LEVELS AND IAEA SAFETY STANDARDS ADDRESSED 3
4. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION 5
5. ADVICE TO ASSESSORS 6
6. REFERENCES 12
7. APPENDIX 1 LIST OF SUPPORTING PRINCIPLES 15
8. APPENDIX 2 ABBREVIATIONS AND GLOSSARY 18
9. APPENDIX 3 TECHNICAL GUIDANCE FOR ASSESSING SOFTWARE ASPECTS OF COMPUTER BASED SYSTEMS IMPORTANT TO SAFTEY 21
10. APPENDIX 4 SOFTWARE SUBSTANTIATION OF COMPUTER BASED SYSTEMS IMPORTANT TO SAFETY 30
11. APPENDIX 5 USE OF DIVERSE COMPUTER BASED SYSTEMS IMPORTANT TO SAFETY 36
12. APPENDIX 6 CYBER SECURITY OF COMPUTER BASED SYSTEMS IMPORTANT TO SAFETY 38
13. APPENDIX 7 QUALIFICATION OF SOFTWARE TOOLS 45
14. APPENDIX 8 EXPECTATIONS FOR THE JUSTIFICATION OF COMMERCIAL OFF THE SHELF SMART DEVICES 46

Published 04/19

1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established its safety assessment principles (SAPs) which apply to the assessment by ONR of safety cases for nuclear facilities that may be operated by potential licensees, existing licensees, or other duty-holders. The principles presented in the SAPs are supported by a suite of guides to further assist in technical assessment work in support of making regulatory judgements and decisions. This technical assessment guide (TAG) is one of these guides.

2. PURPOSE AND SCOPE

2.1 The purpose of this TAG is to provide additional guidance for applying safety assessment principle (SAP) [Ref. 1] ESS.27. ESS.27 presents the elements of a multi-legged procedure that should be used to demonstrate the adequacy of a computer based safety system.

2.2 This TAG expands upon the guidance provided by ESS.27 to assist ONR assessors in applying judgement when assessing the adequacy of safety cases for computer-based safety systems. Technical assessment guide NS-TAST-GD-003 [Ref. 2] addresses safety systems in general. This SAP is supported by other general and plant specific SAPs. Where a computer based safety system is used, because the technology is inherently complex and not amenable to traditional methods of reliability assessment, SAP ERL.1 and SAP paragraph 191 should also be applied.

Engineering principles: reliability claims	Form of claims	ERL.1
The reliability claimed for any structure, system or component should take into account its novelty, experience relevant to its proposed environment, and uncertainties in operating and fault conditions, physical data and design methods.		

Paragraph 191 states:

Where reliability data is unavailable, the demonstration should be based on a case-by-case analysis and include:

(a) a comprehensive examination of all the relevant scientific and technical issues;
(b) a review of precedents set under comparable circumstances in the past;
(c) where warranted, eg for complex items, an independent third-party assessment; and
(d) periodic review of further developments in technical information, precedent and relevant good practice.

2.3 The purpose of SAP ESS.27 and this TAG is to aid the assessment of computer based safety systems. However, in the absence of any other guidance, the principles of the TAG may be applicable to computer based safety related systems. Where specific expectations for safety related systems are defined, this is highlighted in the relevant section. For example, paragraphs 5.10, 5.11, 9.25, and 9.59 refer specifically to safety related systems.

2.4 Safety systems and safety related systems are distinct in their purpose; the ONR definitions of each are provided in the glossary of this TAG, as well as Refs 2 and 3.

2.5 This TAG also uses the term ‘computer based systems important to safety’ (CBSIS). A system important to safety is considered to be a safety system or safety related system that implements safety functions at categories A to C, and hence is assigned a

corresponding class 1 to 3. The term CBSIS therefore encompasses both safety systems and safety related systems that are computer based.

2.6 The safety integrity requirements of safety systems and safety related systems depend on the risk reduction required, in respect of the scale of the hazard and the presence of other independent systems performing the same function. So there is no explicit linkage between functionality and category or class of a single particular system. Hence, any CBSIS may be safety class 1, 2 or 3 and its designation as either a safety system or safety related system should not be taken to imply any particular level of safety integrity. The approach to categorisation of safety functions and classification of structures, systems and components is defined by SAPs ECS.1 and ECS.2; see NS-TAST-GD-094 [Ref. 4] for further guidance.

2.7 The guidance given in this document also applies to systems that are designed using hardware description languages (HDLs), as the complexity of HDL programmed technologies and the associated design process is similar to that of more traditional computer based safety systems. Therefore, for the purposes of assessment, systems incorporating HDL programmed technology should be treated in the same way as software based systems. IEC 62566 [Ref. 14] defines requirements for use of HDL programmed technology in nuclear plants.

2.8 Comments on this guide, and suggestions for future revisions, should be recorded using the appropriate review form (available on HOW2) and stored in the appropriate electronic record folder.

3. RELATIONSHIP TO SAPS, WENRA REFERENCE LEVELS AND IAEA SAFETY STANDARDS ADDRESSED

KEY SAFETY ASSESSMENT PRINCIPLES

3.1 There is only one key principle that deals specifically with this topic, ESS.27. It is, however, underpinned by two more general principles, ERL.1 and ERL.2. The content of ESS.27 and its explanatory paragraphs are reproduced below for ease of reference.

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.		

The complexity of computer-based safety systems means they are usually not amenable to traditional methods of reliability assessment. This principle therefore provides for elements of a procedure to demonstrate the adequacy of such systems. The safety demonstration for hardware elements of these systems should include the items listed in paragraph 416.

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 proportionate 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. It should include the following elements:

(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.

Independent 'confidence-building' should provide an independent and thorough assessment of the safety system's fitness for purpose. This should include the following elements:

(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.

When demonstrating 'production excellence' and applying 'confidence-building' measures for computer-based safety systems:

- *verification is the process of ensuring that a phase in the system lifecycle meets the requirements imposed on it by the previous phase; and*
- *validation is the process of testing and evaluation of the integrated computer system (hardware and software) to ensure compliance with functional, performance and interface requirements.*

Statistical testing is highly recommended as an approach for demonstrating the numerical reliability of computer-based safety systems. Such testing may play a role in both 'production excellence' and 'confidence-building' aspects of the safety justification.

If 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.

SUPPORTING PRINCIPLES

3.2 The key principle is supported by a number of other principles of relevance to computer based safety systems. The SAPs identified in appendix 1 are explicitly referenced in the main body of this TAG. Appendix 3 is informed by additional SAPs, eg from the ESS and ESR series. NS-TAST-GD-003 'Safety systems' [Ref. 2] specifically addresses the safety system SAPS (ie ESS.1 to ESS.27).

3.3 SAP FP.4 requires duty-holders to "…demonstrate effective understanding and control of the hazards posed by a site through a comprehensive and systematic process of safety assessment." This technical assessment guide is an interpretation of how FP.4 could be satisfied through the development of a suitable and sufficient safety case for CBSIS. Further guidance on the production of safety cases is provided in NS-TAST-GD-051 'The purpose, content and scope of safety cases' [Ref. 5].

WENRA REFERENCE LEVELS

3.4 There is one section of the WENRA safety reference levels for existing reactors [Ref.6] that is directly relevant to the use of computer based safety systems (ie Issue E: Design basis envelope for existing reactors, subclause E10.10). The software aspects of subclause E10.10 are implemented through application of SAP ESS.27 and the guidance shown in this TAG (other SAPs address hardware aspects). Subclause E10.10 from Ref.6 (September 2014 revision) is as follows [with references to the paragraphs in this TAG where each requirement is discussed].

Computer based systems used in a protection system, shall fulfil the following requirements:

- *the highest quality of and best practices for hardware and software shall be used;* [paragraphs 5.21 to 5.28]
- *the whole development process, including control, testing and commissioning of design changes, shall be systematically documented and reviewed;* [paragraphs 5.21 to 5.28;]
- *in order to confirm confidence in the reliability of the computer based systems, an assessment of the computer based system by expert personnel independent of the designers and suppliers shall be undertaken* [paragraphs 5.29 to 5.37]*; and*
- *where the necessary integrity of the system cannot be demonstrated with a high level of confidence, a diverse means of ensuring fulfilment of the protection functions shall be provided.* [paragraphs 5.1 to 5.20 and appendix 5]

References to 'best practices' in the WENRA reference levels should be interpreted in a regulatory context as meaning 'relevant good practice'.

4. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

4.1 Licence Condition (LC) 14 (safety documentation), LC15 (periodic review), LC17 (management systems), LC20 (modification to design of plant under construction), LC22 (modification or experiment on existing plant), LC27 (safety mechanisms, devices and circuits) and LC28 (examination, inspection maintenance and testing) are all relevant.

4.2 Computer based safety systems that implement both nuclear and environmental protection functions may also be expected to comply with the Environment Agency's RSR environmental principles.

5. ADVICE TO ASSESSORS

GENERAL

5.1 SAP ESS.21 – Reliability – states that the design of safety systems should avoid complexity, apply a failsafe approach and incorporate means of revealing internal faults at the time of their occurrence. The complexity of computer-based safety systems means they are more vulnerable to systematic failure, including cyber-attack, but there may be safety benefits to be realised from features such as diagnostics. The need to use computer based safety systems should be justified, since their inherent complexity means that demonstrating adequate safety is more difficult. It is important that this demonstration is proportionate; therefore assessors should use safety function(s) categorisation and the corresponding safety system's classification to inform regulatory expectations.

5.2 ONR's expectation is that the design of computer based systems will seek to minimise complexity, both in the functionality of the system and in its implementation. No feature of a CBSIS should be detrimental to safety and the impact of any added complexity justified. This complexity should not compromise any other design principles (for example, independence, redundancy, diversity).

5.3 Where diverse safety systems are required to implement category A safety functions and one is computer based, one of the other safety systems should be provided using a non-computer based system (EKP.3, EDR.2 and EDR.3). Assessors should be aware that this can also apply to the implementation of category B safety functions. The topic of diversity is addressed in appendix 5.

5.4 The advice presented below outlines the multi-legged procedure used in this TAG. This procedure comprises two components:

- Production excellence: a demonstration of excellence in the production of the computer based system important to safety to minimise the likelihood of the introduction of latent systematic faults in the software development process; 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.

5.5 This TAG also provides information on software development, software reliability, CBSIS diversity, cyber security and the qualification of software tools.

5.6 For any production excellence or independent confidence building element of the multi-legged procedure, the duty-holder may not be able to demonstrate full compliance with relevant standards, guidance or relevant good practice. Where this is the case, duty-holders need to justify the approach taken and demonstrate that the safety objectives are still met. If necessary, duty-holders should also demonstrate that any consequences of the non-application of relevant standards or relevant good practice are compensated for suitably by other measures. As a result of the challenges in substantiating CBSIS, the multi-legged approach should include a justification of the duty-holder's confidence in the system, and why the implementation of additional measures is not considered to be reasonably practicable.

5.7 Assessors should ensure that the duty-holder's safety management system (MS.1 to MS.4) is adequate for the needs of producing and building confidence in a CBSIS. The organisational arrangements should clearly define roles and responsibilities. The competence of those involved should be demonstrated and adequately managed [Ref. 17].

5.8 In general, the reliability claim on systems incorporating computer based or HDL programmed technology should be limited to the order of 3E-1 probability of failure per demand (pfd), unless a sufficiently robust justification can demonstrate the appropriateness of a lower value. The application of SAP ESS.27 to CBSIS is a means of demonstrating the appropriateness of a lower value. The value of 3E-1 is used to ensure that claims of the region of 1E-1 pfd (e.g. those that fall under the requirements of IEC 61508 [Ref. 9]) are clearly within the boundary for ESS.27 requirements.

5.9 International relevant good practice recognises the difficulty in quantifying software reliability. IEC 61513 [Ref. 10] states that software reliability "…is usually a qualitative measure." For this reason, substantiation of software elements of CBSIS should be primarily based on deterministic methods but may be supported by quantitative methods (eg statistical testing) where appropriate.

5.10 Assessors should be wary of attempts to reduce the frequency of a fault sequence through risk reduction claims involving multiple low integrity computer based safety related systems (ERL.4). The concern is that inappropriately large amounts of credit may be claimed in total by combining several small amounts of risk reduction and the potential for common mode, systematic failure of software elements can be difficult to determine. This could result in the combined risk reduction having a large impact on the assumed demand frequency for any protection functions (called the initiating event frequency) and may inappropriately skew the categorisation of the safety function and / or classification of the safety system requirement. Although such low integrity systems may have a functional safety role, they are usually embedded in other large systems that are classified as safety related. The claim for each of the contributing risk reduction elements of safety related systems taken together in a given fault sequence should be no better than of the order of 1E-1 pfd. If this is not the case, the assessor should consider whether it would be more appropriate for the duty-holder to treat each so-called safety related system as though it is a safety system, and therefore apply ESS.27.

5.11 Assessors should consider whether it is desirable to also apply ESS.27 to computer based safety related systems such as control systems. For each separate computer based safety related system that requires a reliability claim of lower than 3E-1 failures per year, paragraphs 5.8 and 5.10 above apply. Expectations for safety related systems in general are addressed in NS-TAST-GD-031 'Safety Related Systems and Instrumentation' [Ref. 3].

5.12 With current techniques, and taking all relevant factors (see appendix 4) such as complexity into account, a probability of 1E-4 pfd is considered to be the best (minimum) that can justifiably be claimed for any single computer based safety system [Refs 7, 8, 11 and 16, EDR.3 (paragraph 185), ERL.1 and ERL.2]. Future advances in software engineering techniques could lead to a situation where an adequate case could be made for a lower figure. This case would need to be subject to assessment.

5.13 For a nuclear facility's probabilistic safety analysis (PSA), it is typical for best estimate figures to be used (see appendix 4). Unless otherwise stated, all other references to failure probabilities in this document should be taken to be conservatively estimated, meaning a confidence level of 95-99%. Where 95-99% confidence testing is used, the PSA can use a corresponding lower reliability figure when modelling the performance of CBSIS.

MULTI-LEGGED PROCEDURE

5.14 ESS.27 [Ref. 1] has two key legs: production excellence demonstration and independent confidence building. The philosophy of this multi-legged procedure is that substantiation of the system centres on both a demonstration of high quality production and an independent searching examination of the system's fitness for purpose that reveals no significant faults or errors that compromise the system's required safety performance.

5.15 The techniques used by the duty-holder to demonstrate a CBSIS's fitness for purpose should be appropriate for the class and application of the system. Duty-holders should consider and justify the suitability of the selection of techniques used to substantiate the system. As the integrity requirements become less onerous, proportionate gradation should be used in the application of general principles, ie with due consideration given to the nuclear safety significance of the functions being carried out. This graded approach is informed by the category of each of the functions implemented by the system, the system classification and its integrity requirements (required by SAPs ECS.1, ECS.2 and ECS.3). Application of the appropriate standards [Refs 9, 12, 13 and 14] ensures effective proportionality. Further information on the safety demonstration of safety critical software for nuclear reactors is contained in section 1.1 (safety demonstration) of Ref. 8.

5.16 Where the independent confidence building measures reveal a significant number of faults, the quality of the production process is brought into question and the argument for adequacy of the system is weakened. Any remedial action must go further than error correction; the duty-holder must restore confidence in the system by thoroughly re-examining the production process to establish that similar errors have not arisen elsewhere. The duty-holder must then demonstrate that the corrected system is capable of satisfying all relevant safety functional requirements by a sufficient repetition of the independent confidence building measures.

5.17 Judgement will be required in determining the detailed scope and rigour of the software based justification elements (including applicable techniques and measures). Guidance may be obtained from standards [Ref. 9, 12 and 13] on the techniques and measures used to provide confidence in the CBSIS appropriate to its class, and this topic is discussed further in appendix 4. The procedure should be underpinned by a comprehensive review of the relevant factors taking account of past precedents (required by SAP ERL.1).

5.18 When considering past precedents, assessors should note that the expectation for particular techniques and measures in the production excellence and independent confidence building legs may evolve. In addition, increasing the strength of one leg might lead to a reduction in requirements for the other, but both legs need to be sound.

5.19 Where a bespoke CBSIS is being assessed, early discussion on the adequacy of the outline safety case for the system, including the applicable techniques and measures to be used for their substantiation, should be sought with the duty-holder. The objective should be to fix the status of the agreed techniques and measures for the project's duration. Nevertheless, if some relevant technology or additional safety measure later emerges with significant potential to improve real plant safety, then its adoption should be considered in terms of 'reasonable practicability'.

5.20 Pre-developed items, such as commercial off the shelf (COTS) smart devices and platforms, should be adequately substantiated. Any non-safety functions should be shown not to compromise the safety functions of the item, either by demonstrating non-interference or by constructing a safety demonstration that considers the non-safety functions as if they are safety functions. Substantiation of pre-developed items requires significant information to be provided by the manufacturer / supplier in order

for a duty-holder to demonstrate production excellence and arrange the required independent confidence building measures. For example, static analysis requires access to code. To enable this, duty-holders will need cooperation from the supply chain. Duty-holders should also develop strategies for managing maintenance, software / firmware upgrades and obsolescence. Further guidance on the expectations for substantiation of COTS smart devices is provided in appendix 8.

PRODUCTION EXCELLENCE

5.21 *'Production excellence' is a demonstration of excellence in all aspects of production from the initial specification through to the finally commissioned system. It should include the following elements*:

(a) *thorough application of technical design practice consistent with current accepted standards for the development of software for computer based safety systems* e.g. Refs 12 and 13 (ECS.1, ECS.2 and ECS.3);
(b) *implementation of modern standards quality management system* (ECS.3 and 6.16 to 6.18); and
(c) *application of a comprehensive testing programme formulated to check every system function* (ECS.3), *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.*

Text above in *italics* above is taken directly from SAP paragraph 423.

5.22 Production excellence is associated with the design, development, manufacturing and factory acceptance testing of a supplied system. For COTS systems or devices (eg smart devices), this usually relates to the development of the product before being made commercially available. The integration of a COTS product into the application is addressed though an assessment of the product's suitability to the application, and the implementation of independent confidence building measures. Further guidance on expectations for COTS smart devices is provided in appendix 8.

5.23 Production excellence is achieved through the application of relevant good practice at the time of system development to avoid errors, detect and remove those not avoided and provide in-built system tolerance to those not detected (required by SAPs ECS.3 and EDR.1). It is important that unambiguous, comprehensive and verified specifications of the system requirements, covering both system behaviour and requirements for the full system life-cycle, are available from the earliest stages of the production process.

5.24 Although not mandatory, the case for production excellence is greatly assisted by evidence of the systematic, graded application of national and international standards (e.g. Refs 9, 12 and 13), coupled with a case by case justification of any non-compliances.

5.25 It is important that the licensee adequately demonstrates that the system is capable of satisfactory operation in situ through an extensive pre-operational test. During this stage the system will be operational (with frequent testing) while being progressively integrated with other plant items as part of commissioning (required by SAP ECM.1).

5.26 Dynamic testing during the production excellence phase may take the form of statistical testing, provided the operational profile and transients of the final system are known. Generally, however, manufacturers do not conduct formal statistical testing as part of production excellence and hence, for the purposes of this guide, references to dynamic testing in the production excellence leg should not necessarily be interpreted as meaning statistical testing.

5.27 The safety demonstration of hardware elements of CBSIS should take account of relevant standards. In particular, systems classified as either class 1 or class 2 should follow IEC 60987 [Ref. 15]. Class 3 systems should follow IEC 61508 [Ref. 9] as a minimum. In addition, the demonstration should include the following (SAPs paragraph 416 requirements in *italic*):

- *a comprehensive examination of all the relevant scientific and technical issues;*
- *a review of precedents set under comparable circumstances in the past;*
- *an independent third-party assessment in addition to the normal checks and conventional design; and*
- *periodic review of further developments in technical information, precedent and best* (ie informing relevant good) *practice.*

5.28 Should the production excellence assessment identify weaknesses in the production process, compensating activities should be applied to address them. The type of compensating activities will depend on, and should be targeted at, the specific weaknesses found (required by the final explanatory paragraph (427) for ESS.27). Compensating activities should not be confused with the independent confidence building measures. If a particular technique or measure is used as a compensating activity, its application as an independent confidence building measure should be suitably diverse from its use as a compensating activity. Suitable diversity can often be achieved in the same broad category (for example static analysis of source code through use of a different tool).

INDEPENDENT CONFIDENCE BUILDING

5.29 The confidence building leg provides an independent and thorough 'reasonably practicable' assessment of the safety systems' fitness for purpose (required by SAP ERL.1). It should comprise the following elements applied in a graded manner dependent on the class of the system:

(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* including application of static analysis (appendix 4) and other techniques*,*

(ii) *independent checking of the design and production processes including the activities undertaken to confirm the realisation of the design intent* such as interpretation and adequacy of the specification, application and compliance with design specification, methods and standards*; and*

(b) *independent assessment of the comprehensive testing programme, covering the full scope of test activities* (eg assessment of the verification, validation, commissioning and dynamic testing – including statistical testing) including traceability of tests to specification and confirmation that the specification is met*.*

Text above in *italics* is taken directly from SAP paragraph 424.

5.30 The strategy, means and plan for delivery of independent confidence building measures should be determined at the outset of a project.

5.31 Individuals or teams denoted as independent assessors (ie those undertaking the assessment, who are independent from the system supplier and system specification team) should determine and justify their approach and their level of rigour for each task. Wherever reasonably practicable, the independent assessors should employ dissimilar checking methods to those used by the system's supplier and specifier.

5.32 Techniques chosen for the implementation of independent confidence building measures should be demonstrated to be adequate prior to application. New and unproven techniques will need especially comprehensive demonstrations in order to provide confidence that the chosen technique will achieve its intent.

5.33 It is important to stress that the independent confidence building measures should be applied only to the finally delivered product - ie after completion of the manufacturer's verification and validation, including the completion of any compensating activities. The duty-holder may, however, be able to make a case for applying techniques to code that has completed the manufacturer's independent verification.

5.34 Dynamic testing may be part of the independent confidence building measures (eg negative testing, stress testing etc). Statistical testing is a form of dynamic testing used to demonstrate the probability of failure on demand and is informed by statistical considerations. This might mean that many thousands of statistically defined tests are required for confidence in the dependability of the system to be built up (eg of the order of 46,000 tests with no failures for a demonstration of 1E-4 pfd to 99% confidence). See appendix 4 for more details.

5.35 If statistical testing is used in production excellence, then assessors should not expect it to be repeated as an independent confidence building measure. However in such cases, an independent assessment of the adequacy of the statistical testing should be carried out as part of the independent confidence building leg.

5.36 For class 1 systems (and potentially class 2 systems) a justification of the adequacy and rigour of the combination of chosen independent confidence building measures should performed by suitably qualified and experienced persons who are independent to those undertaking the independent confidence building measures. It is acceptable that those undertaking functional safety assessment (as defined in part 1 of IEC 61508 [Ref. 9]) can undertake this assessment of the adequacy. A graded approach to levels of independence, based on the class of the system, should be adopted (also covered in part 1 of IEC 61508).

5.37 The findings of independent assessors and their reconciliation should be reported within the safety case. All reporting of independent confidence building measures, including findings and their reconciliation within the safety case, should be auditable.

TECHNICAL GUIDANCE

5.38 The guidance provided in appendix 3 should be used in conjunction with IAEA guidance on the design of instrumentation and control systems [Ref. 7], Licensing of safety critical software for nuclear reactors – Common position of international nuclear regulators and authorised technical support organisations [Ref. 8], and IEC standards as appropriate (see below). Appendix 3 is applicable to all safety systems and safety related systems containing software falling within the scope of ESS.27. The appendix and Refs 7 and 8 cover the use and validation of pre-existing software, computer security, use of tools, software diversity, safety demonstration and formal methods. Assessors should ensure that the recommendations and guidance of these documents

have been considered. While the references are directed at nuclear power plants much of their content is applicable to other nuclear facilities.

5.39 The multinational design evaluation programme working group on digital instrumentation and control has produced several common positions relating to the use of CBSIS in nuclear power plants [Ref. 18]. The guidance provided in this technical assessment guide should be considered alongside these common positions.

5.40 Further technical guidance can be found in IEC standards as appropriate, such as:

- IEC 60880 [Ref. 12] and IEC 62138 [Ref. 13] (for software aspects);
- IEC 62566 [Ref. 14] (for systems incorporating HDL technology performing category A functions);
- IEC 61508 [Ref. 9] (for grading of techniques and measures for software development – see also appendix 4);
- IEC 61513 [Ref. 10] (general requirements for systems).

The IEC standards apply in particular to the production excellence leg and should be consulted for topics not addressed by the guidance provided by appendix 3, Ref. 7 or Ref. 8. Additionally, IEC 61508 [Ref. 9] should be consulted to assist with selection of appropriate techniques and measures to be applied as independent confidence building measures.

5.41 Technical guidance on cyber security is provided in appendix 6. This guidance has been developed using existing guidance in international standards [Ref. 19] and UK government publications [Refs 20 and 21]. The purpose of appendix 6 is to provide guidance on principles to be considered when assessing cyber security aspects of CBSIS, and in particular considering whether cyber security measures could undermine the system.

6. REFERENCES

1 Safety assessment principles for nuclear facilities. (ONR 2014 Edition Revision 0)

2 NS-TAST-GD-003 Safety systems

3 NS-TAST-GD-031 Safety related systems and instrumentation

4 NS-TAST-GD-094 Categorisation of safety functions and classification of structures, systems and components.

5 NS-TAST-GD-051 The purpose, content and scope of safety cases

6 WENRA safety reference levels for existing reactors, September 2014

7 IAEA Safety Standards, Specific Safety Guide No. SSG-39 - Design of instrumentation and control systems for nuclear power plants 2016

8 Licensing of safety critical software for nuclear reactors – Common position of international nuclear regulators and authorised technical support organisations, Revision 2018. www.onr.org.uk/software.pdf.

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

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

11 IEC 61226:2009. Nuclear power plants - Instrumentation and control systems important to safety – Classification of instrumentation and control functions.

12 IEC 60880:2009. Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions.

13 IEC 62138:2009 Instrumentation and control important for safety — Software aspects for computer-based systems performing category B or C functions

14 IEC 62566:2012 Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions

15 IEC 60987:2015 Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems

16 The use of computers in safety-critical applications - Final report of the study group on the safety of operational computer systems, (HSE 1998) ISBN 0-7176-1620-7

17 Managing competence for safety-related systems (HSE 2007).

18 MDEP DICWG generic common positions:

a. DICWG-01: Treatment of Common Cause Failure Caused by Software within Digital Safety Systems.

b. DICWG-02: Software Tools

c. DICWG-03: Verification and Validation throughout the Life Cycle of Safety Systems Using Digital Computers

d. DICWG-04: Communication Independence

e. DICWG-05: Treatment of Hardware Description Language (HDL) Programmed Devices for Use in Nuclear Safety Systems

f. DICWG-06: Simplicity in Design

g. DICWG-07: Selection and Use of Industrial Digital devices of Limited Functionality (Update of 20 November 2014)

h. DICWG-08: Impact of Cyber Security Features on Digital I&C Safety Systems

i. DICWG-09: Safety Design Principles and Supporting Information for the Overall I&C Architecture

j. DICWG-10 : Hazard Identification and Control for Digital Instrumentation and Control Systems

k. DICWG-11: Digital I&C System Pre-installation and Initial On-site Testing

l. DICWG-12: Use of Automatic Testing in Digital I&C Systems as part of Surveillance Testing

m. DICWG-13: Common Position on Spurious Actuation

19 IEC 27001:2013 Information technology – Security techniques – Information security management systems

20 https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

21 https://www.ncsc.gov.uk/guidance/security-industrial-control-systems

22 IAEA General Safety Requirement Part 2: Leadership and management for safety, GSR Part 2, 2016.

23 IAEA: Technical Report Series No. 397, Quality assurance for software important to safety. 2000.

24 IAEA Safety Guide GS-G-3.1 Application of the management system for facilities and activities, 2005.

25 IAEA Safety Guide GS-G-3.5 The management system for nuclear installations, 2009.

26 NS-TAST-GD-030 Probabilistic Safety Analysis

27 MDEP Common Position Paper CP-DICWG-13 – Common position on spurious actuation

28 IEC 62340 Ed. 1.0 2010 - Nuclear power plants - Instrumentation and control systems important to safety – Requirements to cope with common cause failure (CCF).

29 NUREG/CR-6303 – Method for performing diversity and defence in depth analyses of reactor protection systems

30 Security assessment principles for the civil nuclear industry (ONR 2017 Edition, Version 0)

31 The Nuclear Industries Security Regulations 2003 (NISR)

32 CNS-TAST-GD-7.1 Effective cyber and information risk management

33 CNS-TAST-GD-7.2 Information security

34 CNS-TAST-GD-7.3 Protection of nuclear technology and operations

35 CNS-TAST-GD-7.4 Physical protection of information

36 CNS-TAST-GD-7.5 Preparation for and response to cyber security events

37 IEC 62859:2016 Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity.

38 IEC 62671:2013 Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality

7. APPENDIX 1 LIST OF SUPPORTING PRINCIPLES

Leadership and management for safety	Leadership	MS.1
Directors, managers and leaders at all levels should focus the organisation on achieving and sustaining high standards of safety and on delivering the characteristics of a high reliability organisation.		
Leadership and management for safety	Capable organisation	MS.2
The organisation should have the capability to secure and maintain the safety of its undertakings.		
Leadership and management for safety	Decision making	MS.3
Decisions made at all levels in the organisation affecting safety should be informed, rational, objective, transparent and prudent.		
Leadership and management for safety	Learning	MS.4
5Lessons should be learned from internal and external sources to continually improve leadership, organisational capability, the management system, safety decision making and safety performance.		
Engineering principles: key principles	Defence in depth	EKP.3
Nuclear facilities should be designed and operated so that defence in depth against potentially significant faults or failures is achieved by the provision of multiple independent barriers to fault progression.		
Engineering principles: safety classification and standards	Safety categorisation	ECS.1
The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be identified and then categorised based on their significance with regard to safety.		
Engineering principles: safety classification and standards	Safety classification of structures, systems and components	ECS.2
Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance to safety.		
Engineering principles: safety classification and standards	Codes and standards	ECS.3
Structures, systems and components that are important to safety should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate codes and standards.		

Engineering principles: design for reliability	Failure to safety	EDR.1
Due account should be taken of the need for structures, systems and components to be designed to be inherently safe, or to fail in a safe manner, and potential failure modes should be identified, using a formal analysis where appropriate.		
Engineering principles: design for reliability	Redundancy, diversity and segregation	EDR.2
Redundancy, diversity and segregation should be incorporated as appropriate within the design of structures, systems and components.		
Engineering principles: design for reliability	Common cause failure	EDR.3
Common cause failure (CCF) should be addressed explicitly where a structure, system or component employs redundant or diverse components, measurements or actions to provide high reliability.		
Engineering principles: design for reliability	Single failure criterion	EDR.4
During any normal permissible state of plant availability, no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function.		
Engineering principles: reliability claims	Form of claims	ERL.1
The reliability claimed for any structure, system or component should take into account its novelty, experience relevant to its proposed environment, and uncertainties in operating and fault conditions, physical data and design methods.		
Engineering principles: reliability claims	Measures to achieve reliability	ERL.2
The measures whereby the claimed reliability of systems and components will be achieved in practice should be stated.		
Engineering principles: reliability claims	Margins of conservatism	ERL.4
Where safety-related systems and/or other means are claimed to reduce the frequency of a fault sequence, the safety case should include a margin of conservatism to allow for uncertainties.		
Engineering principles: commissioning	Commission testing	ECM.1
Before operating any facility or process that may affect safety it should be subject to commissioning tests defined in the safety case.		
Engineering principles: safety systems	Faults originating from safety systems	ESS.17
Potential faults originating from within safety systems (eg due to spurious or mal-operation) should be identified and protection against them provided.		

Engineering principles: safety systems	Failure independence	ESS.18
No design basis event should disable a safety system.		
Engineering principles: safety systems	Reliability	ESS.21
The design of safety systems should avoid complexity, apply a failsafe approach and incorporate means of revealing internal faults at the time of their occurrence.		

8. APPENDIX 2 ABBREVIATIONS AND GLOSSARY

ABBREVIATIONS

CBSIS	Computer based system important to safety
COTS	Commercial off the shelf
CS&IA	Cyber security and information assurance
ff	frequency of dangerous failure per year
HDL	Hardware description language
HSE	Health and Safety Executive
IAEA	International Atomic Energy Authority
LC	Licence Condition
MDEP	Multi-national design evaluation programme
NISR	Nuclear Industries Safety Regulations 2003
ONR	Office for Nuclear Regulation
PIE	Postulated initiating event
pfd	probability of failure on demand
PSA	Probabilistic safety analysis
SAP	Safety assessment principle
SIL	Safety integrity level
SNI	Sensitive nuclear information
SyAP	Security assessment principle
TAG	Technical assessment guide
WENRA	Western European Nuclear Regulators Association

GLOSSARY

ANIMATION - A simulation of a specification such that its behaviour can be observed in real time.

APPLICATION SOFTWARE – Software designed to perform a group of coordinated activities to deliver a specific function.

ASSEMBLY LANGUAGE – A computer programming language based on mnemonics which have a one to one correspondence with the computer's instructions. Assembly language is in general a difficult language in which to write computer programs.

CODE – The individual instructions or statements of a computer language.

COMPILER – A computer program used to translate a higher order language program into its machine code equivalent.

COMPUTER BASED SYSTEM IMPORTANT TO SAFETY – A system, either a safety system or a safety related system, that implements safety functions of category A, B or C, and hence is assigned a corresponding class 1, 2 or 3, that incorporates computer based or HDL programmed technology.

DIVERSITY (OF SOFTWARE) – The provision of dissimilar means of achieving the same objective. The introduction of diversity in any aspect of a system or its manufacture/ production will reduce the likelihood of common mode failures. Systems can be considered as having varying degrees of diversity according to the number of these different aspects which have been achieved by dissimilar means. Diversity in software covers the computer instruction set but also the programming language, support software, design, and all staff involved in the life cycle. Where a claim is made that very high reliability has been achieved through software diversity then it must be shown that dissimilar means have been employed in all aspects of the system and its manufacture/production. Any divergence from this should cause the claim to be down-rated.

DEFENSIVE PROGRAMMING – Incorporation of mechanisms into a program that detects and responds in a predetermined safe manner to erroneous program logic.

DEMILITARISED ZONE – Part of a computer network that is protected by physical or logical protection aimed at preventing unauthorised access to systems within this part.

FAULT TOLERANCE – The ability of a software system to operate in a predetermined safe manner in the presence of a limited number of hardware or software faults.

FIRMWARE – Computer programs and data loaded in a class of memory that cannot be dynamically modified by the computer during processing.

HARDWARE – The physical components that make up a computer system.

HARDWARE DESCRIPTION LANGUAGE (HDL) – Language used to formally describe functions and/or the structure of an electronic component.

HDL PROGRAMMED TECHNOLOGY – Use of integrated circuits configured with hardware description languages and related software tools.

HIGH-LEVEL LANGUAGE – A set of instructions for a computer which are more closely related to natural language and therefore can be more easily understood.

IMPLEMENTERS – That organisation or part of an organisation, whose responsibility is to take a design specification and produce an operational finished article. As opposed to the Designers who use the requirements specification to produce a design specification.

INTERRUPT – The process whereby a sequence of instructions is terminated and another sequence is executed. Upon completion of the second set, control is returned to the first set at the point of interruption. This operation is regarded as unsuited to safety related software since parameters can be updated by the interrupting program only to be changed by the interrupted program.

LINKER – A computer program used to create one load module from one or more independently translated object modules by resolving cross references among the object modules and possibly relocating elements.

PEAK DATA LOADS – The maximum rate of data production requiring handling by a system. For example, large amounts of data could require handling during fault conditions.

PLATFORM – The hardware and software (eg operating system) necessary to run application software.

PROGRAM – A set of computer instructions which perform a particular function.

RECURSION – A programming technique where part of a program initiates repeats of itself, so that an outcome is achieved by multiple repetitions.

SAFETY SYSTEM – A system of high safety importance, which acts in response to a fault or potentially dangerous plant condition to protect against a radiological consequence. See paragraph 395 of the SAPs [Ref. 1] for further explanation.

SAFETY RELATED SYSTEM – An item important to safety that is not part of a safety system (IAEA Safety Glossary). Safety-related systems are therefore systems in place to perform an operational function but which also provide a safety benefit. Safety related systems do not provide the primary means of protection for fault sequences. This is distinct from safety systems which are systems that do not perform any operational functions and are included solely because of the safety functions they perform.

SAFE SUBSET – The subset of instructions from the total set of a programming language which can be regarded as amenable to static analysis and perform the same operation regardless of context.

SOFTWARE LIFECYCLE – All stages from conception to final disposal through which a software product passes.

SUBSTANTIATION –The process used to establish a system's fitness for purpose by sufficient evidence.

TIMING BUDGET – The time allocated for the completion of a particular process or procedure.

VERIFICATION – The process of ensuring that a phase in the system life-cycle meets the requirements imposed on it by the previous phase.

VALIDATION – The process of testing and evaluating the integrated computer system (both hardware and software) to ensure compliance with the functional, performance and interface requirements.

VARIABLE – A parameter within a program whose value will be changed by the action of the program. A declared variable is specified at the beginning of a program as being used. It is also characterised at this stage. This process reduces the likelihood of errors.

WATCHDOG – A device that will force the system to take a safety action if continued correct operation of that system is not detected.

9. APPENDIX 3 TECHNICAL GUIDANCE FOR ASSESSING SOFTWARE ASPECTS OF COMPUTER BASED SYSTEMS IMPORTANT TO SAFTEY

GENERAL

9.1 This appendix provides technical guidance based on an earlier detailed ONR technical assessment guide. Much of the content of the earlier guide is now addressed by modern standards (see below) and hence is not reproduced in detail in this appendix. The guidance presented below may, at the discretion of the assessor, be applied to all computer based systems important to safety (with the exception of those clauses highlighted as “for safety systems”, which apply only in this case).

9.2 The guidance provided below should be used in conjunction with IAEA guidance on the design of instrumentation and control systems (SSG-39) [Ref. 7], Licensing of safety critical software for nuclear reactors; common position of international nuclear regulators and authorised technical support organisations [Ref. 8], and IEC standards (see next two paragraphs). The detailed guidance below addresses topics that require enhancement of the guidance presented in the standards and specific regulatory expectations.

9.3 For nuclear power plants, the IEC standards to be considered for assessing software aspects of computer based systems important to safety are the general requirements for systems (all classes) (IEC 61513) [Ref. 10], software aspects for systems performing category A functions (IEC 60880) [Ref. 12] and category B or C functions (IEC 62138) [Ref. 13]. While this appendix addresses some hardware related topics (see below), the IEC standard requirements for computer based system hardware for nuclear power plants are provided in IEC 61513 and IEC 60987 [Ref. 15] for class 1 and 2 systems and in IEC 61508 [Ref. 9] for class 3 systems.

9.4 For other nuclear facilities such as nuclear chemical plants, IEC 61508 [Ref. 9] is the designated IEC standard, although the requirements of this TAG still apply and the nuclear power plant standards may provide relevant clarification. Note that IEC 61508 part 1 addresses general requirements (analogous to IEC 61513), part 2 systems requirements, hardware design and system integration and part 3 software requirements.

9.5 The duty-holder should produce a statement of the standards used and provide a demonstration of conformance, with all non-conformances fully justified (see 5.24).

9.6 The IEC standards noted above use the concept of system class, function category and safety integrity level (SIL). Appendix 4 discusses the link between system class, function categories and SILs.

ORGANISATION

9.7 The duty-holder should ensure that appropriate standards, procedures and personnel are used at all stages in the software lifecycle to produce the required integrity for computer based systems important to safety, or otherwise justify that the required integrity has been achieved for pre-developed items, such as COTS smart devices and platforms (see also 5.20) . Those persons carrying out this role should be independent from the designers, implementers, verifiers and validators.

9.8 Assessors should, as part of early engagement activities, review the duty-holder’s proposals on the methods to be employed to demonstrate how the required level of integrity will be met. For systems containing bespoke software, especially at class 1 and class 2, regular progress reports should be submitted throughout the software development lifecycle.

9.9 Assessors should ensure that a graded approach, dependent upon system class, is adopted for the independence of personnel undertaking verification and validation activities. So far as is reasonably practicable:

- For a class 1 (SIL 3 or 4) system, verification and validation activities should be carried out by personnel from an independent department, ideally with a different line management chain to the department responsible for specification and design.
- For class 2 (SIL 2) and class 3 (SIL1) systems, verification and validation of an activity should be performed by competent persons who did not participate in the activity.

SYSTEM SPECIFICATIONS

9.10 The requirements for developing system specifications (eg system requirements specification and system design specification) can be found in the IEC standards, in particular IEC 61513 and IEC 61508 (parts 1 and 2). The specifications should address all functional and performance requirements (eg timing budgets, volumes of data, data transmission speed, peak data loads, maximum values of parameters and calculation accuracies).

9.11 For class 1 systems, where reasonably practicable, the system requirements specification should be animated by executing the specification. Animation aids the process of communicating ideas about a complex set of requirements that should be understood by all professionals involved in the protection system project.

SYSTEM DESIGN

9.12 The IEC standards (eg IEC 61513 and IEC 61508) require that the system should be designed using a structured approach (eg to ensure that the design process is clearly visible).

9.13 The system design must satisfy both the functional and performance requirements expressed in the system specifications. For example, due consideration should be given to the frequency of sampling of input parameters such that varying measurements are truly represented within the system and events are observed within sufficient time to take the necessary action. The use of features not specified by the manufacturers (eg undeclared instructions or clock rates) should be prohibited unless their use is fully justified.

9.14 A reliability analysis should be undertaken to determine hardware failures that are not self-revealing and that require a proof test to ensure they are revealed. These proof tests should be defined and be developed to reveal all undiagnosed dangerous failures (ie failures that either prevent a safety function from operating or decrease the probability that a safety function operates correctly when required) so far as is reasonably practicable. Where automatic tests are used in lieu of or to reduce the frequency of manual (proof) tests:

- The faults that can be detected by the automatic test features should be documented.
- Adequate overall test coverage should be demonstrated.
- The adequacy of the frequencies for automatic tests (as combined with manual (proof) tests) should be justified in accordance with the reliability and safety requirements.
- Adequate detection and management of faults should be demonstrated.
- The safety benefits of automatic tests, such as improved fault reporting and increased reliability, should be balanced against any potential increase in system complexity.

- Execution of automatic tests should neither degrade the performance of the system functions (eg by delaying system response time beyond requirements) nor impair the system's ability to perform its functions (eg by causing system lock-up).

9.15 Any application of test equipment by the duty-holder should be strictly controlled through suitable procedures to reduce the risk of leaving such equipment in place and introducing unidentified dangerous failure modes.

9.16 Where digital data communication from a higher class system to a lower class system is required, duty-holders should consider the use of separation techniques to ensure one-way flow of information / data (eg via a one-way diode). In addition, where reasonably practicable, hardware isolation should be employed between monitoring tools and the safety system or safety related system (e.g. transformers, opto-isolators, etc.) so that a fault on the monitoring tool does not adversely affect the computer based system.

QUALITY ASSURANCE

9.17 Quality assurance should be at least to the IAEA standards and guidance defined in Refs 22, 23, 24, and 25. Requirements on quality assurance are also contained in the IEC standards (eg IEC 61508 part 1 and IEC 61513) noted at the beginning of this appendix.

9.18 An agreed quality assurance programme and plan for the hardware and software, covering all stages of specification, design, manufacture, installation, commissioning, operation and maintenance, should be available and implemented.

9.19 Periodic, independent audits should be conducted by the duty-holder to ensure conformance to the quality assurance programme and plan.

SOFTWARE

9.20 Software implementation requirements are addressed in the IEC standards noted at the beginning of this appendix. In particular, detailed software expectations are contained in IEC 60880 [Ref. 12] (for nuclear power plant class 1), IEC 62138 [Ref. 13] (for nuclear power plant class 2 and 3) and IEC 61508 [Ref. 9] part 3 (applicable to other nuclear facilities).

9.21 The design and implementation of software fault tolerance measures and use of defensive programming techniques is required for safety systems (class 1 and 2) and should be adopted for safety related systems where reasonably practicable.

9.22 Defensive programming techniques should be employed where known states and parameter ranges occur. For example, where the state of a valve can be either open or closed, a check should be made that, after a finite change-over time, one state or the other is achieved. In the case of parameter ranges, computations should be checked for unrealistic answers (eg negative outputs when only positive are expected). An appropriate system response (eg safe state) should be taken in response to such errors.

9.23 For safety systems, if complicated calculated protection functions are required, the program should be written so that additional simple functionality provides an error check and back-up action.

9.24 Because of the potential of unauthorised access via data links (hacking), computer based safety systems and all supporting systems should not be digitally connected to any other networks, either directly or through another computer system, unless an

adequate safety case has been made to demonstrate that there is no capability for unauthorised access to the protection system (see appendix 6).

9.25 For safety systems, programs should be organised on a modular basis. A module based approach should be adopted for safety related systems where reasonably practicable. The use of a module based approach helps to minimise the chance of errors, facilitates independent verification (for example restricting the design of a module to one clearly identified function that requires only minimum interaction with other functions) and minimises the impact of changes. A justification should be provided for the maximum module size utilised.

9.26 Consideration should be given to the testability of the software design. For safety systems, testability for statistical testing should be considered. To do this it is beneficial to minimise the length of history of internal software state on which the computation depends. Information on the design provisions for testability should be made available to the testers.

9.27 For safety systems (class 1 and 2), the program should run in a fixed sequence pattern and should not generally employ interrupts. Where interrupts are used, they should be justified in terms of demonstrably simplifying the program. Their usage and masking during time and data critical operations should be checked for correct operation in-service and be well documented. The hardware and software should be designed to detect both un-serviced and missing interrupts. All interrupt vectors should be initialised, whether used or not. Unused interrupts should point to an error reporting procedure and should initiate protective action (eg initiation of partial trips/actuates). For safety related systems, the use of interrupts should be minimised or avoided where reasonably practicable.

9.28 For safety systems (class 1 and 2), a hardware watchdog of demonstrably adequate reliability should be employed. This should be serviced by a program operating at the highest level of priority so as to detect problems such as programs locked in loops or deadlocks. (See also SAP ESS.17 and ESS.21.)

9.29 Assembly language should be kept to a minimum and subject to the same strict controls as a high-level language. Good practices that would be introduced by a compiler should be implemented in assembly language; for example, array index checking.

9.30 Any proposed operating system important to safety should be shown to comply with this technical assessment guide.

9.31 Coding standards should be mandatory for all systems important to safety and should, as a minimum, cover naming conventions, house style, level of commenting and software production procedures. The following paragraphs provide guidance on the content of coding standards, in particular, examples of what should be avoided and encouraged. The rigour of application of the guidance should be highest for safety systems. For safety related systems, the guidance can be relaxed provided adequate justification is provided.

9.32 The coding standards should address the avoidance of the following practices:

- unsafe mixing of variable types;
- assembly and machine code inserts into high level language code;
- tricks (ie non-intuitive use of programming constructs);
- recursion (unless it produces simpler code than by other means), re-entrancy and unnecessary code compaction – it should be noted that recursion is not amenable to static analysis;

- program halts – unless it is not possible to action (by bringing the plant to a safe state) and report the error;
- dynamic storage allocation – this causes problems with static analysis, since memory overflow and overwriting of variables cannot be checked;
- dynamic instruction changes;
- multiple use of variables – variables should not be used for more than one function;
- default conditions in case statements – all cases should be covered; the default should be a fail-safe condition;
- multiple module entry points – single entry and return points should be employed (other than error return where required); where a module is a subroutine or procedure, parameter passing should be the means of conditioning;
- branching into loops;
- complicated calculation of indexes;
- equivalence statements – especially referring to a common or global area;
- procedural parameters (where a parameter of a procedure is itself a procedure);
- modification of loop control variables within the loop;
- similar names for variables and procedures;
- use of deprecated features;
- direct memory manipulation commands;
- computed branching (note that good program structure such as use of if-then-else and case statements is required).

9.33 The coding standards/procedures should encourage the following:

- use of a high-level, strongly typed, programming language;
- explicit declaration and assignment of variables and data;
- program layout that aids understanding;
- arithmetic expressions reflecting the equations they represent;
- rate of change checking, where possible;
- dynamic checking for overflow, underflow and compatibility between precisions;
- transfer of data by parameter passing – the unnecessary use of global variables should be discouraged;
- constraining of loop iterations to a declared maximum value (this ensures loop termination);
- explicit initialising of all variables;
- representing constants by symbolic names;
- meaningful variable names and types;
- nesting limited to a maximum depth of four;
- minimisation of procedure and subroutine parameter numbers (ideally not to exceed four);
- careful use of indirect addressing so that the ultimate address is as clear as possible;
- the performance of arithmetic operations in binary fixed-point arithmetic, unless the use of floating-point arithmetic can be demonstrated to contribute to safety – in the latter case, the hardware and software used to implement floating point functions should be suitably qualified;
- checking of computer array subscripts for dimensional range;
- specify literals in full (eg real as 23.0 rather than 23, booleans as true / false);
- consistent commenting (eg module headers with version, author, reviewer, date etc);
- detailed commenting.

HARDWARE CONSIDERATIONS (SOFTWARE ASPECTS)

9.34 The design of computer system hardware is addressed by IEC 61508 [Ref 9] and IEC 60987 [Ref 15]. IEC 60987 does not address complex hardware components such as microprocessors.

9.35 Since computer system components (such as microprocessors) involve complex design with the potential for introducing errors, only proven components should be used. Proof of suitability should include either evidence of extensive installation years free of design faults or rigorous formal proof of the design plus comprehensive type testing (see also the guidance provided in IEC 61508 part 2, in particular, clause 7.4.6.1 and its note).

9.36 Redundant portions of the system should not be operated synchronously unless it can be established that this gives a safety advantage.

HARDWARE FAULT MONITORING

9.37 The design of CBSIS should employ self-supervision and diagnostic checks. Guidance on the need and specific requirements for self-supervision and diagnostic checking is contained in IEC 61513 [Ref. 10] (e.g. subclauses 5.4.2.3.c and 5.4.2.4.b and c), IEC 60880 [Ref. 12] (e.g. subclauses 6.2, 7.1.1.1 and A.2.2, 7.1.1.12 and B3), IEC 62138 [Ref. 13] (e.g. subclauses 6.2.1.2.4, 6.3.3.4 and 5.3.3.4) and IEC 61508 [Ref. 9] (e.g. part 2 subclauses 7.4.8, 7.4.9.4.k, Table A.1 and 2 etc, and part 3 subclauses 7.2.2.8 and 7.2.2.10).

VERIFICATION AND VALIDATION

9.38 The requirements for verification and validation are contained in the IEC standards [Refs 9, 10, 12 and 13]. The requirements for independence of those undertaking verification and validation activities are discussed in paragraph 9.9 above.

9.39 Use of appropriate tools for verification and validation activities is recommended - see appendix 7. In assessing the relative importance of errors found using software verification tools, the possibility that a tool may only produce one example of each type of error found, which could mask another example of greater safety significance, should be considered. If this is possible, it should be avoided by an appropriate verification process or any instances detected and corrected by an appropriate investigation.

9.40 As part of the design verification and validation processes, the software should be statically analysed. Static analysis should also be part of the independent confidence building measures. The static analysis tool used for independent confidence building should be of proven design, qualified (see appendix 7) and diverse from the tools used by the designers.

9.41 For safety systems (class 1), as a precaution against the introduction of erroneous or unwanted code, the machine code of the system should be translated into a form suitable for comparison with the specification (reverse engineering). Any errors should then be corrected. This process can be carried out either manually or using software aids. For example, the system machine code might be disassembled using a software tool and the resulting code translated into a form suitable for performing mathematical proofs of equivalence. Note this activity can be performed either as part of the production excellence activities or the independent confidence building measures.

9.42 The verification and validation tests should exercise the software across the full range of the requirements specification paying particular attention to boundary conditions. Also, by inspecting the code, tests should be devised which seek to detect such errors

as stack overflow, divide by zero, numerical overflow, timing conflicts including bus contention problems etc.

9.43 Consideration should be given to cliff edge effects to ensure that the system does not generate unsafe conditions when taken marginally beyond the specification limits. Adequacy of spare processor time, scan times and data transfer rates should be demonstrated.

9.44 Off-site test coverage should be such that all lines of code and (at system integration) all module calls are exercised at least once; this to be confirmed by coverage analysis. For safety systems, additional code coverage metrics should be adopted to address both branch (class 1 and 2) and path coverage (class 1). Operations on data items should be exercised at least once unless a bounding case can be made. All time critical sections of code should be tested at least once under realistic conditions. Where calculations are performed in the software, their result should be checked against pre-calculated values. The fault tolerance of the system should also be tested by subjecting the system to appropriate tests, including those that are only implied by the specification.

9.45 Once installed on-site, a test program should exercise cyclically all aspects of the hardware (including inputs and outputs), over an extended period of time (typically 400 hours) to establish that the hardware is sufficiently reliable to commence plant commissioning.

9.46 The full system (software and hardware) should be tested on-site for an extended period (the duration will depend on system complexity), for example 12 months for a class 1 reactor safety system before active commissioning (see also 5.25). Actual plant inputs should be used as far as is reasonably practicable; the validity of simulated inputs should be justified and tests should demonstrate the correct operation. The results of the on-site testing should be analysed prior to commencement of active commissioning in order to determine the impact on the claims made in the safety case.

DOCUMENTATION

9.47 The need for documentation to support the safety case (eg providing evidence to substantiate claims and arguments) must be recognised by the system suppliers and the duty-holder. The duty-holder will need to ensure that ONR and its technical support contractors have ready access to the documentation in the UK.

9.48 Documentation requirements are contained in the IEC standards (eg IEC 61513 [Ref. 10] subclauses 5.3, 5.6, 6.4, 7.3 and 8.3, and IEC 61508 [Ref. 9] part 1 clause 5 and annex A). The documentation should be provided in English and cover all aspects of the CBSIS. It should reflect the as-built state, ie be correct, up-to-date and under a documentation management regime.

9.49 Sufficient documentation should be readily available on-site to enable suitably qualified duty-holder staff to understand and maintain the system. The following list provides examples of documents that should be available as a minimum. The information outlined below may be contained in the documents as named or other such documents so long as the full set of information is provided by the complete document set.

- Operators' manual – details facilities and use of the system in a non-technical language. Normal and abnormal operation should be described.
- Systems description manual – details in full the functions of the different parts of the system and the facilities offered to the operator and maintainer.
- Standard hardware documents – handbooks, instruction manuals and drawings for all bought-in items.

- Special hardware documents – full circuit diagrams, complete with component layouts and indications of normal signal levels plus a full parts list. Design principles, circuit operation, test procedures and fault diagnosis information should also be included (for class 3 COTS devices supported by a third party supplier/manufacturer, some of this documentation may not be available on site).
- System hardware documentation – details of equipment arrangement, first line fault diagnosis information including the use of any test procedures and module replacement procedures.
- Standard software - all software documentation for bought-in software such as compilers, linkers, utilities etc.
- Systems and applications software - details of the operation of the software system and individual programs should be given as follows. The content should be such that the system maintainers (for class 3 systems, not necessarily on-site) can readily gain an appreciation of the overall system and individual programs.
    - Descriptions of all functions, major task and programs together with their interrelationships.
    - The following data should be provided with each program module as a minimum:
        - purpose of module,
        - system linkage,
        - initialisation,
        - data and parameter input,
        - data and parameter output,
        - data and files accessed,
        - data and files modified,
        - timing,
        - interrupts,
        - hardware interfaces,
        - program structure,
        - functional description of the program,
        - error returns,
        - size of module,
        - any special considerations.
    - Detailed memory maps showing disposition of programs, data areas and spare memory.
    - Data areas:
        - details of purpose,
        - format,
        - type,
        - cross-references to programs using data,
        - size of file/array.
    - Listings - a complete listing of the source code fully commented.
    - A complete memory-dump.
    - Control and data flow should be illustrated either in graphical or pseudo-code form for the overall system and for individual modules.
    - Quality assurance plan compliance record.
- Software and hardware part numbers and versions in use.
- Test results.
- List of software and hardware design standards.
- Failure modes and effects analysis / fault tree analysis for hardware and software.
- Verification and validation results.

TRAINING

9.50 All duty-holder staff associated with the operation of the system should have received adequate training in their particular role and be able to demonstrate competence prior to being permitted access to the system.

OPERATION AND MAINTENANCE

9.51 Formal procedures should be in place for the documenting and timely reporting of residual software errors that occur during the operational stage. The safety implications of such errors should be reviewed by appropriately authorised personnel.

9.52 The system and procedures should be arranged so that only an approved program as a whole can be loaded into the system.

9.53 Suitable arrangements should be made for the secure storage of copies of the software that is to be loaded in the event of a system failure. Due regard should be given to all possible means of corruption of the software. Particular attention should be paid to the secure storage of pre-programmed memory devices if they are used. Means should be provided to verify that the software has not been corrupted prior to its use both before and after loading. Automatic means are preferred.

9.54 All necessary hardware and software for maintenance of the system should be in place prior to active commissioning.

9.55 Safety system software should not be altered to overcome operational or maintenance difficulties, other than on an equivalent off-line system using agreed modification procedures. Engineered facilities should be provided where there is a need to change specific system parameters such as trip settings, calibration constants etc for operational reasons. The available range should be limited to values supported by the safety case. A display of current values or states of such parameters should be provided.

9.56 Where software has been modified, an analysis of the impact of the modification on the system's safety functions should be performed. The tools and techniques used in the development and testing of the modification should accord with relevant good practice at the time of the modification. The level of rigour should be proportionate to the impact of the modification and the class of the system.

9.57 The duty-holder should ensure that modified software is tested on a computer system that uses identical equipment to the installed system.

9.58 The duty-holder should maintain histories of all hardware operation so that reliability claims can be monitored. Certificates of conformance should be available, and a policy for sufficiently recording the detection and repair, or replacement, of faulty hardware should be employed so that operating histories can be maintained, traced and properly interpreted.

9.59 The duty-holder should undertake repair and modification of both safety system hardware and software off-line. If safety related system repair and modification is to be undertaken on-line then a justification of adequacy should be provided. Such repair and modification should only be performed by personnel with proven competence in the relevant field and knowledge of that part of the system.

9.60 The mean time to repair has an effect on total system reliability. Therefore, the duty-holder should ensure there are sufficient spares, test equipment, and adequately trained staff readily available to enable the assumed mean time to repair value to be met during real-life operation. The maximum on-line repair time allowed before the reactor or process must be shutdown should be stated and justified.

10. APPENDIX 4 SOFTWARE SUBSTANTIATION OF COMPUTER BASED SYSTEMS IMPORTANT TO SAFETY

GENERAL GUIDANCE

10.1 This appendix applies to all CBSIS (ie both computer based safety systems and safety related systems) where a reliability claim is made of less than 3E-1 probability of failure on demand (pfd) / frequency of dangerous failures per year (ff) – see paragraphs 5.8 to 5.11.

10.2 Assessors should consider the category of each safety function, informed by the initiating event frequency and the radiological consequences, as the starting point for their assessment [Ref. 4]. This in turn should be used to determine the appropriate class of the CBSIS [Ref. 11]. The function's safety categorisation and the system's safety class broadly establish the regulatory expectations (see also NS-TAST-GD-094 'Categorisation of safety functions and classification of structures, systems and components' [Ref. 4]).

10.3 In providing suitable and sufficient substantiation of the software used in CBSIS, duty-holders should apply a selection of techniques and measures to demonstrate the system's fitness for purpose. Due to the complexity of CBSIS and their vulnerability to systematic failure, assessors should focus on deterministic expectations set out in TAGs (e.g. Refs 2, 3 and 4), standards (e.g. Refs 10, 12 and 13) and relevant good practice.

10.4 Duty-holder's claims may be supported by probabilistic numerical claims. These numerical claims are strengthened by the application of techniques such as statistical testing.

10.5 The overall reliability of a system containing software should account for both software and hardware factors. Satisfaction of the reliability requirement should be demonstrated by an appropriate hardware reliability analysis, and fitness for purpose of the software demonstrated through robust production excellence and the application of suitable and sufficient independent confidence building measures. Duty-holders should demonstrate that both the hardware and software aspects are commensurate with the system's class.

FUNCTIONAL CATEGORISATION, SYSTEM CLASSIFICATION AND SAFETY INTEGRITY LEVEL

10.6 IEC 61513 [Ref. 10] does not provide an explicit link between safety class and safety integrity level (SIL, as defined in IEC 61508 [Ref. 9]). However, it does acknowledge that there are similarities between the assignment of SILs to safety functions in IEC 61508 and the classification of nuclear safety functions in IEC 61226. ONR has adopted the position outlined in NS-TAST-GD-003 [Ref. 2] and NS-TAST-GD-094 [Ref. 4], whereby the system class is aligned to probabilistic targets and deterministic expectations.

10.7 Numerical claims for computer based systems important to safety can range from of the order of 1E-1 to 1E-4 probability of failure on demand (pfd) or frequency of dangerous failure per year (ff). These claims are denoted "high confidence" to distinguish them from best estimates used in PSA (see paragraph 10.18). In particular circumstances, it may be acceptable for duty-holders to claim a best estimate reliability of lower than 1E-4 for the purposes of a probabilistic safety analysis only. ONR's assessors should look at the adequacy of the duty-holder's arguments and evidence to support this claim in the PSA model. However, ONR's expectation is that, for the purposes of C&I assessment, numerical claims are "high confidence" in accordance

with table 1 and a claim of 1E-4 is considered to be the best (minimum) that can justifiably be claimed for any single CBSIS (see paragraph 5.12).

10.8 Table 1 provides indicative guidance on the range of numerical claims with regards to class, and an initial expectation on the application of techniques and measures that would be applied to substantiate the system according to relevant standards and relevant good practice (e.g. Refs 9, 10, 12, 13 and 16).

Table 1 – Link between categorisation, classification and SIL

Category and class according to TAG94	IEC 61508 probability of failure on demand (pfd) range (high confidence)	IEC 61508 frequency of dangerous failure per year (ff) range (high confidence)	ONR's initial expectation regarding the application of techniques and measures according to IEC 61508	Initial acceptable nuclear safety case probability of failure on demand (pfd) value or frequency of dangerous failure per year (ff) (high confidence)	Limit to the reliability claim providing relevant assessment criteria has been met (high confidence)
Cat A / class 1	1E-5 ≤ pfd < 1E-3	1E-5 ≤ ff < 1E-3	SIL 4	1E-4 *	1E-4 *
Cat B / class 2	1E-3 ≤ pfd < 1E-2	1E-3 ≤ ff < 1E-2	SIL 2	1E-2	1E-3
Cat C / class 3	1E-2 ≤ pfd < 1E-1	1E-2 ≤ ff < 1E-1	SIL 1	1E-1	1E-2

* Note the best (minimum) that should be claimed for computer based safety system is 1E-4 (high confidence). A claim of 1E-4 (high confidence) should always be delivered by a SIL 4 system.

10.9 For demonstration of production excellence, assessors should confirm that a graded approach to the application of techniques and measures is taken in accordance with these relevant standards and relevant good practice.

10.10 Assessors should look for the proportionate application of independent confidence building measures in line with the class of the system, and consider whether the duty-holder has demonstrated a suitable level of confidence in the system's fitness for purpose. This should be informed by techniques and measures defined in international standards. The techniques and measures selected should be tailored to the specific system application, address any gaps in the knowledge of the system performance and take account of any uncertainties associated with a particular method (eg if a particular technique has a high level of uncertainty associated with it then the duty-holder should consider the application of a diverse technique or measure to provide additional confidence). Assessors should look for a higher level of confidence in fitness for purpose where duty-holders are looking to substantiate numerical claims at the lower (more onerous) end of the reliability range within the class / SIL band.

10.11 Expectations in relation to smart devices are provided in appendix 8.

10.12 There are public statements on justifiable claims for computer based systems in nuclear reactors [Refs 7, 8, 11 and 16]. The maturity of current techniques, their practicability of application to real life systems important to safety and other factors such as computer based system complexity, configurability, novelty and maintainability should also be considered.

10.13 For example, the initial expectation for a category B function is that it should be delivered by a class 2 system. If a duty-holder wanted to claim 1E-3 pfd (high confidence) for this system, the hardware reliability analysis should demonstrate that it

meets this figure, and the production excellence, compensating activities and independent confidence building measures should holistically demonstrate a strong deterministic case for the software supported by probabilistic evidence where appropriate.

NUMERICAL CLAIMS (PROBABILISTIC ANALYSIS)

10.14 The estimation of the contribution of potential software faults on the reliability of the system should be based on a qualitative evaluation which takes account of the design complexity, the quality of the development process, the result of robust testing and feedback from operational experience.

10.15 Any numerical reliability claim for a computer based system should take account of the demonstrated hardware reliability figure and the breadth, rigour and strength of the production excellence, compensating activities and independent confidence building measures. Following this assessment, the assessor should determine whether or not there is sufficient confidence in the system case for a reliability claim at the lower (ie more onerous) end of the range in table 1 to be justified.

10.16 For example, a nuclear safety claim of 1E-2 pfd /ff for a CBSIS might be justified by demonstrating the rigorous application of the full range of techniques and measures applicable for a SIL 1 system, as well as an appropriate selection of SIL 2 techniques and measures.

10.17 The safety demonstration should be assessed to determine the effectiveness of what has been done to control or avoid systematic failures, and what other measures have been considered. The effectiveness of the techniques and measures used and the breadth and rigour of what is required will depend on the circumstances of the specific case.

10.18 CBSIS reliability claims can also be used for the purposes of PSA. Evaluation of systems important to safety for PSA purposes is usually undertaken on a best estimate (50% statistical confidence level) basis. In addition, PSA can be used to inform the design process, support the process of safety function categorisation and system classification, and assist in the specification of reliability targets for safety systems and safety related systems. The substantiation of computer based systems important to safety should be on a conservative, high statistical confidence, basis (ie 95-99%). Paragraph 10.28 provides more information.

10.19 A normal duty function continuous mode (ie with a failure frequency defined per year rather than per demand) control system may provide a safety function for a number of fault sequences (as is the case for a data processing and control system, for example). If so, the duty-holder should justify its PSA approach and demonstrate how the analysis is used to inform the CBSIS deterministic requirements. For example, a duty-holder should separately model the probability of each function being delivered only if it is reasonable to claim that the system delivering each function is independent. If, however, a common cause (ie systematic) failure of the control system impacts on the delivery of a number of functions, as is likely if they are implemented in the same control system, then the licensee should model the loss of all control functions as a credible simultaneous event within the PSA.

INITIATING EVENT

10.20 Spurious failures of computer based systems important to safety are considered postulated initiating events (PIEs). These failures, if not mitigated, may start a fault sequence leading to radiological consequences. Evaluation of the PIE frequency for design basis accident analysis, transient analysis, and accident progression analyses is usually undertaken on a best estimate (50%) basis. When models are used for the

calculations of input probabilities (for example failures of computer-based systems), then the methodologies used by duty-holders should be justified, and should account for all key influencing factors. Duty-holders should give due regard to uncertainties in input probability and frequency values used, and their impact on the results from the analyses. Where necessary, assessors should seek assistance from PSA specialist inspectors and/or consider guidance provided in NS-TAST-GD-030 'Probabilistic safety analysis' [Ref. 26]. Further guidance on evaluating spurious failures is included in Ref. 27.

TECHNIQUES AND MEASURES

10.21 In order to demonstrate that a system has achieved a particular safety class, both random hardware failure and systematic aspects must be considered.

- The hardware reliability achieved for a system should be demonstrated through appropriate hardware analysis techniques, and should be shown to be at least as good as the lower end of the SIL range identified for the SIL / class in Table 1.
- For systematic aspects, the assessor should consider the overall production excellence, compensating activities and independent confidence building measures applied to the system.

10.22 Duty-holders may choose to use a variety of techniques and measures to provide confidence of the system's fitness-for-purpose. Guidance on particular techniques and measures highlighted here are not necessarily more important than other techniques and measures. Assessors should consider the suitability of all techniques and measures when considering the adequacy of the duty-holder's software substantiation.

Static analysis

10.23 Static analysis can identify and correct some systematic faults that could lead to failure of the CBSIS. The technique analyses the properties of the software source code, detects inconsistencies, and identifies undesirable program constructs. It can provide strong confidence in the software but requires access to the software source code which may limit its use in pre-developed software, especially in lower integrity systems.

10.24 Relevant good practice [Refs 7, 8 and 12] requires analysis of the source code to be rigorously applied for a class 1 safety system (ie for reliability claims lower than 1E-3 pfd). ONR's regulatory expectation is that reasonable efforts should be made to obtain access to the source code for all CBSIS, regardless of safety classification, in order to apply static analysis as an independent confidence building measure in the substantiation of the system. A proportionate approach to software static analysis is required. For example, for class 3 a design review may be appropriate, for class 2 a control flow and data flow analysis may be added and for class 1 boundary value analysis, formal inspections and run time error behaviour would also be expected. In cases where access to source code has not been obtained duty-holders should provide a justification to demonstrate that reasonable efforts to obtain the code were made, and that no reasonably practicable alternatives exist.

Dynamic testing

10.25 IEC 61508 [Ref. 9] describes dynamic testing as executing software and/or operating hardware in a controlled and systematic way, so as to demonstrate the presence of the required behaviour and the absence of unwanted behaviour. It should be applied to a near-operational prototype of the safety-related system with test input data that is typical of the intended operating environment and that demonstrates the required safety functionality. The test results are satisfactory if the observed behaviour of the

CBSIS conforms to the required behaviour. Any failure of the CBSIS must be corrected and the revised operational version must then be retested.

10.26 For CBSIS (which is inherently complex), it may not practicable to test all possible combinations of inputs and operational configurations. Statistical testing is a dynamic testing technique used to give confidence, in a practicable standardised manner, that the claims on a CBSIS are reasonable. Importantly, statistical testing increases confidence in the processes used during a product's development. Although statistical testing may challenge both the software and hardware of the system, it is mainly used to gain confidence in the reliability of the application software. When statistical testing is carried out on application code and platform code together, it tests the interaction between the application and platform code. It can also be used at device level for smart devices.

10.27 Any statistical tests should be:

- representative of the operational transients randomly selected from the input space,
- proportional to the frequency of occurrence of system demands (ie the operational profile), and
- statistically independent of one another (ie the result of any particular test cannot be affected by any other test, ensuring that the system is in the same state after each test).

10.28 Where statistical testing is required as part of the equipment substantiation, this should be to a high statistical confidence level (eg 99%). This requires, for example, of the order of 46,000 tests with no failure for a 1E-4 pfd [Ref. 12]. Where statistical testing is being used to determine a reliability estimate for modelling purposes (eg PSA), best estimate confidence may be appropriate (eg 50%). This requires, for example, of the order of 7,000 tests with no failure for the same pfd of 1E-4.

10.29 Assessors should note:

- statistical testing is only applicable to demand based systems (ie not continuous mode systems);
- for statistical testing to give valid results it is essential to demonstrate that all tests start with the system in an identical state;
- the configuration of the system undergoing statistical testing should be identical to the operational configuration of the system when in use – for systems with multiple divisions (eg for a 2 out of 4 system) the suitability of the configuration of the system undergoing statistical testing should be justified;
- a significant portion of the effort required during statistical testing is associated with the specification of the test profile and creating a "harness" to facilitate the testing; and
- interpretation of the results of statistical testing should consider the limitations deriving from the scope of the testing and areas of uncertainty – the creation of an oracle to judge whether or not a test has been successful can be a challenge.

LOW INTEGRITY SYSTEMS

10.30 For systems with low integrity (ie class 3 with a 1E-1 claim), assessors should consider that it may be sufficient for duty-holders to use information published by accredited independent test houses to support production excellence aspects of the safety case. However, the process used by the independent test house would need to be documented, and the duty-holders should have assessed the suitability of the available information. Assessors may wish to assess a sample of this information themselves to gain confidence in the assessment process. This assessment should include a

statement of the standards against which the assessment has been conducted and should consider any limitations placed on the use of the system or device. Specifically, it should determine whether the information is applicable to the proposed application of the system and whether the methods applied are equivalent to established production excellence assessment methods – for example whether they check against relevant good practice established within international standards. Some duty-holders have developed processes and procedures that may provide an adequate alternative approach to justification of systems with low integrity claims.

THE DIFFERENCE BETWEEN SOFTWARE AND HARDWARE RELIABILITY

10.31 When assessing the reliability of a CBSIS, it is appropriate to consider the hardware and software aspects separately since their failure behaviour can be quite different.

10.32 Simple hardware failures are considered to be predominantly random; hence coincident failures have a low probability of occurrence unless occasioned by a common cause. Hardware reliability can, therefore, be improved by the use of simple redundancy, although a limitation is imposed due to the incidence of common cause failures.

10.33 In contrast, software failures are due to systematic faults; their occurrence depends upon the values of input and stored parameters causing paths containing faults to be executed. Here simple redundancy gives a limited reliability improvement that is challenging to prove since each program may see the same input values. The software equivalent of hardware redundancy is achieved by software diversity, since only by such means can coincident failures be rendered less likely. Where a claim is made that very high reliability has been achieved through software diversity then the assessor should consider the guidance provided in appendix 5 and Ref. 2.

FAULT DETECTION

10.34 When evaluating the numerical reliability claimed for the hardware of a computer based system, limited credit (depending upon the software production method employed) can be claimed for the diagnostic software designed to detect hardware faults.

10.35 Where credit is claimed for self-revealing fault detection and automatic testing in reliability calculations, the contribution attributable to system and operator response, and mean time to repair, should be specified and justified. Failures which are not self-revealing should be deemed to exist until the next test that would reveal them.

10.36 The claimed effectiveness of the fault detection system should be justified. A claim of 100% should be rejected as such a claim is not considered credible on the basis that it is unfeasible to have a high confidence that 100% of faults could be detected in complex systems.

11. APPENDIX 5 USE OF DIVERSE COMPUTER BASED SYSTEMS IMPORTANT TO SAFETY

11.1 The guidance provided in this appendix applies to both nuclear power plants and other nuclear facilities, depending upon the safety claims.

11.2 A major issue during the design and construction of Sizewell B was justifying the high level of risk reduction provided by the reactor protection system comprising the primary protection system and secondary protection system. The risk reduction requirement for the overall protection was 1E-7 pfd (typically 1E-3 pfd from the primary combined with 1E-4 from the secondary protection system to give 1E-7 pfd). The justification relied on a claim that the secondary protection system was a simple hardware based system.

11.3 Demonstrating that two complex computer based protection systems are "independent" and “diverse” (eg will not tend to fail on the same demands) and hence that the reliability claims for each can be multiplied together remains an open question despite significant research[1]. Hence, where a high level of risk reduction is required that is greater than the accepted common cause cut-off limit for a single computer based safety system (ie 1E-4 pfd for a computer based safety system where the consequence in the event of failure of the safety system could potentially involve large releases of radioactive material) then ONR’s current expectation is that a simple hardware based secondary safety system should be provided.

11.4 However, the use of two diverse computer based safety systems to implement a safety function requiring high reliability (eg such as a reactor protection system comprising primary and secondary systems) may be acceptable, provided the guidance in SAP ERL.1 paragraph 191 is followed. This “special case” procedure should also be considered for application where high reliability is required from a combination of a computer based safety system and a computer based safety related system. In this context “high reliability” is taken as a reliability requirement for a safety function that is lower than the common cause cut-off limit (i.e. 1E-4 pfd/ff for a CBSIS where the consequence in the event of failure of the system could potentially involve large releases of radioactive material). For ease of reference the content of SAP ERL.1 paragraph 191 is repeated below:

191 Where reliability data is unavailable, the demonstration should be based on a case-by-case analysis and include:

- *a comprehensive examination of all the relevant scientific and technical issues;*
- *a review of precedents set under comparable circumstances in the past;*
- *where warranted, eg for complex items, an independent third-party assessment* (note this is not associated with ICBM activity – rather a verification of the work undertaken by the person undertaking the analysis)*, and*
- *periodic review of further developments in technical information, precedent and best* (ie relevant good) *practice.*

[1] Key references for research on this issue (2019/119004) include:

Chen, L & May, JHR 2016, 'A Diversity Model Based on Failure Distribution and its Application in Safety Cases' IEEE Transactions on Reliability, vol. 65, no. 3. doi: 10.1109/TR.2015.2503335; and

Littlewood, B. and Povyakalo, A A (2013). Conservative bounds for the pfd of a 1-out-of-2 software-based system based on an assessor’s subjective probability of “not worse than independence”. *IEEE Transactions on Software Engineering*, 39(12), pp. 1641-1653. doi: 10.1109/TSE.2013.31.

11.5 Each of the diverse CBSIS should meet the requirements of SAP ESS.27. With regard to the implementation of SAP ERL.1 in the context of diverse computer based systems important to safety the case should include:

- application of relevant good design practice (eg functional and equipment diversity),
- adoption of appropriate nuclear standards (e.g. Refs 7, 10, 12, 13 and 28) for the production and assessment of diverse computer based systems,
- an independent assessment of all factors that could lead to common cause failure,
- examination and implementation of relevant research.

11.6 The section on diversity contained in Ref. 11 is particularly relevant providing recommendations on functional diversity, use of relevant good practice, simplicity of software design, analysis of common cause failure within the safety demonstration, use of dissimilar means throughout the development lifecycle and conservative reliability claims etc. Detailed guidance on performing diversity analyses of reactor protection systems is provided in Ref. 29.

12. APPENDIX 6 CYBER SECURITY OF COMPUTER BASED SYSTEMS IMPORTANT TO SAFETY

BACKGROUND

12.1 This appendix describes ONR's expectations for the management of potential cyber threats (malware) to the performance of CBSIS. These threats include sabotage and/or maloperation that could result in plant damage or spurious challenge resulting in the tripping of protection systems, with the potential of ultimate failure of a protection system and hence the possibility of radiological release. Good security is also necessary to avoid non-intentional maloperation (for example regarding access, connections and service infringements). The appendix does not consider the security of non-safety related computer systems.

12.2 The intent of this appendix is to provide technical guidance on principles to be considered when assessing cyber security aspects of CBSIS. ONR has produced a set of security assessment principles (SyAPs) [Ref. 30] and associated TAGs to provide the essential foundation for outcome focussed regulation of security disciplines. As part of their overall strategy for cyber security, duty-holders may follow an approach to developing security cases for CBSIS that provide evidence that can be assessed against SAPs and SyAPs to satisfy both LCs and the Nuclear Industries Security Regulations 2003 (NISR) [Ref. 31].

12.3 A series of TAGs has been produced to provide detailed guidance on the assessment of matters relating to cyber security and information assurance (CS&IA). This appendix is intended to be complementary to the relevant SyAPs and TAGs and should be read in conjunction with those documents.

RELATIONSHIP TO LICENCE CONDITIONS AND RELEVANT LEGISLATION

12.4 LC27 requires the duty-holder not to operate, inspect, maintain or test its facility unless suitable and sufficient safety mechanisms, devices and circuits are properly connected and in good working order. The reliable delivery of safety functionality from safety mechanisms, devices and circuits can be undermined through weaknesses in cyber security.

12.5 NISR [Ref. 31] Regulation 4 (2) requires that an approved plan be provided for each nuclear premises which describes in writing the standards, procedures and arrangements adopted or to be adopted by the responsible person to ensure the security of equipment or software used or stored on the premises in connection with activities involving nuclear material. NISR Regulation 7 (1) requires that the responsible person in relation to each nuclear premises must comply with the standards, procedures and arrangements described in the approved security plan for the premises.

RELEVANT SAPS

12.6 The following SAPS [Ref. 1] relate to the cyber security of CBSIS:

Engineering principles: layout	Access	ELO.1
The design and layout should facilitate access for necessary activities and minimise adverse interactions while not compromising security aspects.		

Engineering principles: layout	Unauthorised access	ELO.2
Unauthorised access to, or interference with, structure, systems and components or their reference data (including Building Information Modelling (BIM)) should be prevented.		
SAP Paragraph 225 – Unauthorised access includes remote access to computer programs and reference data.		
Engineering principles: safety systems	Prevention of service infringements	ESS.12
Adequate arrangements should be in place to prevent any infringement of the services supporting a safety system, its sub-systems or components.		
Engineering principles: safety systems	Avoidance of connections to other systems	ESS.20
Connections between any part of a safety system and a system external to the facility (other than to safety system support and monitoring features) should be avoided		

RELEVANT SyAPS

12.7 The following SyAPs [Ref. 30] relate to the cyber security of operational technology (including CBSIS) used in connection with activities involving nuclear material. (SNI is an abbreviation for sensitive nuclear information.)

Fundamental Security Principle	**Cyber Security & Information Assurance**	**FSyP 7**
Duty-holders must implement and maintain effective cyber security and information assurance arrangements that integrate technical and procedural controls to protect the confidentiality, integrity and availability of SNI and technology.		

FSyP 7 - Cyber Security and Information Assurance	Effective Cyber and Information Risk Management	SyDP 7.1
Duty-holders should maintain arrangements to ensure that CS&IA risk is managed effectively.		
FSyP 7 - Cyber Security and Information Assurance	Information Security	SyDP 7.2
Duty-holders should maintain the confidentiality, integrity and availability of sensitive nuclear information and associated assets.		
FSyP 7 - Cyber Security and Information Assurance	Protection of Nuclear Technology and Operations	SyDP 7.3
Duty-holders should ensure their operational and information technology is secure and resilient to cyber threats by integrating security into design, implementation, operation and maintenance activities.		

FSyP 7 - Cyber Security and Information Assurance	Physical Protection of Information	SyDP 7.4
Duty-holders should adopt appropriate physical protection measures to ensure that information and associated assets are protected against a wide range of threats.		
FSyP 7 - Cyber Security and Information Assurance	Preparation for and Response to Cyber Security Incidents	SyDP 7.5
Duty-holders should implement well-tested plans, policies and procedures to reduce their vulnerability to cyber security incidents (especially from the most serious threats of terrorism or cyber-attack), non-malicious leaks and other disruptive challenges.		

GENERAL GUIDANCE

12.8 The use of CBSIS in nuclear facilities increases the vulnerability of these facilities to malicious exploitation. Systems and the arrangements for the protection of systems from malicious attack are at risk of compromise due to the complex nature of the threats. Effective arrangements include:

- selection of systems and equipment that are not vulnerable to cyber-attack, unless this is not reasonably practicable;
- confidence in the integrity of the security of the system throughout the supply chain and lifecycle (as vulnerabilities can be exposed at multiple points through development, manufacture, construction, installation, commissioning and maintenance);
- a robust and integrated approach to quality assurance and testing to ensure security vulnerabilities are effectively managed;
- suitable and sufficient control of software and hardware systems to prevent unauthorised access;
- a robust version control system;
- arrangements to maintain operational knowledge to take account of the complex and dynamic nature of the threat; and
- maintenance of security protection features such as anti-virus, firewall rules etc.

12.9 Cyber security threats should be considered early in the specification and design of each CBSIS as the implementation of adequate controls may affect the system architecture. Any need for external communications (eg data logging) should be specified. Ensure any requirement for system and software maintenance is considered early to avoid the need for remote access when the plant is in service.

12.10 All software, including all support software and tools (eg development tools and compilers) should be covered by a suitable and sufficient configuration management system throughout the lifecycle. Users should be able to access only those items within the configuration management system for which they have authority.

12.11 The hardware and software of each CBSIS should be protected by suitable and sufficient security arrangements for preventing unauthorised access. This includes a suitable management system, processes, controls and physical measures. The arrangements should be regularly reviewed for possible breaches. If there is an unavoidable need for the system to be linked to an off-site network, robust measures should be put in place to minimise the risk.

DUTY-HOLDER'S ARRANGEMENTS

12.12 The regulatory expectation is that duty-holders should ensure that the approved security plan for their nuclear premises clearly details arrangements for:

- cyber risk management in support of maintaining effective CS&IA arrangements (TAG 7.1 [Ref. 32]),
- protection of information in support of maintaining effective CS&IA arrangements (TAG 7.2 [Ref. 33]),
- protection of nuclear technology and operations (TAG 7.3 [Ref 34.]), and
- physical protection of information and associated assets in support of maintaining effective CS&IA arrangements (TAG 7.4 [Ref 35.]).

12.13 TAG 7.5 on preparation for and response to cyber security events [Ref. 36] and IEC 27001 [Ref 19] specify the requirements for establishing, implementing, maintaining and continually improving arrangements for managing information security. These requirements include the development of a policy and establishing responsibilities within the organisation, and the assessment and treatment of information security risks. For IEC 27001, any part of the software of a CBSIS should be considered 'information'.

12.14 IEC 62859 [Ref. 37] specifies the requirements for coordinating safety and cyber security in CBSIS. A fundamental principal of this standard is to ensure that cyber security does not interfere with safety, and does not compromise the effectiveness of safety functions.

12.15 A duty-holder's arrangements for the effective and efficient management of cyber security for CBSIS should include the following:

- the identification of all CBSIS – this should include any computer based system with a claim in the facility's safety case and any systems that provide information to operations, where the information can influence operator actions that are required for safety;
- a policy that clearly defines responsibilities in line with IEC 27001 [Ref. 19];
- the allocation and communication of roles and responsibilities;
- a safety, and hence security, class for each CBSIS to enable the duty-holder to prioritise its effort towards systems where the consequences of cyber-attack are greatest;
- arrangements for the regular review of security risks including changes in the nature of threats;
- a CBSIS security training and awareness programme to ensure that the relevant personnel are suitably qualified and experienced – this should entail the provision of cyber security training to personnel responsible for safety, and reciprocally for the training on safety principles for personnel focussing on cyber security;
- suitable and sufficient review and monitoring of the duty-holder's arrangements to ensure continuous improvement; and
- sharing operational experience within the duty-holder's organisation and, where necessary, to the broader industry.

12.16 IEC 27001 states that the duty-holder shall define and apply an information security risk assessment process. This risk assessment should be proportionate, focused on identifying any control measures needed, and include plans for the implementation of measures to ensure risks are reduced to a level as low as reasonably practicable. It should take in to account the nuclear significance (eg extent of radiological release) of a failure of a CBSIS to perform any of its safety functions (indicated by its safety classification).

CBSIS SECURITY CONTROL MEASURES

12.17 As a result of their risk assessments, duty-holders should introduce control measures to reduce the security risks to ALARP. The following list of control principles is based on existing guidance [Refs 20, 21 and 37] but should not be considered to be prescriptive or used by assessors as a check list. However, the guidance may help inform assessors when considering whether all reasonably practicable measures have been implemented by the duty-holder. It should be acknowledged that implementing cyber security features in CBSIS will inherently increase their complexity, which has the potential to introduce new failure modes into the system. As a result IEC 62859 [Ref. 37] states that cyber security features implemented in CBSIS shall be qualified to the same level as the system in which they reside (ie in line with the basic safety expectations for CBSIS).

- Secure software storage and configuration management
  - Corporate polices and processes should be developed to secure software builds, and manage the configuration and use of systems throughout the software lifecycle (ie from development, manufacture, installation, test and maintenance).
  - Inventory of authorised devices – All CBSIS hardware devices (including tools and removable media) on the site should be identified so that their existence and location is known, and should be actively managed.
  - Inventory of authorised software – All CBSIS software on the site should be identified and actively managed and only authorised software should be installed and executed on equipment.
- Network and device security
  - Connection of any plant/engineering networks to external services should be avoided wherever practicable.
  - If connection of a plant/engineering network to external services is required, ensure the security risk is sufficiently mitigated, for example by establishing a demilitarised zone with diverse firewalls.
  - Wherever practicable the network should be monitored with tools to detect and prevent intrusion.
  - Wherever practicable the security controls should be regularly tested, for example through penetration tests and simulated cyber-attacks.
- Managing user privileges
  - Appropriate processes and procedures should be established for user identification and access control, for control systems and any tools associated with them.
  - A personnel screening process should be in place commensurate with the sensitivity of the information / nuclear safety significance of the control system they will have access to.
  - An effective account management process should be implemented to ensure accounts are added, reviewed and deleted appropriately.
- The number of users and their privileges should be limited, and there should be strict control the number of privileged accounts.

- Malware prevention

  - Corporate policies should be developed and published to establish comprehensive anti-malware defences and these should include control systems.
  - All computer based equipment, wherever practicable, should be protected with anti-virus, white listing or another similar defence.
  - All data imports (or exports) should be scanned for malicious content. Stand-alone workstations equipped with two anti-virus products should be considered.

- Removable media controls

  - Policies that control the use of removable media for the import and export of information should be produced and implemented.
  - The use of removable media should be minimised. Where their use is unavoidable the types of acceptable media should be limited and specified. Controls on the extent of users, systems and types of information stored on removable media should be limited and controlled.

- Change management and system modification

  - It is important to recognise that software updates for the purposes of cyber security are a type of software modification, hence should be treated as such and managed in accordance with the duty-holder's policies on software modification.
  - The rapid evolution of cyber security threats is difficult to reconcile with software modification processes for CBSIS, therefore security features for CBSIS should limit dependency on updates as far as is practicable.
  - The decision to introduce modifications, whether driven by safety or cyber security considerations, should be taken as a consensus on the basis of consultation with all stakeholders; ie review of changes driven by cyber security should also involve personnel principally responsible for safety, and vice versa.

- User education and awareness

  - User policies should describe the acceptable and secure use of the duty-holder's computer systems. Employment terms and conditions should formally acknowledge the user policies.
  - All users should receive regular training on cyber risks.
  - Specialist training should be provided to system administrators, incident management teams and those undertaking investigations.

- Incident management

  - Incident response and disaster recovery capability should cover the full range of potential incidents.
  - The arrangements should be regularly tested.
  - Incidents and near-misses should be recorded and investigated to identify vulnerabilities and the remedial action necessary to improve resilience.

- Cyber-attacks should be reported to the relevant law enforcement agency to help the UK build a clear view of the national threat and deliver an appropriate response.
- Security delivery principle (SyDP) 7.5 applies to preparation for and response to cyber security incidents.

- Review and update

  - All cyber-security arrangements should periodically be reviewed to take account of any significant changes, potential improvements and operational experience.

13. APPENDIX 7 QUALIFICATION OF SOFTWARE TOOLS

13.1 Software tools are necessary for the development and maintenance of software for CBSIS and can play an important role in ensuring its quality. These tools include, but are not limited to: requirements engineering tools; design tools; development operating systems; transformation tools (eg compilers); verification and validation tools; compliance tools; records keeping, change control and configuration management tools; service tools; and monitoring and diagnostic tools.

13.2 The qualification requirements for an individual tool will be a function of its impact on the target software, and the likelihood that other tools or processes may detect faults introduced by that tool. The combined set of tools should be qualified to a level that preserves the required properties of the target software. One means of tool qualification is to use independent confidence building measures as part of an assessment, to identify the nature of the faults that can be introduced in the target software and their consequences. The qualification process should take into account available experience from prior use.

13.3 Qualification of an individual tool is only valid for a specific version of the tool; any tool revision should be the subject of an impact analysis to determine the extent of the changes and the degree of requalification required.

13.4 Where it is not reasonably practicable to build or obtain monitoring, diagnostic service or maintenance tools that are the same class as the safety system or safety related system they are applied to, it may be acceptable for the tool to be justified at a lower class. However, in such cases, this justification should show that the tool cannot unintentionally undermine the delivery of the safety function. In addition, maintenance, monitoring and diagnostic service tools should be designed such that they protect the independence of measures put in place to separate systems at different defence in depth levels.

13.5 Computer security associated with the use of software tools should be assessed and any necessary measures introduced to eliminate or minimise risks (see appendix 6 on cyber security).

13.6 The compiler of the programming language used to write the software should be validated, its error detection capabilities defined and the code restricted to a safe subset. The same version of compiler should be used on all the software. All software must be retested if regenerated by a new version of the compiler, unless it can be demonstrated that the machine code has not changed. Any compiler code optimisation should be simple and provably correct. Also, the same optimisation options should be used on all the software. Array bound checking should be included.

13.7 The following additional considerations should be applied to the selection and use of software tools:

- The functionality and limits of application of all tools used for the development and maintenance of software for CBSIS should be identified and documented.
- The tools and their output should not be used outside their declared functionality or limits of application without prior justification.
- All tools should be subject to appropriate configuration management.
- Tool parameters used during the development, verification, or validation of baseline equipment or software should be recorded in the development records.

13.8 Further guidance on the qualification and use of software tools is provided in Refs 7, 8 and 9.

14. APPENDIX 8 EXPECTATIONS FOR THE JUSTIFICATION OF COMMERCIAL OFF THE SHELF SMART DEVICES

14.1 The purpose of this appendix is to outline ONR's expectations for the safety justification of COTS 'smart' devices. Smart devices are instruments, sensors, actuators or other previously electromechanical components (eg 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.

14.2 The general principles outlined in this TAG should be applied to smart devices used for safety applications in the same way as they would to any other CBSIS. However, a key difference between the substantiation of commercial off the shelf smart devices as opposed to bespoke computer based systems is the fact that much of the evidence required to underpin an assessment is contained in manufacturer's commercially sensitive intellectual property. The framework set out in this appendix aims to allow for this difficulty as much as possible, while taking advantage of the relatively low complexity of smart device functionality compared to other computer based systems.

14.3 The method developed in the UK for the justification of commercial off the shelf smart devices, through nuclear industry research, is based on IEC 61508 [Ref. 9], which expects demonstration against the requirements of a target SIL. While there is no direct mapping in standards between SIL and safety classification, ONR interprets the link as described in table 1 (see appendix 4).

14.4 Some duty-holders have developed processes for the justification of commercial off the shelf smart devices, which adopt a graded approach to justification based on the safety classification or SIL target of the device under assessment. Before assessing projects where smart devices may be used, assessors should review these processes against the expectations of the multi legged procedure outlined in this TAG.

14.5 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. It is recognised that some duty-holders undertake 'generic' assessments to enable devices to be used in multiple safety applications. While this may be an acceptable approach it is important that the limitations of such assessments are understood and accounted for. In particular, any restrictions on use that may constrain operability within certain operational profiles should be identified. Furthermore, specific applications that take credit for a 'generic' justification should provide an adequate demonstration of the device's fitness for purpose; this may require additional assessment activities to be undertaken (for example, it may be necessary to conduct additional independent confidence building measures that are specifically targeted to use of the device in the chosen application).

PRODUCTION EXCELLENCE

14.6 The expectations outlined in paragraphs 5.21 – 5.28 apply to the production excellence assessment of smart devices.

14.7 In general commercial off the shelf smart devices are developed for general industrial applications, and as such are unlikely to have been specifically developed in accordance with nuclear standards (e.g. Refs 7, 10, 12, 13, 28). The established approach in the UK is for the production excellence of smart devices to be assessed against the requirements of IEC 61508 [Ref. 9]. Assessment to other standards, such

as IEC 62671 [Ref. 38] may be acceptable, but this should be demonstrated to have achieved an equivalent level of breadth and rigour to provide a comparable level of confidence.

14.8 The production excellence assessment should demonstrate that appropriate techniques and measures, informed by the relevant standard(s) and commensurate with the class/SIL of the device under assessment, have been applied throughout the development lifecycle.

14.9 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. In some cases, 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 (for example, a review of staff CVs and qualifications may mitigate the lack of a formal staff development programme). 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.

14.10 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 (for example, the improvement of design documents to show adequate traceability through lifecycle phases, where there exists a robust and pre-existing foundation to be documented). In such cases, a justification should be provided that the activity addresses the gap such that the overall justification is no longer compromised.

14.11 As discussed in paragraph 10.30, ONR recognises that some duty-holders have developed processes and procedures which may provide an alternative approach to substantiation of systems and/or devices with low integrity claims. The use of such processes should be considered on a case by case basis, but the expectation is that they should apply the principles of ESS.27.

INDEPENDENT CONFIDENCE BUILDING

14.12 The expectations outlined in paragraphs 5.29 – 5.37 apply to the selection and implementation of independent confidence building measures for commercial off the shelf smart devices.

14.13 It may not always be practicable to determine independence confidence building measures at the outset of the project, given that details regarding the architecture, language and technologies, as well as the techniques applied during development, may not be known until the production excellence leg has commenced. In such circumstances, the independent confidence building measures will need to be specified once details of the device are understood.

14.14 Currently, there is no comprehensive guidance on the selection of independent confidence building measures to support safety justification, beyond the details provided in this TAG. However, some duty-holders have developed processes for the justification of smart devices that adopt a graded approach to the selection of measures. Table 2 presents an example of such a graded approach, based on the safety classification of the system. Table 2 is not intended to be definitive; there is no agreed generic approach to the selection of measures. The duty-holder should provide a justification for the adequacy of the set of chosen measures, accounting for the device and its application, which ONR will then assess on a case by case basis.

14.15 In certain circumstances, it may be necessary for the duty-holder to vary or broaden the selection of independent confidence building measures to achieve sufficient

confidence in the fitness for purpose of the device. For example, should it be feasible to obtain source code for a device at class 3, ONR's expectation is for static analysis and dynamic analysis to be performed as far as is practicable. Similarly, at class 2, should all reasonably practicable attempts to obtain source code prove unsuccessful, it may be appropriate for the duty-holder to conduct statistical testing, supported by a justification of reasonable practicability as discussed in paragraph 10.24.

14.16 It may be acceptable for the duty-holder to justify a smart device for use at class 3 where it is not possible to obtain access to the device source code. In such cases it would be expected that the independent confidence building measures include a breadth of activities to establish confidence in the device (for example additional dynamic testing).

Table 2 – Example graded approach to the selection of measures to support justification of commercial off the shelf smart devices

	Class 3	Class 2	Class 1 (SIL 3 only)
PRODUCTION EXCELLENCE	There should be evidence of production excellence assessed using techniques and measures appropriate for SIL 1. Application of compensating activities as required to address gaps in production excellence.	There should be evidence of production excellence assessed using techniques and measures appropriate for SIL 2. Application of compensating activities as required to address gaps in production excellence.	There should be evidence of production excellence assessed using techniques and measures appropriate for SIL 3. Application of compensating activities as required to address gaps in production excellence.
INDEPENDENT CONFIDENCE BUILDING MEASURES *NOTE: This list is not exhaustive and does NOT rule out the use of other techniques*	**Example of suitable techniques and measures** Device type tests; Commissioning tests; Examination, inspection, maintenance and testing (EIMT) records; Data on prior use from reputable sources; Evidence of manufacturer pedigree; Device hardware failure modes and effects analysis; **Justification may require the following, as appropriate:** Dynamic analysis of source code; Static analysis of source code; Independent desk top review of source code; Statistical testing; Certification by an independent body (supported by evidence); Independent Functional Safety Assessment (FSA); Independent tool review.	**Example of suitable techniques and measures** Device type tests; Commissioning tests; EIMT records; Data on prior use from reputable sources; Evidence of manufacturer pedigree; Device hardware failure modes and effects analysis; Dynamic analysis of source code; Static analysis of source code; Independent desk top review of source code; Certification by an independent body (supported by evidence). **Justification may require the following, as appropriate:** Statistical testing; Independent FSA; Independent tool review.	**Example of suitable techniques and measures** Device type tests; Commissioning tests; EIMT records; Data on prior use from reputable sources; Evidence of manufacturer pedigree; Device hardware failure modes and effects analysis; Dynamic analysis of source code; Static analysis of source code; Independent desk top review of source code; Statistical testing; Certification by an independent body (supported by evidence); Independent FSA; Independent tool review.