Office for Nuclear Regulation

ONR GUIDE			
CONTROL AND INSTRUMENTATION ASPECTS OF NUCLEAR PLANT COMMISSIONING			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-028 Revision 4		
Date Issued:	September 2016	**Review Date:**	September 2019
Approved by:	D Senior	Director Regulatory Standards	
Record Reference:	Trim Folder 1.1.3.755. (2016/365704)		
Revision commentary:	Routine update		

TABLE OF CONTENTS

Published 09/16

1. INTRODUCTION

1.1 ONR has established its Safety Assessment Principles (SAPs) which apply to the assessment by ONR specialist inspectors 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 ONR's inspectors in their technical assessment work in support of making regulatory judgements and decisions. This technical assessment guide is one of these guides.

2. PURPOSE AND SCOPE

2.1 This guide aims to assist ONR C&I specialist inspectors in judging the adequacy of plant commissioning arrangements with respect to nuclear safety. It is worth stressing that the guide is for the specialist inspector, not the commissioning engineer, so it does not deal with detailed commissioning practice. The inspector's task is to be satisfied that, for nuclear safety concerns, the licensee has in place both the intent and the means to achieve proper commissioning, so the guide addresses those aspects that allow these factors to be established.

2.2 There are of course many interfaces and responsibilities involved in commissioning, not only within the licensee's organisation but also within ONR. These are mentioned in outline in order to set the C&I specialist inspector's work into its proper context.

2.3 This TAG contains guidance to advise and inform ONR inspectors in the exercise of their professional regulatory judgement. Comments on this guide, and suggestions for future revisions, should be recorded on How2.

3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

3.1 Licence Condition 21 (Commissioning) applies in particular.

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

4.1 This guidance enlarges on that guidance provided in the SAPs [2], notably Principle ECM.1 and its associated discussion paragraphs.

4.2 Commissioning is mentioned in the WENRA Reference Levels document, generally with respect to the need to carry out commissioning in relevant circumstances, but details of how it should be conducted are not included.

4.3 The guidance in this document is consistent with the high-level commissioning guidance provided in IAEA safety guide SSG-39 'Design of Instrumentation and Control Systems for Nuclear Power Plant' [6].

5. ADVICE TO INSPECTORS

5.1 Objectives of commissioning

1) "Commissioning" is defined by Site Licence Condition 1.1, namely "the process during which plant components and systems, having been constructed or modified, are made operational and verified to be in accordance with design assumptions and to have met the appropriate safety criteria". Put another way, commissioning consists of the in-situ testing of equipment and systems that have not yet contributed to normal operation of a plant. It is carried out in order to verify that all systems meet their design functional requirements and achieve a satisfactory performance. Any shortcomings are to be revealed and corrected.

2) Commissioning in general is primarily concerned with proving functionality, and the C&I specialist inspector's task is concerned with the subset of activities relating to nuclear safety, i.e. he is concerned with the commissioning of C&I systems providing nuclear safety functions.

3) In particular, commissioning should include the setting to work of systems, validation of design assumptions, proving of system capability at all stages of integration, validation of operating, emergency and maintenance procedures, verification and optimisation of overall performance, and the training of personnel. With respect to nuclear safety, the functionality of all C&I safety systems should be established and where, in the Design Safety Report (DSR) or its equivalent, there are testable safety claims, then they should be confirmed during commissioning. The licensee's procedures should indicate how all such instances are to be identified

4) A summary of the objectives and principal features of C&I commissioning is provided below:

i) Commissioning should follow an orderly process, the scope of which is defined in a schedule.

ii) The starting point in producing a commissioning schedule is the development of a commissioning strategy, which defines the intended testing scope, and justifies its sufficiency, taking into account the safety importance of the associated system and the known extent of pre-installation testing. The commissioning schedule should define clear acceptance criteria.

iii) The scope of commissioning does not normally extend to the testing of the internal sub-system functions in isolation, although evidence (at some level, depending upon the safety importance of the system) of their satisfactory testing (eg prior to commissioning) would be an expected component of the safety case. In the case of a safety system, the licensee should be able to demonstrate that, within the total testing which the system has experienced (ie commissioning together with all recorded earlier testing), every function of the existing system has been tested successfully at least once, and that testing has not been invalidated by any subsequent changes.

iv) Testing of C&I system-level functions should be carried out against the requirements specification (and the additional system-level features emanating from the system design specification) to demonstrate correct operation as an integrated plant system.

v) Commissioning activities may take place at various stages during the construction of a plant since, once an item is installed, the testing of aspects of its functionality (eg leak tightness, the required responsiveness of a gas detector, the calibration of a remote position measurement system, etc) may need to be undertaken before access becomes impeded by the installation of other plant items.

vi) Validation in the actual plant configuration of the required relationships between measured variables and safety parameters is required, eg by comparing samples with measured concentrations and predicted values for process materials.

vii) Commissioning provides an opportunity to train the maintenance and operational staff, and similarly to confirm the details of the training necessary to give new personnel the required competencies.

viii) Diagnostic facilities and the practicabilities of on-line maintenance should be confirmed.

ix) Commissioning, because of its nature and duration, does not lend itself to proving of system reliability targets, although achievement of a lower reliability bound might, in principle, be demonstrated.

x) Checking of the completeness and useability of system manuals/drawings and procedures should be included.

Discussion

1) The basic philosophy should be to MAKE NO ASSUMPTIONS. All plant items from individual components to integrated systems should be proved, under the full range of operating conditions (including reasonably foreseeable or all identified fault conditions) likely to be encountered, and safety systems that are required to function under unusual or adverse conditions should be tested under these actual or simulated conditions.

2) The above represents a doctrine of perfection, and can never be achieved fully during the commissioning phase of a project, but the aim should be to come as close as possible, especially for safety systems. The C&I specialist inspector should check accordingly, and seek additional tests or explicit justification where there are significant shortfalls. The licensee should have in place:

i) a safety justification for the adequacy of commissioning, with supporting fault analyses where there is significant fault potential;

ii) a schedule of specific commissioning tests that encompass all C&I equipment and systems, and which will prove the C&I design assumptions that are associated with safety;

iii) effective QA & management structures with defined responsibilities;

iv) appropriate lines of communication;

v) interface arrangements for handover from the construction phase;

vi) staff training and qualification procedures, with strict allocation of technical responsibilities;

vii) database facilities with controlled access for information recording and retrieving;

viii) linked documentation to tie all aspects together into a coherent whole and to allow for evolution as experience is gained;

ix) related security features, eg access control arrangements to prevent unwanted interference with equipment or systems; and

x) documentation covering;

a) all commissioning test procedures for each phase with statements detailing the objective of each test, appropriate acceptance criteria, prerequisites and post-test actions;

b) QA arrangements and record keeping including traceability and the establishment of audit trails;

c) management of joint activities where more than one department is involved;

d) fault management, including contingency plans for unexpected events with potential to impact on safety;

e) temporary and permanent modifications;

f) specialist measures for dealing with novel processes or systems (the tests for which will need to incorporate type testing to some extent);

g) validation of maintenance procedures;

h) confirmation of assumptions and testable claims made in the design justification;

i) the demonstration that no component or system is depended upon for safety purposes until it has been fully tested; and

j) justification of adequate safety when a system may be required to function without associated systems or components that would normally be present.

3) Commissioning should be a confidence building process carried out in a bottom up manner through gradually increasing levels of integration of systems. There should be clear phase demarcations separating the levels, and especially before the introduction of radioactive material, which will normally be a regulatory hold point. At this time a high level of confidence in the integrity of involved systems is required, in order ensure that the associated risks are ALARP. Special conditions will apply at such times, since the plant may be only partially functional, and the radioactive material may be handled differently than during normal operation. The licensee must show that all credible risks have been considered, and that all systems needed to maintain safety have been properly commissioned and are functional. This applies to supporting service functions such as ventilation, electrical supplies, instrument air, and supply of inactive materials such as feedstocks.

C&I assessment guidance

1) ONR C&I assessment is generally undertaken as part of a much wider commissioning assessment co-ordinated by a project officer or site inspector. Many aspects of this wider assessment have been outlined above and are addressed by Licence Condition 21 and its guidance. Although there are specific C&I matters that are directly the concern of the C&I specialist inspector, there are many more aspects that C&I either interfaces with or is a part of. Liaison with other relevant inspectors is therefore essential to ensure adequate understanding of the processes involved. It is recommended to approach the assessment in a top-down manner, considering first all aspects of safety and function, and only then becoming involved in specific C&I detail, rather than by attempting to consider C&I in isolation. In this way the behaviour of the plant remains paramount, and the C&I systems are assessed with this behaviour in mind.

2) General questions to be answered from the C&I point of view include:

i) Are the proposed tests able to fulfil their intended functions.

ii) Are the safety system tests adequate in scope & detail.

iii) Does the paperwork address all aspects adequately.

iv) Has a structured & methodical approach been adopted for the testing of all systems, in particular for those embodying complexity.

v) Are safety systems being commissioned adequately prior to introduction of radioactive materials into the facility.

3) Subsystems will have generally been tested to some extent at manufacturers' works prior to shipping, but inspectors should take into account that many aspects of these tests may have focused on contractual purposes and are therefore not normally claimed as part of the commissioning tests. If any such claim is made then where relevant these tests should be assessed in the same way as the site tests.

4) It is normal during commissioning to have only parts of systems functional, so that much of the testing is carried out in circumstances that are different to those that will prevail during operation. In such circumstances dummy inputs and outputs are used, systems are forced into unnatural configurations, and assumptions are made about interfacing systems, all of which need to be shown not to invalidate the tests. The C&I specialist inspector should examine such cases carefully and challenge the assumptions where there is doubt, since system behaviour is often different under fully dynamic operation than during relatively static testing.

5) A reasonable range of "robustness" type tests should be included during which systems are subjected to a certain amount of stress testing. This applies especially for systems that interface with operators. For example, inputs should be applied in the wrong order and all at once; range end values should be applied; zero, out of range, and invalid values should be used; and values corresponding to failed sensors. The aim is to give confidence that the system can tolerate operator and interfacing systems faults without becoming deadlocked or failing in some other way. The scope of such testing should be related to the complexity and safety criticality of the system; the more complex or safety critical, the wider the scope. Such tests should be within the scope of the system specification where it explicitly requires particular performance under abnormal conditions, but the absence of such explicit aspects in the specification should not preclude such testing, since these aspects of system performance can easily be overlooked or regarded as implicit requirements by the system specifier.

6) Ergonomic aspects (including task analysis assumptions) of control stations should be tested in conjunction with Human Factors specialists, as should other operator interacting arrangements such as alarm response strategies.

7) The extent of input and output range and combination testing should be examined, since usually only part ranges and relatively few combinations are tested, it being assumed that all others will behave appropriately. Generally, the greater the dependence for safety upon a system, the greater the required extent of such testing.

8) It should be verified that at some stage during the integrated testing full end-to-end tests (including logic, sequence, and timing aspects) are carried out for instruments, controls and protection systems, ie from sensor to display and/or actuator. It should be ensured further that no system required for safety purposes is depended upon for its safety function until such tests have been carried out fully.

9) Duration tests should be included for equipment that must function for prolonged periods. A system may function effectively for a few minutes but this is an inadequate test if it will be required to run for hours. Problems such as overheating or vibration are likely to be revealed only by a suitably long operating test.

10) Power failure tests should be included for complete plant areas, and fuse failures simulated in order to cause partial power failure (partial failure can be worse than complete failure since some equipment may still operate even though the equipment interfaces are unavailable). These tests should also include supply fluctuations where equipment behaviour is sensitive to such fluctuations.

11) Software controlled systems should be subjected to special tests and procedures. These should cover as wide a range of operating circumstances as possible, since the possibility of design errors may be greater for software systems (due to the fact that they tend to be more complex than hardware systems) and extensive testing (often combined with rigorous analysis and verification procedures) are required to provide confidence that the risk of failure due to such errors has been adequately addressed prior to operation. Procedures should be devised and approved to cater for configuration control, temporary and permanent modifications, access control and software security; to prevent unauthorised changes and to safeguard against cyber-attack. Temporary modifications may be set up within the software to facilitate the testing of specific functions. These should only be introduced when unavoidable and a log maintained to show their status. The associated procedures should not allow the temporarily modified software to have the changes removed, but should require the reloading of original software and the modified version to be discarded; to avoid the potential for error introduction during the modification removal stage.

12) Where there are data highways (generally but not always associated with software systems) data overload tests should be carried out to verify the capacity and time response of the receiving system during periods of high activity. There should be a comfortable margin between maximum capacity and expected loading.

13) Validation of periodic proof tests should be carried out, both to establish the effectiveness of the proposed procedures (possibly by inclusion of seeded faults where there are doubts), and to confirm any assumptions that are implicit in the proof tests themselves. In some cases, it may be impracticable to permit a function to be tested during plant operation and it may be necessary to, for example, provide a substitute to check that a relay contact is made by confirming a short circuit between two terminal points. In such cases the assumption is that the terminal points are appropriate places to introduce such a short circuit, and the proof test validation procedure (performed when plant is not operational) should establish full end-to-end correct operation.

14) Records of temporary modifications should be maintained and procedures implemented to ensure that systems are reinstated correctly, (see above for removal of temporary software modifications by the reloading of original software).

15) Where there are variable set points for control, protection or warning functions, tests should be carried out to verify correct function for values across the full range of setpoints intended to be used in practice.

16) Sensitive systems should be tested for susceptibility to electromagnetic interference, including electrostatic discharge. This applies especially where high power electrical equipment or cables are in close proximity to such systems.

17) Where, after malfunction, operators are required to carry out diagnostic procedures, commissioning tests should be included to validate expected plant behaviour during such procedures.

18) If a plant simulator is to be used to assist in carrying out control system tests, and if its accuracy is depended upon to any extent for safety, its fidelity should be established by specially designed validation procedures.

19) Calibration procedures for temporary and permanent measuring instruments should be shown to be comprehensive and reliable, and such procedures should address instrument identification, certification, operation and calibration (at appropriate intervals).

6. REFERENCES

Licence condition handbook. Office for Nuclear Regulation Web site.
http://www.onr.org.uk/

Safety Assessment Principles for Nuclear Facilities. Office for Nuclear Regulation Web Site
http://www.onr.org.uk/

IAEA Specific Safety Guide SSG-39 Design of Instrumentation and Control Systems for Nuclear Power Plant.
https://www.iaea.org

7. GLOSSARY AND ABBREVIATIONS

ALARP	As Low As Reasonably Practicable
CCF	Common Cause Failure
C&I	Control and Instrumentation
HSE	Health and Safety Executive
IAEA	International Atomic Energy Agency
ONR	Office For Nuclear Regulation
SAP	Safety Assessment Principle(s)
SCC	Structures, Systems and Components
QA	Quality Assurance
TAG	Technical Assessment Guide(s)
WENRA	Western European Nuclear Regulators' Association