Office for Nuclear Regulation

OFFICIAL

ONR GUIDE			
Procedure Design and Administrative Controls			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-060 Revision 2		
Date Issued:	November 2014	**Review Date:**	November 2017
Approved by:	D Senior	Director of Regulatory Assurance	
Record Reference:	TRIM Folder 1.1.3.776. (2016/301017)		
Revision commentary:	Revision		

TABLE OF CONTENTS

Published 11/14

1. INTRODUCTION

1.1 The Office for Nuclear Regulation (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 (TAG) is one of these guides.

2. PURPOSE AND SCOPE

2.1 ONR has the responsibility for regulating the safety of nuclear installations in Great Britain. The SAPs for Nuclear Facilities [1] provide a framework to guide regulatory decision-making in the nuclear permissioning process. The SAPs are supported by TAGs which further aid the decision-making process.

2.2 This TAG provides guidance to aid Inspectors in the interpretation and application of SAPs related to procedure design and the use of administrative controls, specifically SAPs EHF.4 and EHF.9. It also assists with the application of other SAPs which set out expectations regarding administrative safety measures and procedures designed and implemented by a dutyholder, including those related to compliance with Operating Rules.

2.3 The TAG provides broad expectations on key points that the experienced Human Factors (HF) Inspector may wish to consider when judging whether a licensee's procedures and administrative safety controls are designed and implemented effectively. This TAG is not intended to be a detailed design guide for procedures and administrative controls; nor does it prescribe specific methods and approaches for assessing them or offer guidance on how to judge the adequacy of their technical content. Inspectors should exercise their own judgement and discretion in the depth and scope to which they apply the guidance, but should be cognisant of the safety reliance that is placed on human action and the contribution that failure to implement the administrative controls and procedures makes to risk.

Procedures and Administrative Control

2.4 SAP EKP.5 sets out a hierarchy of preferred options for delivering safety functions and maintaining the plant within its safe operating envelope. The SAP identifies the preference for passive safety measures, but sets out alternatives including the use of administrative safety measures where an engineered control is not possible or reasonably practicable to implement. Where administrative safety measures are proposed, the safety case should include a robust justification demonstrating why alternative measures are not reasonably practicable, and showing that claims on the administrative safety measure can be substantiated.

2.5 Procedures form an essential part of any administrative safety measure. The mechanisms in place to ensure that procedures are designed in accordance with good practice HF guidelines, such that they support the end user and reflect safety case requirements will influence the reliability with which safety significant tasks are controlled and should form part of the substantiation. Administrative safety measures may be defined as Operating Instructions in accordance with Licence Condition (LC) 24(1).

Definitions

2.6 This TAG uses the term ‘procedures’ to refer to all written instructions that describe the way in which operations affecting safety should be carried out. The term ‘Operating Instruction’ is used within LC 24. Licensees use a range of terminology for LC 24 operating instructions and this term is generally taken to mean, but is not limited to, procedures. As much of what is carried out on operating sites is controlled by lower level documents that support ‘operating instructions’ the term ‘procedures’ has been used to indicate the broader application of the guidance within this TAG.

2.7 Administrative control within this TAG refers to a safety measure that is claimed to maintain operations within the plant’s safe operating envelope derived from the safety case, and which is implemented by operator action

3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

3.1 The Nuclear Site LCs [2] place legal requirements on the licensee to make and implement arrangements to ensure that safety is being adequately managed. The licence conditions provide a legal framework which can be drawn on in assessment.

3.2 LCs 23 (limits and conditions in the interests of safety) and 24 (Operating Instructions) particularly apply. Also of relevance are LCs 14 and 15 (preparation and review of safety cases), LC 11 (emergency arrangements), LC 17 (quality assurance), and LC 28 (examination, inspection, maintenance and testing). Most other licence conditions also touch on the topic of procedures and administrative controls. Procedures providing guidance and instruction to staff are instrumental in ensuring that all activities throughout the life cycle of an installation are carried out reliably and efficiently such that the potential for introduction of errors is minimised.

3.3 Regulation 3(1) of The Management of Health and Safety Work Regulations 1999 places a legal requirement on dutyholders to produce suitable and sufficient risk assessments and Regulation 4 the requirement to introduce preventive and protective measures to control risk. In order to be considered suitable and sufficient, such assessments may need to identify and consider the need for and influence of, suitable and sufficient procedures and administrative controls as part of the dutyholder’s measures for controlling risk.

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

ONR’s SAPs and the WENRA reference levels were re-issued in 2014. This TAG will be updated to reflect these changes in due course and in the meantime inspectors need to check that they are using the correct versions of those publications during their assessments.

SAPS

4.1 ONR’s expectations concerning the adequacy of administrative controls and procedures are set out in a number of SAPs. The primary references relating to procedures and administrative controls are contained in the following SAPs [1]:

4.2 EHF.4. Identification of administrative controls:

“Administrative controls used to remain within the safe operating envelope should be systematically identified”.

4.3 Para 378 expands upon EHF.4:

The design of these controls should be such that the requirements for personnel action are clearly identified and unambiguous to those responsible for their implementation.

4.4 EHF.9 Procedures

"Procedures should be produced to support reliable human performance during activities that could impact on safety".

4.5 Para 388 expands upon EHF.9:

Procedures should be accurate and designed and presented in a format that is compatible with the needs of the end user and suitable for the task that they are designed to support.

4.6 References to procedures and administrative controls, either implicit or explicit, are also noted throughout the SAPs in general, and these are presented in Annexe A.

WENRA Reactor Safety Reference Levels

4.7 The objective of The Western European Nuclear Regulators Association (WENRA) is to develop a common approach to nuclear safety in Europe by comparing national approaches to the application of International Atomic Energy Agency (IAEA) safety standards.

4.8 The guidance in this TAG is consistent with the following harmonisation issues from the WENRA Reactor Safety Reference levels [3], which represent good practices in the WENRA member states, are relevant and should be taken into account by the inspector:

- Issue H: Operational Limits and Conditions (OLCs).
- Issue K: Maintenance, In-Service Inspection and Functional Testing.
- Issue L/M: Emergency Operating Procedures and Severe Accident Management Guidelines.
- Issue O: Probabilistic Safety Analysis (PSA).
- Issue Q: Plant Modifications.
- Issue S: Protection against Internal Fires.

IAEA Safety Standards

4.9 The guidance is also consistent with the following IAEA safety requirements and guidance:

NS-R-2: Safety of Nuclear Power Plants: Operation Safety Requirements, 2000 [4]

SSR-2/2: Safety of Nuclear Power Plants: Commissioning and Operation Specific Safety Requirements, 2011 [5].

NS-G-2.4: The Operating Organisation for Nuclear Power Plants Safety Guide, 2001 [6].

NS-G-2.14: Conduct of Operations at Nuclear Power Plants Safety Guide, 2008 [7].

4.10 The IAEA Safety Standards (Requirements and Guides) were the benchmark for the revision of the SAPs in 2006 and are recognised by ONR as relevant good practice. They should therefore be consulted, where relevant, by the Inspector.

5. ADVICE TO INSPECTORS

Introduction

5.1 LC 24 requires that all operations which may affect safety are carried out in accordance with written instructions. The licensee should be able to demonstrate that its administrative controls and procedures are designed and implemented such that they support reliable human performance of actions that keep the plant within the safe operating envelope. The guidance provided in this section can be used to assess all types of procedures and administrative controls.

General Expectations

5.2 Inspectors should seek to gain confidence that safety claims made upon administrative controls and procedures can be substantiated. This may involve considering:

- the dutyholder's process for identifying the need for administrative controls and procedural support within the safety case;
- its capability – often embedded in its HF resource - to support effective specification and design of administrative controls and procedures, drawing upon a proportionate use of task analysis;
- the processes in place to ensure that administrative controls and procedures are implemented effectively and are subject to suitable management controls, for example configuration control and review of modifications;
- learning from experience, for example implementing appropriate improvements following events, feedback for personnel following use (during operation, training, drills, etc.), periodic reviews of safety, etc.

5.3 Claims on administrative control should be identified and assessed from a HF perspective in all operating states commensurate with their risk. Where a high reliance is placed upon the administrative control, it would be expected that a detailed HF assessment involving the use of task analysis would be conducted and robust justification made for the usability and reliability of that control. ONR expects HF/ergonomics principles and practices to be incorporated in the design, specification, implementation and through-life management of procedures and administrative controls. It should be noted that procedures are only one of the factors affecting the reliability of operator action associated with implementation of administrative controls. Other factors such as Human-Machine Interface (HMI), task design, supervision and training will also be relevant, and the Inspector should recognise this when defining interventions.

5.4 Key elements for ensuring the provision of suitable and sufficient administrative control and procedures to support the safe operation of nuclear plant include explicit consideration of:

- The safety goal to be achieved,
- The nature of the task and human-based safety claim related to the delivery of administrative safety functions

- The needs of the end user

5.5 Inspectors may consider whether:

- The dutyholder's process for the identification of administrative control requirements draws upon the safety case and covers all plant operational modes/states including maintenance, testing and calibration activities, override facilities, fault and emergency response.
- Where appropriate, the dutyholder's administrative controls take into account the need to demonstrate compliance with conditions and limits necessary in the interests of safety; detect non-compliance and facilitate the successful performance of recovery actions. This includes factors such as supervision and surveillance tasks, compliance records, alarm set points, the communication of time constraints associated with non-compliance, operator awareness and training about the safety limits and conditions.
- Administrative controls and the associated safety-related activities that operators need to carry out to achieve compliance with operating rules are clearly identified as such in operating instructions. The instructions clearly state what needs to done, when, by whom, under what circumstances, the success criteria for each activity and actions to be taken if an operating rule is breached.
- The specification and design of administrative control (and procedures) is included as part of the dutyholder's Human Factors Integration (HFI) process (see Technical Assessment Guide T/AST/058 – Human Factors Integration [8]).
- The dutyholder has declared and justified the standards/guidelines used for the design/modification and substantiation of its administrative controls.
- The actions being claimed are
    - feasible,
    - potential for human error is identified and minimised to As Low As Reasonably Practicable (ALARP) and
    - the actions can be carried out with an appropriate level of reliability given the equipment, procedures and operator interfaces provided.
- The dutyholder has considered each individual administrative control to consider management of safety issues that can contribute to the adequate implementation of the controls, such as competency assurance and management actions to ensure compliance. The following aspects should be evident in the dutyholder's design of administrative controls:
    - Task requirements, potential for errors/violations and demands placed upon operators are clearly identified and understood;
    - Adequacy of the supporting systems, such as the interfaces and procedures that operators are reliant on to implement the administrative control;
    - Competence levels and training of operators to perform the task;

  - Task environment/context including Performance Shaping Factors and the prevailing safety culture to support operator performance.
- The dutyholder's arrangements include elements of evaluation, verification, validation and review.
- The dutyholder has carried out an operational experience review (existing or similar plants), including a review of any simulations or mock-ups of its proposed administrative controls.
- The dutyholder can demonstrate that the design and specification of administrative controls has been used as an input to the design of procedures and operator training needs/competence requirements.
- The dutyholder has conducted suitable evaluation and testing/trials of the design, specification, implementation and use of administrative controls and procedures to demonstrate their effectiveness in the context of the safety case claims and assumptions.

Dependency in claims on administrative control

5.6 The impact of dependency on the reliability of the administrative control should be considered as this is an importance failure mechanism that is often overlooked or inadequately defended against. Whilst the design of administrative controls should aim to minimise dependency, it can be difficult to identify, or eliminate, all forms of dependency in human actions, such that claims on multiple human actions to offer high levels of protection are likely to be unrealistic. Claims on several 'independent' administrative controls in order to claim an unrealistically high level of protection should therefore be avoided.

5.7 Inspectors may consider whether:

- The dutyholder has identified dependent failure mechanisms associated with its administrative controls and has implemented credible defences and mitigations against dependency where these effects are identified.

Assessment of administrative controls

5.8 This section provides general advice to the Inspector regarding good practice expectations for the assessment and substantiation of administrative controls. The guidance provided in T/AST/063 on Human Reliability Analysis is also relevant.

5.9 Inspectors may consider whether:

- Where a high reliance is placed on administrative control or it delivers an important safety function, the dutyholder has used task analysis and drawn upon end user input to understand the task and demonstrate the suitability, feasibility and reliability of the associated operator actions and managerial arrangements. These include but are not limited to:
  - The operating instructions and the extent to which they clearly and unambiguously prescribe any required actions and success criteria for the administrative controls.
  - Performance shaping factors and error mechanisms associated with context in which administrative controls are implemented including, where appropriate, the dynamic nature of these.

- The provision of adequate human-system interfaces; in providing indication of safety-related parameters and their associated operating limits, whether in a central control room or local-to-plant.
- Operator awareness of the required actions and their role as defined within the safety case.
- Operator training and competence for the specific tasks to be performed.
- The prevailing culture within the relevant parts of the operating organisation.

- Where feasible, the dutyholder has used simulator trials to support the analysis of administrative controls. Alternatively, the dutyholder has conducted walk-through/talk-through or observation of the use of administrative controls to confirm that users are familiar with the controls and fluent in their use.

Other Administrative Controls

5.10 The Inspector should note that administrative controls with an impact on safety extend beyond those directly involved in the execution of activities such as operations or maintenance. These include, for example, controls such as Permit to Work, use of waivers, temporary instructions etc. The Inspector should seek confidence that the licensee's arrangements for these other controls are adequate.

5.11 Inspectors may consider whether:

- The dutyholder has a system to identify and assess administrative controls indirectly or implicitly claimed to provide assurance of the level of protection assumed within the safety case.
- The dutyholder has adequately substantiated the robustness and reliability of the following where they are claimed, either implicitly or explicitly, to provide adequate nuclear safety:
  - Administrative controls used for configuration and surveillance and maintenance of automatically initiated engineered safety systems.
  - Administrative controls used as a substitute for an engineered safety system e.g. during a planned or unplanned outage, or for short-term high risk activities.
  - Temporary instructions, workarounds and/or Permit-to-Work systems that may be used to implement temporary safety measures as an alternative to provide adequate safety during unplanned engineered safety system outages, or to act as the controls for non-routine hazardous activities.
  - Override facilities; safe use of overrides and vetoes is dependent on effective administrative control. Inspectors should check that the administrative control arrangements ensure that operators understand the plant state and any change in plant state associated with the requirement for and application of an override and that is recognised by all personnel who may at risk in order to avoid inadvertent actions being taken and unintentionally creating a significant hazard.
- The dutyholder has adequate arrangements for conducting periodic audit to ensure that the level of control can be (and is being) maintained over a period of time.

Procedures

5.12 This section is intended to supplement Technical Inspection Guide (TIG) NS-INSP-GD-024 [9] (LC 24 Operating Instructions) rather than repeat the information contained therein. It is recommended that the reader also refers to NS-INSP-GD-024 as part of their inspection and/or assessment.

General Expectations

5.13 All activities which may affect safety should be carried out in accordance with written procedures. However, carrying out activities in accordance with procedures does not necessarily mean that there must be a procedure in hand, followed step by step for every task. Decisions on the way that procedures are used to support consistent and reliable task performance must be based on the nature of the task, its safety significance, the potential for error and the experience of the user. The inspector should consider whether:

- The dutyholder's operating instructions are consistent with any operating rules they implement. This includes any procedures that provide indirect support to operating rules, such as those involved in the maintenance of safety related plant.
- The dutyholder's procedures define how plant should be brought back within operating rule limits and conditions if discovered to be outwith these.

Management arrangements

5.14 It is also important for the inspector to recognise the role of lower level procedures in assuring safety, as the presence and use of these is often implicitly assumed within the safety case. The dutyholder is expected to consider the role of such procedures in delivering safety. Inspectors may consider whether:

- The dutyholder has a controlled process for the production, maintenance, review, amendment and version control of procedures. Mechanisms are in place to ensure that the safety case is not undermined by subsequent changes to procedures and vice versa
- The dutyholder has a process for validation and verification of procedures, which includes: end user involvement, consideration of the way they are used to confirm their technical accuracy and usability.
- Consideration of assumptions within the safety case to ensure that the safety case is not undermined.
- The dutyholder has a process of learning from experience to ensure procedures are appropriately revised based on use. Changes that are made as a result of this process should be evaluated to ensure that the procedure has delivered its intended improvement.
- The dutyholder's modification and change management process has the capacity to identify all design, organisational and safety case changes that may impact procedures and the process should have the capacity to identify procedures that are obsolete.
- The dutyholder can demonstrate the suitability and sufficiency of the procedure to support safe and reliable task performance. For example, through implementation of a hierarchy of procedure classification relating to the safety significance of the operations, its complexity and frequency to inform the

assignment of a category of procedure format, use and availability. This may include ‘use categories’ similar to the following:

- Level 1 – Continuous use; where the procedure is ‘in-hand’ and referred to step by step each time the task is performed.
- Level 2 – Reference use; the procedure is available at the work location and may be referred to periodically during the performance of a task and relevant blocks of task steps are verified to confirm that all steps have been completed.
- Level 3 – Information use; the procedure is available for use as needed.

- The dutyholder maintains accurate records to demonstrate compliance with operating procedures in line with LC 24(1)
- The dutyholder’s procedures are clearly linked with the claims and assumptions in the safety case and the procedures have been developed based on the output of the Design Basis Analysis (DBA), PSA and Safety Assessment (SA), appropriate to the specific procedures.

Procedure Design and Methods

5.15 The development of technically accurate and usable procedures will rely on the application of appropriate methods such as task analysis and on the quality of the verification and validation processes. Engaging procedure users in the development and amendment of procedures will also increase both the accuracy and validity of the procedure. The rigour applied to the development of procedures should reflect the relative contribution to safety of the task being controlled. The methods adopted should be appropriate to the nature of the task or process.

5.16 Inspectors may consider whether:

- The dutyholder uses a systematic and defined process to develop procedures and this includes proportionate use of internal and/or external standards or guidelines and the practices listed below, to ensure the uptake of relevant good practice in procedure writing and to ensure consistency of presentation and format (see for example references [10], [11] & [12]).
  - Task analysis.
  - Desktop or walk-through/talk-through approaches, wherein operators use the procedures and verify their accuracy and suitability for the task and the options available to them at each step.
  - Simulator, or some other high fidelity method, is used wherever possible and in particular for post-fault actions.
- The dutyholder has a responsive approach for updating procedures, from the user point of view. This is important to motivate change where it is needed. This process identifies the safety implications of such changes to ensure that the safety case is not undermined.
- The dutyholder is able to demonstrate that the standard of procedures used by contractors is commensurate with what is expected from the dutyholder’s own internally developed procedures.
- The dutyholder uses its procedures to inform the identification and delivery of competence and training needs associated with particular tasks to ensure that these are clearly defined and that associated procedures do not assume any knowledge and skill for which the user has not been trained and is competent to carry out. The process also includes any unfamiliar/infrequently used

procedures e.g. annual maintenance instructions, fault and emergency response procedures.

- The dutyholder has clearly identified roles and responsibilities with regard to procedures. There is a reasonably practicable process for ensuring that procedure compliance is assured and demonstrated and this covers management expectations about compliance.
- The dutyholder's procedures are provided in an appropriate format.
    - Procedures should provide suitable navigation aids and be consistent in their use of cautions, warnings, hold points and independent verification to control safety significant task steps.
    - A "one size fits all" approach to procedure formatting is unlikely to be appropriate. For example, an appropriate procedure format for use in normal operations might be very differently from one to be used following an accident / incident. Different formats might be appropriate to support the specific task requirements (e.g. sequential for normal operations, symptom-based for design base faults, state / event based for severe accidents, etc.).
    - Procedures should also support their users through the potential difficult transition between normal and abnormal conditions (and back again). It should be clear to the user the appropriate procedure they need to use in response to the specific scenario they face.
    - Where independent verification is used, it should be clear what is being checked and how, such that any sign-off is meaningful to the verifier. The procedure user should be made aware of the significance of the step through its clear demarcation within the procedure and through training.
- The dutyholder can demonstrate an understanding of safety significant task steps in the procedures and any errors that may occur; these have been given consideration in the design and maintenance of procedure quality.

Plant Commissioning Procedures

5.17 The general expectations for procedures, their design and methods of production equally apply to procedures that are used for commissioning. However, during commissioning operations are often performed with the plant in unusual and changing configurations. Procedures must still be available under such circumstances. Commissioning procedures are likely to be more detailed and require the bases of the contents of the procedure to be explicit. During later operation, once the procedures have been tested in use, this additional detail may no longer be required within the procedure itself. The dutyholder should detail the bases upon which the commissioning procedure content is decided and verified. This should also be linked to the safety case, training and competency assessments.

Computerised Operating Procedures

5.18 Advances in digital technology are resulting in increasing availability of Computerised Operating Procedures (COPs), for assisting operators with various plant control tasks, fault diagnosis and response [13], [14]. The purpose of this section is to provide high level guidance to inspectors where the licensee proposes to use such systems.

5.19 ONR considers COPs to be any computer application that presents operating procedures/instructions through electronic, rather than printed, media. This is taken to include procedure-based automation whereby the evaluation and execution of a

predefined sequence of procedure steps is carried out by a computerised operating system.

5.20 In their simplest form, computer-based procedures simply represent the procedure text in electronic form. This type of COPs may include the ability to call up another relevant procedure from a hyper-link in the procedure and allow the user to track progress through the procedure steps. More sophisticated COPs may automate the gathering and display of plant data relevant to a task and procedure step. They incorporate additional functionality such as automated data gathering and processing capability, evaluation of plant parameters and procedure step logic, and the display of the results to the operator to support decision-making and/or prompt the operator to take a specific action. This type of COP may also provide links to soft controls where operators may take plant control actions.

5.21 Further advanced COPs include all the functionality above and also have the ability to issue plant control commands and automatically carry out a pre-defined sequence of procedure steps once authorised by the operator. This type of COP can make decisions as to whether and when to execute each step in the procedure sequence based on real time plant conditions.

5.22 Regardless of the type of COPs proposed by dutyholders, it is important to recognise that operators are responsible for the proper application of any procedures and COPs are an operator aid for controlling the plant. In the case of automatically executed actions it is expected that this is flagged to the operator in such way that he can reach a judgement on their suitability. Loss of an aid should not prevent the operator from performing any required safety and control actions. In addition, failure of COPs should not have any impact on safety systems or control systems.

5.23 The same general principles applied to the design of paper-based procedures also apply to COPs in terms of presentation principles, processes for updating, verifying and validating etc. However, there are other specific issues that must be addressed if COPs are to be used including the consideration of Human Machine Interface (HMI) and software design and verification [15] – [19]. (See also NS-TAST-GD-059 – Human Machine Interface [20]).

5.24 Where the dutyholder uses, or proposes to use, COPs, Inspectors may consider whether:

- The choice and use of COPs is appropriate for the operational concept, tasks and safety functions to be delivered.
- The COPs are designed and implemented such that operators remain in command of the plant and processes being operated. Operator pre-defined hold-points are included in the COP that defines the start and end of any automated sequences that are commanded by the operator.
- The operator should be able to manually interrupt a COP execution safely and at any point in a sequence of steps. Any automatic interrupts include a salient alerting function and identify the cause of why the sequence has stopped. The operator should be able to revert to manual control or resume automatic procedure execution if desired.
- COPs provide adequate information on initial plant conditions that must be met before any automated sequence may be started.
- COPs that process plant data and evaluate procedure-step logic can only make deterministic decisions (e.g. yes/no) and all data evaluated by a COP is available to the operator. The results evaluated by the COP are the same as those expected from operator evaluations of the same procedure steps.

- Failure modes or loss of the COP can be readily detected and identified by operators and these do not affect the operator's ability to safely recover and operate the plant.
- COPs should not determine what procedure should be used; the operator should decide what procedure to be used for a given task in any given situation.
- Suitable back-up procedures are accessible and available (alternate COPs or paper-based procedures) in case of COP failure. The structure and format of the information in the back-up procedures is consistent and compatible with that in the COP. Consideration has been given to the feasibility of the means of transition to back-up procedures. The time required for the operator to effectively transfer to back-up procedures should be known and demonstrated to be feasible within required timeframes determined in the safety case. After transferring to a back up procedure the operator should be able to safely stop the processing of the COP.
- COPs should be commanded and controlled by a single dedicated operator with multiple read-only facilities displaying the COP elsewhere to assist the operating team/crew situational awareness.
- COPs provide adequate feedback to operators informing them of what the current state of procedure execution is and what the system being controlled is doing.
- The COPs conspicuously display the current system mode and have the ability to alert the operator should an unexpected mode or state change occur.
- The characteristics and behaviours of any embedded soft controls in a COP are consistent and compatible with other plant controls and user expectations.
- There is a robust COP management and configuration control process to ensure that COP content and functionality are fully verified and validated prior to use and following any changes. This process also ensures that consistency is maintained between COPs and back-up procedures. This process should meet good practice expectations and standards for Control, Electrical and Instrumentation (CE&I) systems.
- The dutyholder has addressed the issue of the safety integrity level requirements of the data display upon which the operator is required to respond. The HF inspector should consult with the relevant Fault Studies and CE&I discipline inspectors regarding substantiation of reliability claims.

6. REFERENCES

1 *Safety Assessment Principles for Nuclear Facilities. 2006 Edition Revision 1. HSE. January 2008. http://www.onr.org.uk/saps/saps2006.pdf.*

2 *Licence condition handbook. ONR. October 2014. http://www.onr.org.uk/silicon.pdf*

3 *WENRA Reactor Reference Safety Levels. Western European Nuclear Regulators' Association. Reactor Harmonization Group. WENRA. September 2014. www.wenra.org.*

4 *IAEA Safety Standards, Safety of Nuclear Power Plants: Operation Safety Requirements, NS-R-2, IAEA, 2000. http://www-pub.iaea.org/books/*

5 *IAEA Safety Standards, Safety of Nuclear Power Plants: Design, SSR-2/2, IAEA, 2011. http://www-pub.iaea.org/books/*

6 *IAEA Safety Standards, The Operating Organisation for Nuclear Power Plants Safety Guide, NS-G-2.4, IAEA, 2001. http://www-pub.iaea.org/books/*

7 *IAEA Safety Standards, Conduct of Operations at Nuclear Power Plants, Safety Guide, NS-G-2.14, IAEA, 2008. http://www-pub.iaea.org/books/*

8 *ONR How2 Business Management System. Human Factors Integration. T/AST/058, Issue 1. ONR. September 2010. http://www.onr.org.uk/operational/tech_asst_guides/*

9 *ONR How2 Business Management System. LC 24 Operating Instructions, NS-INSP-GD-024, Revision 2, ONR, January 2013. http://www.onr.org.uk/operational/tech_insp_guides/index.htm*

10 *Good practices with respect to the development and use of nuclear power plant procedures, IAEA-TECDOC-1058, IAEA, 1998*

11 *Writer's Guide for Technical Procedures. DOE-STD-1029-92, U.S. Department of Energy, December 1998.*

12 *Procedures, Human Factors Briefing Note 4, HSE. www.hse.gov.uk/humanfactors/topics/04procedures.pdf*

13 *Computer-based Procedure Systems: Technical Basis and Human Factors Review Guidance. NUREG/CR-6634, USNRC, March 2000.*

14 *Human Factors Considerations with Respect to Emerging Technology in Nuclear Power Plants, NUREG/CR-6947, USNRC, October 2008.*

15 *Human – System Interface Design Review Guidelines, NUREG 0700 Rev 2, May 2002.*

16 *IAEA SAFETY GUIDE - Software for Computer Based Systems Important to Safety in Nuclear Power Plants, Safety Series No. NS-G-1.1, IAEA, Vienna, 2000. http://www-pub.iaea.org/books/*

17 *Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC 61508, International Electrotechnical Commission.*

18 *The Use of Computers in Safety-Critical Applications. Final Report of the Study Group on the Safety of Operational Computer Systems. HSE Books ISBN 9780717616206*

19 *Implementing Digital Instrumentation and Control Systems in the Modernisation of Nuclear Power Plants No. NP-T-1.4. IAEA, Vienna, 2009, http://www-pub.iaea.org/books/*

20 *ONR How2 Business Management System. Human Machine Interface, NS-TAST-GD-059, Revision 2, ONR, November 2013. http://www.onr.org.uk/operational/tech_asst_guides/*

7. GLOSSARY AND ABBREVIATIONS

CE&I	Control, Electrical and Instrumentation
COP	Computerised Operating Procedure
DBA	Design Basis Analysis
HF	Human Factors
HFI	Human Factors Integration
HMI	Human Machine Interface
IAEA	International Atomic Energy Agency
LC	Licence Condition
OLC	Operational Limit(s) and Condition(s)
ONR	Office for Nuclear Regulation
PSA	Probabilistic Safety Analysis
SA	Safety Assessment
SAP	Safety Assessment Principle(s)
TAG	Technical Assessment Guide(s)
TIG	Technical Inspection Guide(s)
WENRA	Western European Nuclear Regulators' Association

8. ANNEXE A

SAP	Area	Relevance to this TAG
EHF.5	Human Factors: Task Analysis	In supporting task performance and providing the basis for the design of procedures.
FA.6	Fault analysis: Design basis analysis	Claims on operator actions to be supported by procedures, and compliance with procedures assured.
FA.9	Fault analysis: Design basis analysis	Design Based Assessment input to limits and conditions for safe operation; and the identification of requirements for operator actions, and input to operating instructions.
FA.14	Use of PSA	Use of PSA in developing and changing operating procedures.
AM.1	Accident management: Design and operation	Procedures contribution to accident management and emergency preparedness.
EMT.5	Engineering principles: maintenance, inspection and testing	Inspection and test procedures
EMT.6	Engineering principles: maintenance, inspection and testing	Testing, maintaining, monitoring and inspecting and relevance of operating rules and instructions.
SC.4(h)	The regulatory assessment of safety cases: Safety case characteristics	Operating and maintenance instructions; rules and contingency and emergency instructions, in relation to the management for safety and the safety case.
SC.6	The regulatory assessment of safety cases: Safety case characteristics	The safety case in relation to maintenance, inspection and testing regimes; operating limits and conditions; emergency planning.
MS.2	Leadership and management for safety: Capable organisation	The design of procedures and the factors that affect reliable performance of the organisation.
MS.4	Leadership and management for safety: Learning from experience	Learning from errors in safety procedures and processes; monitoring, review and audit of procedures; testing and validation of safety procedures.
EKP.5	Key principles: Safety measures	Safety assured by: Passive safety measures in preference to automatically initiated engineered safety measures, in preference to engineered safety measures that need to be manually brought into service in response to the fault in preference to administrative safety measures.
ERL.3	Reliability claims: Engineered safety features	Minimise the dependence on human action to maintain a safe state. Use administrative control for less demanding or longer timescale.