|  |
| --- |
|  |
| ONR Technical Assessment Guide  Procedure Design and Administrative Controls |



ONR Technical Assessment Guide (TAG)

Procedure Design and Administrative Controls

Authored by: Principal Inspector

Approved by: Deputy PL for Human and Organisational Capability

Professional Lead: PL for Human Organisational Capability

Issue No.: 5

Publication Date: Dec-2022

Next Major Review Date: Dec-2027

Doc. Ref.: NS-TAST-GD-060

Record Ref. No.: 2020/265773

Table 1: Revision commentary

|  |  |
| --- | --- |
| Issue No. | Description of Update(s) |
| Issue 4 | Review period updated |
| Issue 4.1 | Format of document updated |
| Issue 4.2 | Minor update to document to extend the review date to align with the review date of NS-TAST-GD-063 |
| Issue 5 | Update which adds clarification, corrections, and updated references |

Contents

[1. Introduction 4](#_Toc121303833)

[2. Purpose and Scope 5](#_Toc121303834)

[2.1. Procedure Design and Administrative Control 5](#_Toc121303835)

[2.2. Definitions 6](#_Toc121303836)

[3. Relationship to Licence and other Relevant Legislation 8](#_Toc121303837)

[4. Relationship to Safety Assessment Principles, WENRA Reference Levels, and IAEA Safety Standards and Guides 9](#_Toc121303838)

[4.1. SAPs 9](#_Toc121303839)

[4.2. WENRA Reactor Safety Reference Levels 9](#_Toc121303840)

[4.3. IAEA Safety Standards 10](#_Toc121303841)

[5. Advice to Inspectors 11](#_Toc121303842)

[5.1. Introduction 11](#_Toc121303843)

[5.2. General Expectations 11](#_Toc121303844)

[5.3. Administrative Controls 12](#_Toc121303845)

[5.4. Procedures 16](#_Toc121303846)

[References 25](#_Toc121303847)

[Glossary and Abbreviations 28](#_Toc121303848)

[Appendix A: Additional Relevant SAPs 29](#_Toc121303849)

# Introduction

1. ONR has established its [Safety Assessment Principles](http://www.onr.org.uk/saps/saps2014.pdf) (SAPs) (see reference document (ref. [1]) for further information) 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 dutyholders. 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. This TAG has been written to support assessment activities associated with ONR’s nuclear safety statutory purpose. The guidance presented may also be relevant in relation to ONR’s other statutory purposes namely: nuclear site health and safety; nuclear security; nuclear safeguards; and safety of transport of nuclear and radioactive materials.

# Purpose and Scope

1. ONR has the responsibility for regulating the safety of nuclear installations in Great Britain. The SAPs for Nuclear Facilities 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. This TAG provides guidance to aid Inspectors in the interpretation and application of SAPs related to administrative controls and procedures, 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.
3. The TAG provides broad expectations on key points that the ONR Human Factors 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.
4. Whilst the Inspector’s focus should be targeted on the administrative controls and procedures of greatest importance to nuclear safety, the guidance presented in this TAG is applicable to all activities which may affect safety.

## Procedure Design and Administrative Control

1. SAP EKP.5 sets out a hierarchy of preferred options for delivering safety functions and maintaining the plant within its safe operating envelope[[1]](#footnote-2). It 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.
2. The safety case should therefore include a robust justification demonstrating why alternative measures (from higher up the hierarchy) are not reasonably practicable and should show that claims on human action can be substantiated proportionate to the risk reduction claimed. This should include where:

* administrative safety measures are proposed;
* active engineered safety measures need to be manually brought into service in response to a fault or accident; or
* human action is required to support an engineered safety measure to deliver the required safety function.

1. Administrative controls need to be defined to ensure the above human actions are enacted, in the manner expected, when required.
2. Administrative controls may not be restricted to human actions that are formally claimed in safety measures within the safety case. It may be appropriate for the dutyholder to identify them where important human-based risk reduction is claimed to reduce the requirement for or limit the likely demand placed on formal safety measures[[2]](#footnote-3). For example, where human actions are used as the basis for reducing the estimated unmitigated consequence or where the human actions significantly change consideration of what constitutes credible initiating events.
3. Procedures form an essential part of any safety measure where human action is claimed by prompting personnel to complete specific actions and communicate key information to maintain or return activities to compliance with limits and conditions. The mechanisms in place to ensure that procedures are designed in accordance with good practice human factors 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 contribute to the substantiation. Additional details regarding the precise human actions expected to be undertaken to fulfil administrative controls may be defined within operating instructions in accordance with Licence Condition (LC) 24(1).

## Definitions

1. Administrative control within this TAG refers to a safety measure that is claimed to maintain activities within the plant’s safe operating envelope derived from the safety case, and which is implemented by operator action.
2. Actions which have the potential to influence the availability of, significantly reduce the requirement for, or control the demands placed upon a safety measure, may also be considered to be administrative controls.
3. For clarity, an administrative control may include human actions which:

* are claimed as an administrative safety measure;
* are required to support an engineered safety measure;
* are considered to significantly reduce the requirement for, or demands placed on, safety measures by:
  + reducing the unmitigated consequence;
  + reducing the initiating event frequency; or
  + maintaining the plant / activties within certain parameters such that fault sequences progress (and terminate) in a specific manner.

1. Administrative controls therefore have the potential to contribute to barriers at all defence in depth levels (see EKP.3). If a failure to successfully complete such human actions is reasonably foreseeable, and that failure could significantly increase risk, an administrative control should be considered.
2. It is recognised that dutyholders may use a range of terminology in relation to administrative controls and their designation. In considering such definitions and their use, Inspectors should be guided by whether this supports targeted and proportionate scrutiny of controls important to safety.
3. This TAG uses the term ‘procedures’ to refer to all written instructions that describe the way in which actions affecting safety should be carried out. The term ‘operating instruction’ is used within LC 24 whilst the term ‘procedures’ is used in EHF.8 to reflect a broader suite of documentation. 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.

# Relationship to Licence and other Relevant Legislation

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 LCs provide a legal framework which can be drawn on in assessment.
2. LCs 23 (Operating Rules) and 24 (Operating Instructions) particularly apply to this TAG. Also of direct relevance are LCs 14 and 15 (Safety Documentation and Periodic Review), LC 11 (Emergency Arrangements), LC 17 (Management Systems), LC 27 (Safety Mechanisms, Devices and Circuits) and LC 28 (Examination, Inspection, Maintenance and Testing). Most other LCs also touch on the topic of procedures and administrative controls.
3. 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 human error is minimised as low as reasonably practicable (ALARP) and safety case claims and assumptions remain valid.
4. 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. Procedures should reflect the actual hazards faced and specify the risk control measures that will be implemented when undertaking the work. Adherence to the work procedure is key to ensuring risk assessments are, and remain, valid.

# Relationship to Safety Assessment Principles, WENRA Reference Levels, and IAEA Safety Standards and Guides

## SAPs

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:
2. EHF.4. Identification of administrative controls:

Administrative controls needed to keep the facility within its operating rules for normal operation or return the facility back to normal operations should be systematically identified.

1. Para 448 expands upon EHF.4 with the expectation these controls be designed such that the requirements for personnel action are clearly identified and unambiguous to those responsible for their implementation.
2. EHF.9 Procedures:

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

1. Paras 458 through 461 expands upon EHF.9 including the expectations that procedures should be accurate, designed and presented in a format compatible to user needs and suitable for the task. Procedures should also be controlled and periodically reviewed to ensure that they remain up to date and fit for purpose.
2. References to procedures and administrative controls, either implicit or explicit, are also noted extensively throughout the SAPs in general, and examples are presented in Appendix A.

## WENRA Reactor Safety Reference Levels

1. 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.
2. The guidance in this TAG is consistent with the following harmonisation issues from the WENRA Safety Reference Levels (SRLs) for Existing Reactors [3], Waste and Spent Fuel Storage [4], Decommissioning [5], Radioactive Waste Disposal Facilities [6] and Existing Research Reactors [7]. The SRLs which represent good practices in the WENRA member states, are relevant and should be taken into account by the inspector:

## IAEA Safety Standards

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

* SSR-2/2: Safety of Nuclear Power Plants: Commissioning and Operation Specific Safety Requirements [8]
* NS-G-2.2: Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants [9]
* NS-G-2.4: The Operating Organisation for Nuclear Power Plants Safety Guide [10]
* NS-G-2.14: Conduct of Operations at Nuclear Power Plants Safety Guide [11]
* SSG-51: Human Factors Engineering in the Design of Nuclear Power Plants [12]
* SSG-61: Format and Content of the Safety Analysis Report for Nuclear Power Plants [13]

1. The IAEA Safety Standards (Requirements and Guides) were the benchmark for the revision of the SAPs in 2014 and are recognised by ONR as relevant good practice (RGP). IAEA standards and guidance undergo periodic revision and supplementation and the inspector should consult the IAEA website to confirm they are using up to date documentation.

# Advice to Inspectors

## Introduction

1. LC 23(1) requires the licensee to produce an adequate safety case to demonstrate the safety of those activities and to identify the conditions and limits necessary in the interests of safety (operating rules). LC 23(3) requires that operations are at all times controlled and carried out in compliance with such operating rules. A clear distinction is expected between the limits and conditions and the arrangements via which those operating rules are implemented. Operating rules communicate the constraints on how the facility, plant or process should be operated to ensure compliance with the safety analysis and define the safe operating envelope. The dutyholder is required to define suitable and sufficient administrative controls to ensure and demonstrate compliance with its operating rules, some of which will be implemented via operating instructions[[3]](#footnote-4).
2. 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

1. 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 human factors resource - to support effective specification and design of administrative controls and procedures, drawing upon a proportionate use of task analysis[[4]](#footnote-5);
* 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.

1. 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. To achieve this, ongoing discussion with the end user should be an integral part of the specification, design, and implementation processes.

1. ONR expects human factors / ergonomics principles and practices to be incorporated in the design, specification, implementation and through-life management of procedures and administrative controls. It should be recognised that procedures are only one of the Performance Shaping Factors (PSFs) which affect the reliability of operator actions associated with implementation of administrative controls. Other factors such as Human-Machine Interface (HMI) [14], task design [15] , supervision and training [16] will also be relevant, and the Inspector should recognise this when defining interventions.
2. The licensee’s approach to the development of administrative controls and procedures should therefore be captured within its formal arrangements. Suitably detailed guidance should be incorporated within the licensee’s safety assessment, engineering design and Human Factors Integration (HFI) processes. Further guidance on HFI can be found in NS-TAST-GD-058 [17]).

## Administrative Controls

1. This section is intended to supplement the guidance presented in the LC 23 Operating Rules Technical Inspection Guide (TIG), NS-INSP-GD-023 [18]. It is recommended that the reader also refers to Limits and Conditions for Nuclear Safety (Operating Rules) TAG, NS-TAST-GD-035 [19] as part of their inspection and/or assessment.

### General Expectations

1. Claims on administrative control should be identified and assessed from a human factors perspective in all operating states commensurate with their risk.
2. Where a high reliance is placed upon the administrative control, it would be expected that a detailed human factors assessment involving the use of task analysis would be conducted and robust justification made for the usability and reliability of that control.
3. 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 (plus commissioning and decomissioning) and 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 be 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 dutyholder has suitable arrangements which are used to inform the design or modification and substantiation of its administrative controls.
* The actions being claimed:
  + are feasible,
  + the 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, environment[[5]](#footnote-6), and HMI[[6]](#footnote-7)s available at the time the control needs to be enacted[[7]](#footnote-8).
* 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 and 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 and 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 and competence requirements.
* The dutyholder has conducted suitable evaluation and testing or 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

1. The impact of dependency on the reliability of the administrative control should be considered as this is an important 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.
2. Inspectors may consider whether the dutyholder has identified dependent failure mechanisms associated with its administrative controls (i.e. between initiating events and safety measures, or within and between different safety measures) and has implemented credible defences and mitigations against dependency where these effects are identified.

### Assessment of Administrative Controls

1. This section provides general advice to the Inspector regarding good practice expectations for the assessment and substantiation of administrative controls.   
   The guidance provided in ONR’s Human Reliability Analysis TAG, NS-TAST-GD-063 [20], is also relevant.
2. Inspectors may consider whether:

* Where a high reliance is placed on administrative control or it significantly contributes to 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. See NS-TAST-GD-059 [21] for further guidance.
  + 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. See NS-TAST-GD-027 [16] for further guidance.
  + The prevailing culture within the relevant parts of the operating organisation.
* Where feasible, the dutyholder has used trials (simulator or operational) 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

1. 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.
2. 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 be 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

1. This section is intended to supplement the ONR LC 24 Operating Instructions TIG, NS-INSP-GD-024 [22] 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

1. 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 paper procedure in hand, followed step by step for every task undertaken on the site[[8]](#footnote-9). 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 out with these.
* The dutyholder has clearly communicated how the procedure is to be used.

### Management Arrangements

1. 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. These activities should be undertaken by personnel with the requisite skills, knowledge and experience. Those undertaking the reviews should be supported by suitable corporate guidance which incorporates good practice principles. Dedicated training in procedure development may be required to ensure that personnel are competent to complete these activities and ensure alignment with RGP.
* The dutyholder has a process for validation and verification of procedures which includes:; end user involvement; confirmation of technical accuracy; ways of use and overall usability for the environment in which they are to be used.
* Consideration of assumptions within the safety case to ensure that the safety case is not undermined. Mechanisms should be in place to ensure that the safety case is not undermined by subsequent changes to procedures and any changes to the safety case flow into revised procedures.
* 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. Similarly significant changes to procedures, for example, a change of presentational format or move from paper-based to computerised procedures, should be subject to robust risk assessment.
* 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 activities, their 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 25(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), Probabilistic Safety Analysis (PSA) and Severe Accident Analysis (SAA), appropriate to the specific procedures.

### Procedure Design and Methods

1. The development of technically accurate and usable procedures will rely on the application of appropriate methods and guidance such as task analysis, application of good practice principles for procedure design and robust verification and validation processes. Engaging procedure users and Subject Matter Experts (SMEs) 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.
2. 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 RGP in procedure writing and to ensure consistency of presentation and format (see for example [23] [24] [25] [26] [27] and [28] – note this reference list is not definitive). This process may be informed by the following.
  + 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 “Signal Words”[[9]](#footnote-10)” (such as cautions, warnings), hold points and independent verification to control safety significant task steps.
  + Actions are presented appropriately and consistently, for example: the use of single action steps with a defined outcome; limiting one action to each sentence; clearly distinguishing actions that need to be completed sequentially; and highlighting differences between similar procedural steps.
  + A “one size fits all” approach to procedure formatting is unlikely to be appropriate. For example, an appropriate procedure format used for normal operations or management of design basis faults might be very different from one to be used to respond to a beyond design basis or severe accident. Different formats might be appropriate to support the specific task requirements (e.g. event-based for normal operations, symptom-based for beyond design basis faults, etc.). The task environment will also impact what form and format of procedures is appropriate to support task performance.
  + 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.

### Emergency Response and Accident Management Procedures

1. Human action during emergency response and accident management is likely to have a significant impact on consequence. Experience demonstrates that good human performance can prevent or significantly mitigate consequence whereas poor performance can exacerbate the situation. By their nature, such events occur very infrequently, may be extremely stressful and physically demanding to those involved. The work environment may be significantly degraded by the initiating event or damage caused by fault’s progress. Procedures used under such circumstances need to be specially designed, to take account of these PSFs, and effectively support human performance
2. Inspectors may wish to consider the following when assessing these types of procedure:

* Whether it is clear when personnel should transition to emergency or accident procedures. There may be unwillingness to accept that conditions have deteriorated to the extent that transition is required resulting in valuable time being lost.
* Personnel may be unfamiliar with emergency or accident conditions and increased uncertainty as a facility transitions outside its design basis. Symptom based procedures may therefore be more effective.
* The procedures should be as clear and concise as possible and typically limited to simple steps highlighting required actions and associated plant status verification. Explanatory text within such procedures is as likely to be a hinderance as a help.

1. Given the unique and uncertain nature of emergency response and accident management scenarios it is difficult to provide definitive guidance applicable in all cases. The IAEA has published extensive guidance related to the development and review of plant specific emergency operating instructions [29] which is likely to be of value to inspectors undertaking assessments.

### Testing and Commissioning Procedures

1. The general expectations for procedures, their design and methods of production equally apply to procedures that are used for testing and commissioning.   
   Such activities may be performed with the plant in unusual and changing configurations with potentially less defence in depth than during normal operations. Procedures must be available to manage such circumstances and any reasonably foreseeable outcomes which could negatively impact nuclear safety. Testing and commissioning procedures may therefore need to be more detailed and require the bases of the contents of the procedure (i.e., key assumptions regarding limits and conditions prior to and during the activity) to be explicit. During later stages of commissioning, once the procedures have been verified and validated in use, this additional detail may no longer be required and removed from the procedure itself. The dutyholder should detail the bases upon which testing, and commissioning procedures content are decided and verified. This should also be linked to the safety case, training and competency assessments.

### Computerised Procedures

1. Advances in digital technology are resulting in increasing availability of computerised procedures, for assisting operators with various tasks including plant control, maintenance, fault diagnosis and response [30] [31]. Computerised procedures cover a broad range of very different applications for which RGP continues to evolve. It is important that each application is considered on its individual merits against good practice which is relevant to the specific circumstance. The purpose of this section therefore is to provide high level guidance to inspectors where the licensee proposes to use such systems.
2. ONR considers computerised procedures[[10]](#footnote-11) to be any computer application that presents operating procedures or instructions through electronic, rather than printed, media. This is taken to include the simple representation of procedure text in electronic form, the automated gathering and display of plant data relevant to a task and procedure step through to procedure-based automation whereby the evaluation and execution of a predefined sequence of procedure steps is carried out by a computerised operating system.
3. Regardless of the type of computerised procedures proposed by dutyholders, it is important to recognise that operators are responsible for the proper application of any procedures and computerised procedures 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 a way that s/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 computerised procedures should not have any impact on safety systems or control systems.
4. The same general principles applied to the design of paper-based procedures also apply to computerised procedures in terms of presentation principles, processes for updating, verifying and validating, etc. However, there are other specific issues that must be addressed if computerised procedures are to be used including the consideration of HMI and software design and verification (see refs. [14], [32], [33] [34], [35], [36], [37], [38] and [39]).
5. Whilst computerised procedure systems offer many potential benefits, they may introduce significant risk if such systems are inadequately conceived and / or executed. Proposals to implement such systems should, where appropriate, be subject to proportionate application of the licensee’s LC 22 arrangements or alternatively should be supported by a suitable and sufficient risk assessment of comparable robustness. Inspectors may wish to consider the following in any judgement of adequacy.

* How RGP has been used to inform allocation of function, design and operational decision making and broader HFI.
* That there is a clear understanding as to how the use of computerised procedures differs from paper-based procedures for the specific tasks, and any potential errors that this could introduce.
* Human actions and administrative controls that are necessary for safety remain achievable with at least the same reliability as previously.
* The benefits to the procedure user, in terms of human performance, and how these outweigh any potential negative impacts.

1. Where the dutyholder uses computerised procedures, Inspectors may consider whether:

* The choice and use of computerised procedures are appropriate for the operational concept, tasks and safety functions to be delivered.
* The computerised procedures 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 computerised procedures 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 computerised procedures 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.
* Computerised procedures provide adequate information on initial plant conditions that must be met before any automated sequence may be started.
* Computerised procedures that process plant data and evaluate procedure-step logic can only make deterministic decisions (e.g., yes/no) and all data evaluated by computerised procedures is available to the operator. The results evaluated by the computerised procedures are the same as those expected from operator evaluations of the same procedure steps.
* Failure modes or loss of the computerised procedures can be readily detected and identified by operators, and these do not affect the operator’s ability to safely recover and operate the plant.
* Computerised procedures should not determine what procedure should be used; the operator should decide what procedure is to be used for a given task in any given situation.
* Suitable back-up procedures are accessible and available (alternate computerised procedures or paper-based procedures) in case of computerised procedures failure. The structure and format of the information in the back-up procedures is consistent and compatible with that in the computerised procedures. 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 backup procedure, the operator should be able to safely stop the processing of the computerised procedures.
* Computerised procedures should be commanded and controlled by a single dedicated operator with multiple read-only facilities displaying the computerised procedures elsewhere to assist the operating team/crew situational awareness.
* Computerised procedures 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 computerised procedures 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 computerised procedures are consistent and compatible with other plant controls and user expectations.
* There is a robust computerised procedures management and configuration control process to ensure that computerised procedures content and functionality are fully verified and validated prior to use and following any changes. This process also ensures that consistency is maintained between computerised procedures 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 Human Factors inspector Inspector should consult with the relevant Fault Studies and CE&I discipline inspectors regarding substantiation of reliability claims.

# References

|  |  |
| --- | --- |
| [1] | ONR, “Safety Assessment Principles (SAPs) for Nuclear Facilities - 2014 Edition (Revision 1),” 2020. |
| [2] | ONR, “Licence Condition Handbook (February 2017)”. |
| [3] | WENRA, *Safety Reference Levels for Existing Reactors 2020,* 2021. |
| [4] | WENRA, *Waste and Spent Fuel Storage Safety Reference levels. Version 2.2,* 2014. |
| [5] | WENRA, *Decommissioning Safety Reference Levels. Version 2.2,* 2015. |
| [6] | WENRA, *Radioactive Waste Disposal Facilities Safety Reference Levels,* 2014. |
| [7] | WENRA, *Safety Reference elves for Existing Research Reactors,* 2020. |
| [8] | IAEA, “SSR-2/2: Safety of Nuclear Power Plants: Commissioning and Operation Specific Safety Requirements,” 2016. |
| [9] | IAEA, “NS-G-2.2: Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants. 2000”. |
| [10] | IAEA, “NS-G-2.4: The Operating Organisation for Nuclear Power Plants Safety Guide,” 2001. |
| [11] | IAEA, “NS-G-2.14: Conduct of Operations at Nuclear Power Plants Safety Guide,” 2008. |
| [12] | IAEA, “SSG-51: Human Factors Engineering in the Design of Nuclear Power Plants,” 2019. |
| [13] | IAEA, “SSG-61: Format and Content of the Safety Analysis Report for Nuclear Power Plants,” 2021. |
| [14] | ONR, “NS-TAST-GD-059 - Human Machine Interface”. |
| [15] | ONR, “NS-TAST-GD-061 Staffing Levels and Task Organisation”. |
| [16] | ONR, “NS-TAST-GD-027 Training and Assuring Personnel Competence”. |
| [17] | ONR, “NS-TAST-GD-058 - Human Factors Integration”. |
| [18] | ONR, “NS-INSP-GD-023 LC 23 Operating Rules”. |
| [19] | ONR, “NS-INSP-GD-035 Limits And Conditions For Nuclear Safety”. |
| [20] | ONR, “NS-TAST-GD-063 - Human Reliability Analysis”. |
| [21] | ONR, “NS-TAST-GD-059 Human Machine Interface”. |
| [22] | ONR, “NS-INSP-GD-024 - LC 24 Operating Instructions”. |
| [23] | “BS EN ISO 20607:2019 Safety of machinery - Instruction handbook - General drafting principles”. |
| [24] | “BS EN IEC/IEEE 82079‑1:2020 Preparation of information for use (instructions for use) of products - Part 1: Principles and general requirements”. |
| [25] | IAEA, “IAEA-TECDOC-1058 - Good practices with respect to the development and use of nuclear power plant procedures,” 1998. |
| [26] | U.S. Department of Energy, “DOE-STD-1029-92 - Writer’s Guide for Technical Procedures,” 1998. |
| [27] | CAA, “CAP 676 Guidance on the Design, Presentation and Use of Emergency and Abnormal Checklists,” August 2006. |
| [28] | “NASA/TM—2016–219421 Designing Flightdeck Procedures,” October 2016. |
| [29] | IAEA, “Safety Report Series No.48 - Devleopment and Review of Plant Specific Emergency Operating Procedures,” 2006. |
| [30] | US Nuclear Regulatory Commission, “NUREG/CR-6634 - Computer-based Procedure Systems: Technical Basis and Human Factors Review Guidance,” 2000. |
| [31] | US Nuclear Regulatory Commission, “NUREG/CR-6947 - Human Factors Considerations with Respect to Emerging Technology in Nuclear Power Plants,” 2008. |
| [32] | US Nuclear Regulatory Commissions, “NUREG 0700 - Human – System Interface Design Review Guidelines - Revision 3,” 2020. |
| [33] | IAEA, “IAEA Safety Standards - SSG-39 - Design of Instrumentation and Control Systems for Nuclear Power Plants,” 2016. |
| [34] | International Electrotechnical Commission, “IEC 61508 - Functional safety of electrical/electronic/programmable electronic safety-related systems,” 2010. |
| [35] | HSE, “The Use of Computers in Safety-Critical Applications - Final Report of the Study Group on the Safety of Operational Computer Systems,” 1998. |
| [36] | IAEA, “NP-T-1.4 - Implementing Digital Instrumentation and Control Systems in the Modernisation of Nuclear Power Plants,” 2009. |
| [37] | *Digital Instrumentation and Controls DI&C-ISG-05. Task Working Group #5: Highly-Integrated Control Rooms - Human Factors Issues (HCIF-HF) - Interim Staff Guidance. US NRC, Revision 1, November 2008..* |
| [38] | EPRI, *Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification - Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance for Operating Plants and New Builds.,* Technical Report 3002004310, December 2015. |
| [39] | U.S. Department of Energy - Office of Nuclear Energy, “Light Water Reactor Sustainability Program - Design Guidance for Computer-Based Procedures for Field Workers. INL/EXT-16-39808, Revision 0.,” September 2016. |
| [40] | ONR, “NS-TAST-GD-062 - Workplaces and Work Environment”. |

# Glossary and Abbreviations

ALARP As Low As Reasonably Practicable

CE&I Control, Electrical and Instrumentation

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

PSF Performance Shaping Factor

RGP Relevant Good Practice

SAA Severe Accident Analysis

SAP Safety Assessment Principle(s)

SME Subject Matter Expert

SRL Safety Reference Level

TAG Technical Assessment Guide(s)

TIG Technical Inspection Guide(s)

WENRA Western European Nuclear Regulators’ Association

# Appendix A: Additional Relevant SAPs

Table – SAPs relevant to this TAG (in addition to EHF.4 and EHF.9)

| SAP | Area | Relevance to this TAG |
| --- | --- | --- |
| MS.2 | Leadership and management for safety: Capable organisation | Para 64 The design of procedures and the factors that affect reliable performance of the organisation. |
| MS.4 | Leadership and management for safety: Learning from experience | Para 76 Learning should drive improvement throughout the organisation. Information should be collected from a range of sources inside the organisation, including from:  (a) workers (eg about strengths, weaknesses, deviations and errors in safety procedures and processes);  (b) monitoring, review and audit of the implementation and effectiveness of governance, safety strategies, policies, plans, goals, standards, processes and procedures;  (d) testing and validation of safety procedures under normal operational and fault conditions. |
| SC.4 | The regulatory assessment of safety cases: Safety case characteristics | Para 101(h) 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 | Para 106. The safety case should justify how the requirements identified within it will be implemented effectively. The means of implementation considered should include:  (a) the operating limits and conditions (operating rules) required to ensure that the facility is operated safely at all times;  (b) the procedures and instructions that need to be followed;  (c) the required examination, inspection, maintenance and testing regimes justified in or assumed by the safety case;  (d) control, supervision, qualification and training and other safety management requirements; and  (e) inputs to emergency planning. |
| SC.8 | The regulatory assessment of safety cases: Safety case ownership | Para 112 Ownership and responsibility require:  (a) an understanding of the safety case, the standards applied in it, its assumptions and the limits and conditions (operating rules) derived from it; |
| EKP.3 | Key principles Defence in Depth | Para 149 International consensus is that the appropriate strategy for achieving the overall safety objective is through the application of the concept of defence in depth. This should provide a series of independent barriers (inherent features, equipment and procedures) aimed at preventing faults in the first instance, and ensuring appropriate protection or mitigation of accidents in the event that prevention fails.  Procedures subsequently referenced in Table 1 in levels of protection and essential means of achieving them |
| EKP.5 | Key principles: Safety measures | Safety measures should be identified to deliver the required safety function(s).  Para 155 Safety should be secured by characteristics as near as possible to the top of the list below:  (c) Active engineered safety measures that need to be manually brought into service in response to a fault or accident.  (d) Administrative safety measures (see paragraph 446 ff.).  Para 156 More generally, priority should be given to providing reliable and effective barriers (inherent features, equipment and procedures earlier in the hierarchy) so that later barriers, though in place, need not be called upon. |
| ERL.3 | Reliability claims: Engineered safety measures | Para 194 For requirements that are less demanding, or on a longer timescale, administrative safety measures, i.e. those involving operator actions based on procedures, may be acceptable. |
| EMT.5 | Maintenance, inspection and testing: Procedures | Commissioning and in-service inspection and test procedures should be adopted that ensure initial and continuing quality and reliability. |
| EMT.6 | Maintenance, inspection and testing: Reliability claims | Provision should be made for testing, maintaining, monitoring and inspecting structures, systems and components (including portable equipment) in service or at intervals throughout their life, commensurate with the reliability required of each item. |
| EMC.21 | Integrity of metal components and structures: Safe operating envelope | Throughout their operating life, components and structures should be operated and controlled within defined limits and conditions (operating rules) derived from the safety case. |
| EMC.24 | Integrity of metal components and structures: Operation | Facility operations should be monitored and recorded to demonstrate compliance with, and to allow review against, the safe operating envelope defined in the safety case (operating rules). |
| ESS.9 | Safety systems: Time for human intervention | Where human intervention is needed to support a safety system following the start of a requirement for protective action, then the timescales over which the safety system will need to operate unaided, before intervention, should be demonstrated to be sufficient. |
| ESS.23 | Safety systems: Allowance for unavailability of equipment | Para 419 The safety case should identify the permitted combinations of equipment unavailability for each permitted operating state (operating rules), applying design basis analysis (see paragraph 631) and probabilistic safety analysis (see paragraph 653). |
| ESR.4 | Control and instrumentation of safety-related systems: Provision of controls | Adequate and reliable controls should be provided to maintain all safety-related plant parameters within their specified ranges (operating rules). |
| ESR.7 | Control and instrumentation of safety-related systems: Minimum operational equipment | The minimum control and instrumentation in each of the facility’s permitted operating modes should be specified (operating rules) and its adequacy substantiated. |
| EHF.5 | Human factors: Task Analysis | Para 451 The analysis should be sufficiently detailed to provide a basis for developing user interfaces, procedures and job aids, as well as helping define operator roles and responsibilities, staffing levels, personnel competence and training needs, communication networks and workspace design. |
| EHF.10 | Human factors: Human Reliability | Human reliability analysis should identify and analyse all human actions and administrative controls that are necessary for safety.  Para 465 Proportionate analysis should be undertaken to support the claims and arguments made in regard to these actions and administrative controls. |
| FA.6 | Fault analysis: Design basis analysis | Para 633 Operator actions can be claimed as part of safety measures only if sufficient time is available, adequate information for fault diagnosis is presented and, for existing facilities, appropriate written procedures exist and compliance with them is assured, and suitable training has been provided. |
| FA.9 | Fault analysis: Design basis analysis | DBA should provide an input into the safety classification and the engineering requirements for systems, structures and components performing a safety function; the limits and conditions for safe operation; and the identification of requirements for operator actions.  Para 643 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 | Fault analysis: Use of PSA | Para 661 Appropriate use of PSA should be made in activities such as:  (i) developing and changing operating procedures and associated training programmes for managing faults and accidents (including severe accidents) |
| FA.16 | Fault analysis: Use of severe accident analysis | Para 672. The severe accident analysis should provide information to:  (b) form a suitable basis for accident management strategies and procedures (see Principle AM.1); |
| AM.1 | Accident management and emergency preparedness Planning and preparedness | Para 775 he strategies and plans should identify all the procedural support requirements that will be needed during an accident. The procedures should define all the roles and responsibilities needed for an effective accident response. Effective storage arrangements should be in place to ensure the timely availability of these procedures in accident conditions.  Para 776 The procedural support requirements should include emergency operating procedures and accident management guidelines. The accident management guidelines should be based on the facility’s severe accident analysis and be written to facilitate timely and well-informed decision-making during accidents. The emergency operating procedures should be written recognising the potential practical difficulties (e.g., degraded state, radiation levels, poor lighting, access issues and communication system failures) that could reasonably be encountered by operators working in accident conditions.  Para 777 The emergency operating procedures and accident management guidelines should be tested during emergency exercises to confirm their accuracy and effectiveness and should also form part of operator training. At operating power reactors, testing of the emergency operating procedures and, where practicable, the accident management guidelines should include the use of full-scope plant simulators. |

1. ONR guidance on allocation of function is presented in NS-TAST-GD-064. [↑](#footnote-ref-2)
2. Essentially where human action / behaviour fulfils a similar role in the risk calculation to engineering claimed as safety related equipment (SRE). [↑](#footnote-ref-3)
3. In addition to administrative controls, the dutyholder may propose other methods to demonstrate operating rule compliance. For example, testing and inspection completed during maintenance may provide evidence of compliance (LC 28). [↑](#footnote-ref-4)
4. ‘Task analysis’ (EHF.5) describes a broad range of techniques that can be used to assess how an activity can be completed, the demands it places on the operator and other factors such as information requirements. A Guide to Task Analysis, Kirwan & Ainsworth (1992) [ISBN-13: ‎978-0748400584] provides an illustrative introduction into a variety of techniques which dutyholders may choose to use when assessing its activities. [↑](#footnote-ref-5)
5. There are many ways the work environment can impact human performance, for example: temperature, noise, light, etc.; which need to be understood (see NS-TAST-GD-062 [40] for further guidance). If the administrative control is completed outside, potential variations in the environment and / or weather conditions should be considered. [↑](#footnote-ref-6)
6. See NS-TAST-GD-059 [21] for further guidance. [↑](#footnote-ref-7)
7. If the administrative control is enacted in response to a fault, conditions may be very different from those experienced during normal operations. This requires consideration to ensure the control is suitably robust and designed for all conditions in which it may be enacted. [↑](#footnote-ref-8)
8. Rigid step-by-step compliance may be required for challenging, safety critical task, but it may not be practicable to have the procedure ‘in the hand’ during task completion (e.g. working in highly contaminated areas, in gloveboxes or where both hands are needed to complete the tasks). Under such circumstance, comparably robust methods, should be applied (e.g. reader – doer). [↑](#footnote-ref-9)
9. ISO 3864-2 defines the appropriate use of the following signal words:  
   DANGER: Signal word used to indicate an imminently hazardous situation which, if not avoided, will result in death or serious injury  
   WARNING: Signal word used to indicate a potentially hazardous situation which, if not avoided, could result in death or serious injury  
   CAUTION: Signal word used to indicate a potentially hazardous situation which, if not avoided, could result in minor or moderate injury [↑](#footnote-ref-10)
10. The IAEA uses the term computerised procedures [12] to describe systems that simply reproduce paper-based procedures (Type I); augment procedures with dynamic embedded process data (Type II) and systems that include embedded soft controls to manipulate equipment (Type III). [↑](#footnote-ref-11)