|  |
| --- |
|  |
| ONR Technical Assessment Guide  Human Reliability Analysis |



ONR Technical Assessment Guide (TAG)

Human Reliability Analysis

Authored by: Nuclear Safety Inspector

Approved by: Deputy PL for Human and Organisational Capability

Professional Lead: PL for Human Organisational Capability

Issue No.: 6

Publication Date: Dec-2022

Next Major Review Date: Dec-2027

Doc. Ref.: NS-TAST-GD-063

Record Ref. No.: 2022/51682

Table : Revision commentary

|  |  |
| --- | --- |
| Issue No. | Description of Update(s) |
| 6 | Updated format, revised the presentation of information and clarified and extended clauses throughout the document. |

Contents

[1. Introduction 4](#_Toc121304868)

[2. Purpose and Scope 4](#_Toc121304869)

[3. Relationship to Licence and other Relevant Legislation 5](#_Toc121304870)

[4. Relationship to SAPs, WENRA Reference Levels and IAEA Safety Standards Addressed Legislation 6](#_Toc121304871)

[4.1. SAPs and Interfacing TAGs 6](#_Toc121304872)

[4.2. WENRA reactor safety reference levels 10](#_Toc121304873)

[4.3. IAEA safety standards 10](#_Toc121304874)

[5. Advice to Inspectors 12](#_Toc121304875)

[5.1. Purpose of Human Reliability Analysis 12](#_Toc121304876)

[5.2. Identification of Human Actions Important to Safety (EHF.3) and Administrative Controls (EHF.4) 14](#_Toc121304877)

[5.3. Analysis and Substantiation of Human Actions important to safety (EHF.5 & 10) 16](#_Toc121304878)

[5.4. Process, Methods and Tools for Undertaking HRA 18](#_Toc121304879)

[References 31](#_Toc121304880)

[Glossary and Abbreviations 33](#_Toc121304881)

[Appendix 1 – Assessment Expectations for Review of HRAs for Nuclear Power Plants 34](#_Toc121304882)

# Introduction

1. ONR has established its Safety Assessment Principles (SAPs) [1] 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 judgments and decisions. This technical assessment guide (TAG) is one of these guides.

# Purpose and Scope

1. The primary aim of this document is to provide guidance to ONR inspectors in the exercise of their regulatory judgment when assessing the adequacy of dutyholder[[1]](#footnote-2) safety cases. Consistent with the scope of the SAPs (in particular paragraph 6), this TAG is intended to be technology neutral. It is not intended to provide prescriptive instructions to dutyholders on how to design their facilities, undertake their activities or write their safety cases.
2. This TAG contains guidance to advise and inform ONR staff in the exercise of their regulatory judgment. Its purpose is to provide guidance to aid inspectors, principally in the interpretation and application of SAP EHF.10 (and its supporting paragraphs 465 – 468). EHF.10 states that “Human reliability analysis should identify and analyse all human actions and administrative controls that are necessary for safety”. This guidance also draws on and assists with the interpretation and application of EHF.3, the “Identification of actions important to safety”; EHF.4, the “Identification of Administrative Controls”; and EHF.5 “Task Analysis”. Application of these SAPs is necessary to achieve the expectations of EHF.10, which states “Proportionate analysis should be carried out of all tasks important to safety and used to justify the effective delivery of the safety functions to which they contribute”. Such analysis is expected to underpin any risk assessment with qualitative and where applicable quantitative human reliability claims.
3. As with all guidance, inspectors should use their judgment and discretion in the depth and scope to which they apply the guidance provided in this TAG. This TAG does not detail or prescribe specific methods and approaches for conducting HRA. Inspectors should use their own knowledge and experience when considering the adequacy of a dutyholder’s approach.

# Relationship to Licence and other Relevant Legislation

1. The Nuclear Site Licence Conditions (LC) place legal requirements on the dutyholder 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. LC 14, 15 and 23 are particularly relevant to this TAG:
3. LC 14 requires the licensee to make and implement adequate arrangements for the production and assessment of safety cases. Proportionate HRA is a key part of the safety case.
4. LC 15 sets out the requirements for periodic review of safety cases. The periodic reviews carried out under these arrangements include those for updating/extending the fault analysis, including any qualitative or quantitative HRA, and using these to support the arguments for continuing operation during the period until the next review.
5. LC 23 requires that the licensee shall, in respect of any operation that may affect safety, produce an adequate safety case to demonstrate the safety of that operation and to identify conditions and limits necessary in the interests of safety. It is ONR’s expectation that analysis of the role and contribution of the human to safety contributes to this.
6. In addition, LC 17 sets out the requirement for management systems which give due priority to safety and for quality management arrangements for all matters that affect safety. In this respect, dutyholders are expected to establish an adequate quality management process that is effectively applied during HRA.
7. Safety cases, including HRA elements, may be produced to support activities such as construction of new facilities, commissioning, modifications and experiments and decommissioning. These activities, covered by licence conditions 19, 20, 21, 22 and 35, require safety documentation.
8. 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. In order to be considered suitable and sufficient, such assessments must identify and consider the impact of human error and the risk of people acting out with established procedures and training.

# Relationship to SAPs, WENRA Reference Levels and IAEA Safety Standards Addressed Legislation

## SAPs and Interfacing TAGs

1. ONR’s expectations concerning HRA are set out in a number of SAPs.   
   The primary reference is SAP EHF.10 which states:

“Human reliability analysis should identify and analyse all human actions and administrative controls that are necessary for safety”.

1. Paragraph 465 to 468 expand upon EHF.10 in relation to the types of safety case analyses HRA may need to be proportionately included within   
   (e.g., Design Basis Accident (DBA), Probabilistic Safety Analysis (PSA) and Severe Accident Analysis (SAA)), the types of human actions that should be analysed, the selection and application of probabilistic data for human errors and consideration of dependency.
2. SAP EHF.10 is strongly linked with EHF.5 and its supporting text:

“Proportionate analysis should be carried out of all tasks important to safety and used to justify the effective delivery of the safety functions to which they contribute”.

1. Paragraph’s 449 to 452 expand upon SAP EHF.5 and identify the factors and demands that should be considered in task analysis. This includes the expected level of descriptive detail and use. It also includes the need to apply task analysis to all actions and controls identified under SAPs EHF.3 and EHF.4, so that the safety case demonstrates high confidence of achieving requisite reliability of these actions and controls.
2. SAP EHF.3 states that:

“A systematic approach should be taken to identifying human actions that can impact safety for all permitted operating modes and all fault and accident conditions identified in the safety case, including severe accidents”.

1. Paragraph 447 expands upon SAP EHF.3 and states that:

“This principle includes identifying all the safety actions of personnel responsible for monitoring and controlling the facility and of personnel carrying out maintenance, testing and calibration activities. It also includes consideration of the impact on safety arising from engineers, analysts, managers, directors and other personnel who may not interact directly with plant or equipment”.

1. SAP EHF.4 states:

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

1. Paragraph 448 supporting SAP EHF.4 states that:

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

1. Paragraph 633 states that:

“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. Appropriate analysis should be carried out on any claimed actions (see Principle EHF.5).”

1. Related to EHF.3 and EHF.4 are SAPs ECS.1 and ECS.2 concerning safety categorisation and classification. Paragraph 164 states:

“Where safety functions are delivered or supported by human action, these human actions should be identified and classified on the basis of those functions and their significance to safety. The methods used for determining the classification should be analogous to those used for classifying structures, systems and components.”

A general approach to classification is outlined in paragraphs 165-166 of the SAPs and further specific guidance is given in NS-TAST-GD-094 [2].

1. In addition to the above, the other SAPs of most relevance to requirement for HRA or task analysis are:
2. SAP FP.4 states:

“Dutyholders must demonstrate effective understanding and control of the hazards posed by a site or facility through a comprehensive and systematic process of safety assessment”.

1. Paragraph 100 supporting SAP SC.4:

“A safety case should:

b) link the information necessary to show that risks are ALARP and what will be needed to ensure that this can be maintained over the period for which the safety case is valid;

c) support claims and arguments with appropriate evidence, and with experiment and /or analysis that validates performance assumptions;

d) accurately and realistically reflect the proposed activity...”

1. Paragraph 101 to SAP SC4 states:

“…. a safety case should:

b) identify the failure modes of the plant or equipment by a thorough and systematic fault and fault sequence identification process;

e) analyse normal operations…

f) analyse identified faults and severe accidents, using complementary fault analysis methods to demonstrate that risks are ALARP;

h) provide the basis for the safe management of people, plant and processes…”

1. Paragraph 618 supporting SAP FA.2 states:

“The process for identifying faults should be systematic, auditable and comprehensive and should include:

(c) …internal faults from plant failures and human error…”.

1. SAP FA.5 states:

“The safety case should list all initiating faults that are included within the design basis analysis of the facility”; paragraph 628 highlights that “initiating faults identified in Principle FA.2 should be considered for inclusion in this list…”.

1. SAP FA. 9 states:

“DBA should provide an input to…the identification of requirements for operator actions”.

1. Paragraph 653 supporting SAP FA13 states:

“The PSA should account for contributions to risk including...:

(e) pre-fault human errors (e.g., misalignments and mis-calibrations);

(f) human errors that lead to initiating faults;

(g) human errors during the course of the fault sequences including those required for repair or recovery actions;

(h) potential dependencies between separate human activities (either by the same or by different operators)”.

1. Paragraph 657 to SAP FA.13 states:

“When models are used for the calculations of input probabilities, for example, in human errors…. then the methodologies used should be justified and should account for all key influencing factors”.

1. Paragraph 658 to SAP FA.13:

“Assumptions made regarding the behaviour of the facility, or its operators should be justified, and the sensitivity to those assumptions should be analysed”.

1. A number of ONR TAGs provide guidance to inspectors on aspects that form part of HRA, or interface directly with it. The following TAGs are referred to in the detailed guidance provided in Section 5 of this document:

* NS-TAST-GD-005: Guidance on the Demonstration of ALARP [3]
* NS-TAST-GD-006: Design Basis Analysis [4]
* NS-TAST-GD-007: Severe Accident Analysis [5]
* NS-TAST-GD-010: Early Initiation of Safety Systems [6]
* NS-TAST-GD-027: Training and Assuring Personnel Competence [7]
* NS-TAST-GD-058: Human Factors Integration (HFI) [8]
* NS-TAST-GD-059: Human Machine Interface [9]
* NS-TAST-GD-060: Procedure Design and Administrative Controls [10]
* NS-TAST-GD-61: Staffing levels and Task Organisation [11]
* NS-TAST-GD-062: Workplaces and Work Environment [12]
* NS-TAST-GD-064: Allocation of Function Between Human and Engineered Systems [13]
* NS-TAST-GD-094: Categorisation of Safety Functions and Classification of Structures, Systems and Components [2]

## WENRA reactor safety reference levels

1. The objective of the Western European Nuclear Regulators Association (WENRA) harmonization programme 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. Their Safety Reference Levels (SRL) for Existing Reactors [14], Waste and Spent Fuel Storage [15], Decommissioning [16], Radioactive Waste Disposal Facilities [17] and Existing Research Reactors [18], which are based on the IAEA safety standards, represent good practices in the WENRA member states and also represent a consensus view of the main requirements to be applied to ensure nuclear safety. Each of these identifies the need for consideration and assessment of the human contribution to safety.
2. The Safety Reference Levels (SRL) for Existing Reactors [14] and the Issue O: Probabilistic Safety Assessment of Existing Research Reactors [19], identifies that:

“Human reliability analysis (HRA) shall be performed, taking into account the factors which can influence the performance of plant staff in all plant states.”

## IAEA safety standards

1. The IAEA Safety Standards (Requirements and Guides) were the benchmark for the revision of the SAPs in 2006, 2014 and 2020 and are recognised by ONR as relevant good practice. They should therefore be consulted, where relevant, by the assessor as complimentary guidance, although it should be appreciated that they are design standards rather than regulatory standards.
2. The guidance in this TAG is consistent with IAEA guidance. Specifically including:

* SSR-2/1: Safety of Nuclear Power Plants: Design [20]
* SSR-2/2: Safety of Nuclear Power Plants: Commissioning and Operation [21]
* SSR-3: Safety of Research Reactors [22]
* SSR-4: Safety of Nuclear Fuel Cycle Facilities [23]

1. These safety requirements set a consistent expectation for the design of facilities to take account of the human capabilities and limitations that could influence human performance through systematic consideration of human factors. They set an expectation that this is included at an early stage in the design process and is continued throughout the lifecycle of the facility.
2. SSG-3: Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants [24] states:

“The human errors that can contribute to the failure of safety systems should be identified and included in the logic models. A structured and systematic approach should be adopted for the identification of human errors, the incorporation of the effect of such errors in the plant logic model (event trees and fault trees) as human failure events and the quantification of the probabilities of such events, i.e., human error probabilities. A structured and systematic approach will provide confidence that a comprehensive analysis has been carried out to determine the contributions to the frequency of core damage from all types of human error.”

1. The following IAEA guidance is also relevant to this TAG.

* SSG-2: Deterministic Safety Assessment for Nuclear Power Plants [25]
* SSG-4: Application of Level 2 Probabilistic Safety Analysis for Nuclear Power Plants [26]
* SSG-20: Safety Assessment for Research Reactors and the Preparation of the Safety Analysis Report [27]
* SSG-25: Periodic Safety Review for Nuclear Power Plants [28]
* SSG-42: Safety of Nuclear Fuel Reprocessing Facilities [29]

# Advice to Inspectors

1. The guidance to inspectors is provided in subsections below and summarised in the *Figure 1*.



Figure Overview of Guidance to Inspectors

## Purpose of Human Reliability Analysis

1. The safety of nuclear installations often requires claims on human action. Where safety important human actions are identified and administrative controls are required, the feasibility and reliability of the actions and administrative controls should be demonstrated qualitatively, in a proportionate way using task analysis.
2. This qualitative task analysis should, where appropriate, be used to support the design of the plant, operational systems and administrative controls as well as the substantiation[[2]](#footnote-3) of the identified safety actions[[3]](#footnote-4). The qualitative task analysis should also form the basis from which to quantify human error probabilities (HEPs) for use in the fault analysis. Qualitative and quantitative analysis should be performed to reduce the risk from human error ALARP and to identify and implement improvements that are reasonably practicable.
3. As such, ONR considers that the process of identifying safety important actions and the necessary administrative controls and the task analytical process to substantiate them, qualitatively and quantitatively, as HRA. The following sections provides advice to inspectors on these individual topics.
4. More specific and detailed expectations for review of HRAs for Nuclear Power Plant (NPP) are given in the checklist in Appendix 1. The guidance provided in this TAG and Appendix 1 reflects relevant good practice expectations for NPP HRA, and more generally provides principles which can be read across, in a proportionate way, to other types of facility.
5. In line with paragraph 99 from the SAPs, the specific content and depth of information in a safety case will vary depending on the stage in the project lifecycle. This applies to the identification and substantiation of human actions and administrative controls that impact safety and the maturity of the qualitative task analysis and quantification used to assess them.
6. As such, early-stage safety case submissions, for example at the pre-construction stage, may be more a statement of future intent, with large numbers of assumptions, which will be confirmed and replaced by more refined analysis and evidence as the safety case and plant and operational design matures (see the ONR HFI TAG [8] for more information on the expectations for managing this). The following are outline expectations and it is acknowledged that some flexibility may be required to accommodate the specific requirements of individual projects.
7. ONR expects the process of HRA to proportionately:

* Support the identification of safety important actions and the necessary administrative controls required to deliver the safety functional requirements identified in the safety analysis.
* To provide an understanding of the extent of the reliance on the human operator for the achievement of nuclear safety.
* Support the design of the plant, process and operational systems through defining the necessary tasks and identifying the requirements of them. The requirements may include equipment, procedures, training, workspace and staffing design, to enable reliable completion of safety important actions and administrative controls.
* Provide documented evidence to substantiate the feasibility and reliability of the actions important to safety and administrative controls necessary to deliver safety functions and support the demonstration that risk is reduced ALARP.

1. Further, ONR consider it good practice for the dutyholder organisation to:

* Manage safety important actions throughout the lifetime of the facility. Doing so supports modifications to plant, processes and equipment. One way of achieving this is by providing a schedule of operational safety measures.

## Identification of Human Actions Important to Safety (EHF.3) and Administrative Controls (EHF.4)

1. EHF.3 expects that the dutyholder should undertake systematic analysis to identify human actions that can impact safety. This analysis should identify all safety important actions and include actions from all plant states [20]. It therefore includes all safety important human actions from the PSA, DBA and SAA.
2. The human actions that should be considered within dutyholder safety cases includes:

* Type A human actions (pre-initiator human error). These are human actions performed during Examination, Inspection, Maintenance and Testing (EIMT) activities, including calibration, where human error can result in a System, Structure or Component (SSC) being unavailable to perform its safety function on demand, or with significantly reduced capability. Such pre-initiating human errors are referred to as latent errors, as they do not have an immediate impact on system safety e.g. by resulting in an initiating event, but are subsequently revealed when an initiating event makes a demand on a safety measure.
* Type B human actions (Initiating event human errors). These are human actions performed during normal operations or maintenance where human error can lead to the initiation of a fault sequence.
* Type C human actions (post-initiator human errors). These are human actions performed to prevent, protect against or mitigate the consequences arising from an initiating event. Post initiator human errors can result in an operator action failing to achieve the required safety function.

1. The safety case should proportionately demonstrate that the likelihood of failure of type A, B or C human actions is reduced in line with the principle of a hierarchy of controls [13] and ALARP as a result of good engineering, task and organisational design.
2. EHF.4 expects dutyholders to systematically identify administrative controls necessary to keep the facility within its operating rules for normal operation or return the facility back to normal operations. ONR defines administrative control in TAG 060 [10] as 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. TAG 060 provides further guidance to inspectors on the design of administrative controls.
3. The inspector may consider the following general principles in the identification of actions important to safety and administrative controls:

* The dutyholder’s process for the identification of safety important human actions covers all planned operating modes and configurations, including shutdown states, decommissioning operations and any other activities that could present a radiological risk. This should include required EIMT, as well as operational tasks.
* The dutyholder’s process for the identification of safety important human actions takes account of the findings from hazard identification studies, fault analyses, engineering substantiation, Task analysis, trial and simulator data and relevant operational experience.
* The dutyholder can demonstrate that all relevant safety important operator actions are identified.
* In line with EHF.2 and the guidance identified in TAG 64 [13], the dutyholder process minimises the reliance on human actions to maintain and recover a stable, safe state. A justification has been presented where administrative controls are identified within the safety case.
* The dutyholder has clearly identified the required safety functions that the actions important to safety and administrative control supports. This safety functional requirement should be categorised according to its safety importance. See TAG 94 [2] for more information.
* Where safety functional requirements are delivered or supported by human action, the dutyholder has classified these human actions according to their importance in delivery of the safety function. The method of classification should be analogous to those used by the dutyholder for the classification of SSCs. See TAG 94 [2] for more information.
* The dutyholder has clearly specified how the human action important to safety or the administrative control contributes to the safety measure. This should consider how the human detects the need for action, decides to act and confirms the performance of the action, to achieve the desired system state.
* The design and wording of the administrative control is based on the findings, as appropriate, from task analyses, trial and simulator data or relevant operating experience and is in line with the guidance included in TAG 060 [10].
* The dutyholder has ensured that administrative controls are meaningful to those who are charged with their implementation and those who subsequently complete them. Specifically, administrative controls should use simple language and communicate requirements in an unambiguous manner. The following aspects may be considered when reviewing the adequacy of the specification of the administrative control:
  + WHAT needs to be achieved?
  + WHO is required to complete / support the action?
  + WHEN is action required? What prompts the activity to commence and in what timescales must it be completed?
  + WHERE does the activity need to be completed?
  + HOW must the activity be completed, including the equipment to be used, to support safety functional requirement delivery?

## Analysis and Substantiation of Human Actions important to safety (EHF.5 & 10)

1. EHF.5 expects that the dutyholder should undertake proportionate analysis of all tasks important to safety (e.g., type A, B and C) to justify the effective delivery of the safety functions to which they contribute. This analysis should be proportionately undertaken on all actions important to safety and administrative controls identified under principles EHF.3 and EHF.4. It enables the dutyholder to meet the expectations of EHF.10 in demonstrating that the claims and arguments made in the safety case, relating to the role of the human in supporting nuclear safety, can be supported.
2. Task analysis undertaken under EHF.5 has several purposes. These include:

* To provide a specification to support the design of the human actions or administrative controls.
* To identify potential errors[[4]](#footnote-5), violations[[5]](#footnote-6) and dependencies[[6]](#footnote-7), which could prevent the delivery of a safety functional requirement.
* To identify barriers to errors through system feedback, protection and other means such that the identified errors are recovered, or dependencies reduced within the task design.
* To identify reasonably practicable improvements to the design of tasks, equipment, staffing, procedures, training and workload to reduce the potential and consequence of errors, violations and dependency effects.
* To provide proportionate evidence to demonstrate that the actions important to safety and administrative controls are feasible and will deliver the required level of reliability to achieve the necessary safety functions. This supports the demonstration that risk has been reduced ALARP.

1. The inspector may consider whether:

* The dutyholder has a process which justifies the type and depth of analysis undertaken for human actions and administrative controls. Factors to be considered when determining the level and type of analysis required include fault consequence, the importance of the action or administrative control for achievement of the safety functional requirement, task difficulty, novelty and the frequency with which it is performed.
* The dutyholder’s analysis in support of the different safety case stages focusses attention on relevant aspects (e.g. the task analysis at the pre-construction safety report phase gathers evidence on aspects such as workspace, layout, staffing levels, and equipment design and raises requirements for aspects delivered later in the design process, such as procedures and training).
* The dutyholder’s analysis actively considers direct dependency[[7]](#footnote-8) between actions in the fault sequence and does not make judgments about feasibility and reliability based solely on individual claims.
* The dutyholder’s analysis assesses the totality of a task (e.g. all subtasks required to achieve the goal) and fault sequence (e.g. all tasks associated with pre initiators, initiators, preventative, protective and mitigative actions) rather than individual safety important actions in isolation. This is important to ensure that the impact of Performance Shaping Factors[[8]](#footnote-9) (PSFs) can be properly understood and managed.
* On a new plant, it is important that the dutyholder’s final qualitative analysis accurately reflects the engineering design, organisational structure and operational practices at commissioning. On an existing facility, it is similarly important that the HRA reflects the actual plant, organisation and work design in order that the analysis reflects tasks as they are undertaken rather than as they might be imagined through design drawings and operating procedures. For both new and existing plants, it is therefore important that any assumptions made during the development of the safety case are recorded and evidence provided to support their closure.
* The qualitative task analysis completed under EHF.5 underpins any subsequent human reliability quantification.

## Process, Methods and Tools for Undertaking HRA

### Data Collection

1. Data collection is an important consideration for determining the adequacy of the task analysis and task substantiation. How data is collected will depend on the maturity of the design and safety case. The inspector may consider the method of data collection to gain confidence that it is suitable and adequate to underpin the claims made within the safety case to an acceptable level for the safety case submission stage. The different ways data can be collected include:

* Tabletop exercises using process flow diagrams, design and layout drawings, procedures and discussion with designers and or operators.
* Models of the plant, both physical and virtual and discussion with designers / operators, supported by operating instructions and / or training material.
* Walkthroughs of the physical plant and discussion with designers / operators, supported by operating instructions and / or training material.
* Trials including optioneering, drills and exercises on actual plant and simulator exercises.
* Relevant operational experience[[9]](#footnote-10).
* Integrated system validation.

1. The inspector may consider whether:

* The dutyholder’s data collection activities include input as required from multiple disciplines including designers, operators, fault analysts and human factors specialists.
* The data collection method provides the greatest practicable level of fidelity to underpin the task analysis (e.g. a walkthrough of the physical plant will provide greater confidence than a tabletop exercise using design drawings).
* Where actions important to safety or administrative controls have a significant role in the delivery of safety functions, then the fidelity of data collection on which confidence judgments are made is commensurate with the novelty, complexity and importance of the action. For example, where high hazard decommissioning activities are planned, then trials of the techniques in a highly realistic simulation may be warranted. In these cases, the inspector should consider if adequate evidence has been collected to demonstrate that safety important actions can be completed with the necessary levels of reliability.
* The dutyholder has undertaken relevant operational experience reviews (including simulator and emergency exercise data) to inform the task analysis and the conclusions of the substantiation. The inspector should consider the relevance and applicability of the operational experience data used.

### Qualitative Data Analysis

1. Qualitative task analysis and the identification of reasonably foreseeable human errors, violations and dependencies provides a structured and systematic approach to understanding and examining the contribution of personnel to nuclear safety. ONR expects that the dutyholder will have a documented process for undertaking qualitative task analysis of actions important to safety, which is consistently applied to achieve the following outcomes:

* Substantiating the feasibility of the associated actions and administrative controls, to confirm that safety functional requirements can be delivered reliably.
* Understanding the errors and violations that may occur and ensuring that they can be adequately recovered by safeguards and system feedback integrated into the task design.
* Identifying dependencies between human actions completed by the same or different people or between humans and engineered systems. Eliminating or reducing dependency coupling mechanisms as far as reasonably practicable through design where these are identified.
* Informing the design of plant, tasks and operational systems and the identification of improvement options.
* Providing evidence to support the achievability and reliability claims made in the fault schedule and analysis. Both in terms of the initiating events and the adequacy of the safety measures that require human action.

1. This qualitative analysis can be broken down into four different but related activities:

* Task decomposition:
  + Breakdown of the task into individual task steps or actions for analysis. There are several methods to present this information. The aim is to gain an understanding of task sequencing and to identify improvements in the task design that will improve reliability.
* Error and violation analysis:
  + Identification of potential errors and violations and their mode[[10]](#footnote-11) that could impact on task reliability. This includes identifying the consequence of failure, as well as the means by which the identified errors and violations will be recovered through system feedback, protection and other mechanisms present or required within the design.
* Analysis of PSFs:
  + Identification of positive and negative factors, which influence task performance, related to aspects of the workspace and environment (see TAG 62 [12]), training (see TAG 27 [7]), procedures (see TAG 60 [10]), task ordering, equipment design and layout (see TAG 059 [9]), supervision, workload, staffing and fitness for duty (see TAG 61 [11]). These are captured in the SAPs against EHF.5 to 9, 11 and 12). The analysis of PSFs should primarily assess their impact on task performance, capture assumptions for what the future design needs to integrate and identify improvements, where this would improve task reliability.
* Direct dependency analysis:
  + Human Dependency - Identification of instances where multiple safety important human actions are claimed within a single fault sequence and the failure of one action increases the likelihood of failure of any subsequent actions. This can involve **within person dependence** where the same operator is responsible for the conduct of multiple safety actions or **between person dependence**, where different persons undertake safety actions to deliver safety functional requirements. The aim of the analysis is to identify dependency coupling mechanisms, assess the level of dependence and identify improvements to reduce this.
  + Human - System Dependence – Identification of instances where the potential exists for over-reliance on engineered or automated protection such that related human actions claimed in the safety case are not undertaken with sufficient reliability. The aim of this analysis is also to identify improvements in task or equipment design that will reduce dependency effects.

1. The inspector may consider whether:

* Task decomposition
  + The dutyholder’s process identifies an appropriate set of different analysis methods (e.g. hierarchical, cognitive, tabular, link, timeline, error analysis) and that guidance is provided to users as to the application of these in suitable settings.
  + The dutyholder’s task decompositions accurately reflect the way in which the plant operates, and tasks are undertaken in practice.
  + The dutyholder’s task analyses adequately model the time taken to complete task steps and compares this against the time available for delivery of the safety function.
    - Where dutyholders claim human actions over sustained periods, the task analysis demonstrates that the actions can be reliably performed under the prevailing conditions that may exist, through the identification of the positive PSFs.
    - Where the dutyholder claims human actions in short timescales, the claims and achievability have been thoroughly investigated[[11]](#footnote-12) (see TAG 010 [6]).
  + The task decomposition identifies the roles required to deliver each step in the task breakdown and identifies where communication and supervision is necessary.
* Error and violation analysis
  + The dutyholder’s process requires the proportionate application of error and violation analysis to identify all reasonably foreseeable mechanisms that could result in failure to deliver the required safety function.
  + The dutyholder’s submission has proportionately identified and assessed the effect of human errors and violations on delivery of the safety functions and their impact on fault sequence progression[[12]](#footnote-13).
  + The dutyholder has proportionately identified and assessed the cognitive error potential of diagnosis and decision-making tasks.
  + Opportunities to recover the effects of previous errors and violations through the design of the plant or organisational factors are identified and assessed. Where reasonably practicable, these have been implemented to demonstrate that the potential for consequences to be realised has been reduced ALARP.
  + Where significant consequences could be realised, specific consideration is given to instances where errors or violations during recovery actions could exacerbate a fault progression.
  + Where the dutyholder has claimed proof tests, acceptance tests or operational realignments as a means of recovering maintenance error, qualitative assessment is used to confirm the adequacy and validity of these claims.
* Analysis of PSFs
  + The dutyholder’s process requires the proportionate analysis of PSFs for tasks that include actions important to safety or administrative controls.
  + The dutyholder’s analysis proportionately identifies and assesses all reasonably foreseeable PSFs that have a positive and negative impact on the reliability with which the task is performed.
  + The dutyholder’s analysis considers the likely dynamics of an evolving event and variation in PSFs that might apply during time phases of the scenarios being addressed. These might include any variations such as different alarm patterns, instrumentation failures, different timing of events, growing impact of smoke from a fire, etc.
  + The dutyholder’s analysis considers reasonably foreseeable hardware failures that may impact the task progression, particularly with respect to diagnosis and decision making (e.g. failure of alarms). This considers and demonstrates how these failures would be revealed / recovered to minimise the negative impact on human performance.
  + Where the dutyholder’s analysis identifies PSFs that degrade task performance, their significance is assessed. Where relevant, shortfall(s) are identified, and suitable recommendations raised to increase the task reliability. These are collated to improve visibility.
* Dependency analysis
  + The dutyholder’s process includes a requirement to undertake proportionate human dependency analysis for faults that include actions important to safety or administrative controls.
  + The dutyholder’s qualitative analyses identifies and assesses the potential and impact of reasonably foreseeable direct dependency within and between persons in the following situations:
    - Dependency between Type A, Type B and Type C human actions identified in the same fault sequence.
    - Dependency between different Type C human actions identified in the same fault sequence.
    - Dependency between different Type A actions undertaken during EIMT activities of a single SSC, particularly with respect to the maintenance activity and return to service testing.
  + The dutyholder’s analysis considers reasonably foreseeable human system dependencies, where these are likely to delay performance of, or degrade the reliability of human actions
  + The dutyholder’s analysis identifies dependency coupling mechanisms (e.g. similarity of task, personnel, closeness in time, location, interfaces and cues) and has specified rules for allocating dependence levels between different actions.
  + Where necessary, the dutyholder has identified improvements to reduce the effects of dependence. This may include changes to allocation of function (see TAG 064 [13]) or measures to reduce the impact of dependency coupling mechanisms (e.g. using different instruments, changing responsibilities for individual task steps).

### Quantitative Data Analysis

1. Quantitative HRA provides HEPs for use in the fault analysis. Not all safety cases require quantification, dependent on the type of facility, complexity and level of risk etc. The aims of quantification are to:

* Provide numerical data for use in the deterministic safety analysis to support the identification of the DBA class and to demonstrate deterministic risk targets have been met by DBA safety measures.
* Provide numerical data for PSA models, including analysis of human errors for initiating event frequencies and the probability of failure of safety measures dependent on human action. Such initiating event frequencies may also provide a basis for the application of DBA.
* Allow use of the PSA to determine the total risk contribution from human action and identify the most important individual human actions through minimum cutset analysis and interpretation.
* Provide a limit on the claim on human action within a fault sequence, using a Human Performance Limiting Value (HPLV), to account for indirect dependency [[13]](#footnote-14).
* Identify where human error is making an unacceptable or dominant contribution to risk, and to identify improvements to reduce the impact of this on the fault sequence frequency, through the identification of shortfalls and recommendations.

1. ONR expects that the dutyholder will have a documented process for undertaking quantitative HRA and generating HEPs for use in fault analyses.
2. Quantitative HRA comprises of three components:

* Generation of HEPs for individual actions.
* Generation of conditional HEPs where multiple human actions are claimed in the same fault sequence (to account for direct dependency).
* Identification and application of appropriate HPLVs to account for indirect dependency effects within a fault sequence.

1. The inspector may consider the following:

* General considerations
  + Qualitative substantiation, considering task feasibility and reliability is used as the basis for the generation of HEPs. The level of analysis presented is proportionate to the task complexity, the importance of the claim and the level of reliably required from the safety case.
  + The dutyholder has appropriately justified the use of each of the techniques used for the derivation of HEPs, conditional HEPs and HPLVs. Special consideration may be warranted in situations where novel, unfamiliar or ‘in-house’ analytical methods and models are used, or where advanced designs or new technology is being applied.
  + In conjunction with the PSA inspector, consider whether HEPs, conditional HEPs and HPLVs have been correctly captured, modelled and positioned in the fault and event trees.
  + The dutyholder has proposed single or combined HEPs of lower than 1E-05 in any single modelled fault tree event or accident sequence. Where claims of this magnitude are made, the inspector may wish to ensure that the application of a hierarchy of controls is appropriate. They may also wish to ensure that the dutyholder can demonstrate that the PSFs and dependency analysis have been qualitatively assessed across the whole sequence and that reasonable risk reduction measures have been considered on an ALARP basis.
* Generation of HEPs for individual actions
  + The dutyholder’s approach to human error quantification is supported by suitable and proportionate qualitative task analysis, supported by the use of relevant operational experience, where appropriate and available. The HEPs derived reflect this analytical approach and show the effects of all relevant PSFs.
  + The quantification of HEPs is transparent and has been performed correctly and is repeatable (e.g. a second analyst would arrive at a similar result). Any limitations associated with the scope, data source and any underlying assumptions of the dutyholder’s quantification models and databases are clearly stated.
  + Where shortfalls and recommendations to improve reliability are identified within the qualitative analysis, the HRA is transparent on whether HEPs account for the implementation of these improvements, and the impact on reliability if they are not delivered.
  + Where the dutyholder has decreased the HEP due to the presence of positive PSFs, a robust justification is presented within the qualitative analysis.
  + Adequate evidence is provided to support the claimed error and violation recovery. The inspector may consider if the evidence has placed over reliance on the impact of extended time without considering the recovery mechanisms that the extended time provides. This might include new prompts such as alarms or plant symptoms, accident management arrangements and / or shift changeover protocols.
  + If a HEP has been selected from a database, justification is provided that the context and factors influencing human performance are sufficiently similar for the scenario under consideration, when compared to data for the actions / errors in the database.
  + Where the dutyholder has used bounding HEPs[[14]](#footnote-15), the dutyholder has provided a justification for the continued validity of the values and their relevance to the fault sequences in which they are applied.
  + If the dutyholder has used screening values[[15]](#footnote-16), an adequate justification is provided both for the use of screening values and for the screening values applied. The inspector may wish to confirm that the values chosen are sufficiently conservative for the case in which they are applied (see Para 70 for additional information on screening values).
  + Individual HEPs have been generated for significant maintenance, testing and calibration activities, where these are not adequately accounted for within equipment reliability figures. These HEPs are based on proportionate qualitative analysis.
* Generation of conditional HEPs to account for direct dependency
  + The dutyholder’s processes provide adequate methods for the derivation of conditional probabilities. The calculation of conditional probabilities uses information from the qualitative direct dependency analysis. Conditional HEPs should replace individual HEPs where more than one action is contained within a fault tree cutset.
* Provision of HPLVs to account for indirect dependency
  + The dutyholder has assessed direct dependency and derived conditional probabilities before the application of HPLVs. HPLVs are not used as a short-cut for preventing assessment to gain qualitative understanding of the task characteristics.

### Evidence Presentation

1. The HRA produced by a dutyholder should be clearly documented, transparent and auditable with coherent links to other parts of the safety case.
2. The maturity of the analysis is dependent on the stage in the design and safety case lifecycle of the plant or modification. At the early design stages, the requirements necessary to enable reliable completion of safety important actions and administrative controls should be identified. These will often be captured as assumptions within the early HRA submissions. As the design and safety case matures, the necessary requirements should be satisfied by the design. This should lead to a decrease in the number of assumptions identified in the HRA and an increase in qualitative analysis and evidence to underpin the feasibility and reliability of administrative controls and actions important to safety (see the HFI TAG [8] for more information).
3. The inspector may consider whether:

* The dutyholder has documented and justified the scope and applicability of the HRA, commensurate with the design and safety case lifecycle stage and the risk arising from human error.
* The HRA provides a demonstration of how the human claims within the safety case are brought together to show the totality of the human contribution to risk and that the human contribution is appropriate and adequately underpinned.
* The HRA adequately details the fault sequences and safety functional requirements considered by it and which actions important for safety and administrative controls have been assessed. The inspector may consider if the HRA is transparent and adequately links to the wider safety case. Where a bounding assessment is presented, the inspector may consider if the HRA explicitly identifies each fault sequence where the claim is made.
* The HRA provides proportionate analysis to demonstrate that the identified personnel will deliver / support delivery of the defined safety functional requirement, to the level of reliability required by the safety case.
* Key assumptions for human reliability and any issues / concerns raised during the qualitative and quantitative part of the HRA are clearly documented along with the approach to integrating the assumptions and issues into the system design.
* The HRA provides a clear conclusion on whether the action or administrative control has been substantiated.
* Where actions or administrative controls are not substantiated, a set of shortfalls to good practice are identified, which includes identification of the risk gap and prioritised recommendations necessary to achieve substantiation. This might include changing the design and where necessary the allocation of function (see ONR TAG 064 [13]).
* Where shortfalls and recommendations are identified, the dutyholder can demonstrate that these are being actively managed and can provide detail on the status of individual improvements, to support the demonstration that risk is reduced ALARP.

### Recording and tracking of actions important to safety

1. Safety important actions require effective management throughout the lifetime of the facility. Doing so supports modifications to plant, processes and equipment. One way of achieving this is using an Operator Schedule. ONR considers the use of such a schedule to be good practice. An Operator Schedule lists all administrative controls and other mitigating actions claimed in the safety case. The key benefit in this approach is to ensure that any changes to plant engineering or operations are developed in such a way that their impact on the human aspects of the safety case can be suitably controlled.
2. The following types of information may be appropriate for inclusion within the schedule, on a proportionate risk informed basis:

* A collated list (with unique identifiers) of all operational safety measures identified in the safety case. The list should identify the importance to delivery of the relevant safety function(s) (i.e. classification).
* The safety function(s) delivered or supported by each of the administrative controls and actions important to safety.
* Fault sequences in which the action is claimed.
* Any SSC’s necessary for the delivery of the operational safety measure safety functional requirement.
* Identification of the document in which the action substantiation is reported and the required review period.
* The dutyholder may also want to record details of the action important to safety including:
  + Where the action is performed.
  + What equipment and Human Machine Interfaces are required to deliver the action / task.
  + Operator instructions in which it is found and documentation demonstrating compliance, including the review periodicity.
  + Training in which it is covered and roles for who this training is provided, including the requirements for refresher training.
  + Personnel responsible for the completion of the action or administrative control and the necessary supervisory / verification requirements.

### HRA - Additional Notes

1. Dutyholders may attempt to argue a reduced need for HRA based on the use of conservative HEP screening values. Inspectors may view such an approach with caution, particularly where safety significant tasks are identified; in which case a systematic HRA should be sought, which includes appropriate task analysis. Inspectors may consider the following points.

* Screening on the basis of risk may fail to capture the safety importance of certain operator actions and errors. Assumptions will have already been made in the risk assessment regarding the human error and its quantification without any supporting HRA.
* Screening out a potentially safety significant task on the basis of what may be perceived to be a low reliability claim on operator action is not a sufficient justification for reduced HRA effort. For such operator actions, demonstration of the feasibility of the action and adequacy of the task context and conditions is still necessary. The dutyholder should always be striving to achieve higher levels of reliability of systems and minimisation of human error.
* Screening out on the basis of a low likelihood that an operator action will be called upon. By inference, such a task will be unfamiliar, hence more confidence and analysis will be required that the operator action is feasible for such circumstances.
* The dutyholder may claim that human errors have no quantitative impact on overall risk. Even if the HEPs are set at 1, the overall risk meets the Basic Safety Objective (BSO) and is tolerant of human error. The dutyholder may then claim that detailed HRA is not warranted. However, this approach requires assurance that all human errors and possible dependencies have been identified. Moreover, this approach does not provide for an ALARP assessment as it fails to seek reasonably practicable improvements to human reliability to prevent faults in the first instance and reduce the risk to ALARP. Such an approach is also implicitly accepting challenges to engineered safety systems and may create a culture in which human errors are implicitly accepted.
* Approaches or claims made by a dutyholder showing that the risk is insensitive to human error can result in the use of numerical based arguments being used in an attempt to justify lowered standards of plant and task design or for not making improvements. For any safety significant tasks argued by dutyholders in this manner, Inspectors should always seek qualitative human factors substantiation of the feasibility of the task.
* Time Response (Reliability) Curves (TRC) are sometimes used to justify not carrying out detailed task analysis. Inspectors should be aware that TRCs have been invalidated in at least two cases and their use by dutyholders should be treated with caution. Preferably, other methods should be used and/or the HEPs corroborated in some other way.

# References

|  |  |
| --- | --- |
| [1] | ONR, *Safety Assessment Principles for Nuclear Facilities. Revision 1,* 2020. |
| [2] | ONR, *NS-TAST-GD-094. Categorisation aof Safety Fucntions and Classification of Structures, Systems and Components.* |
| [3] | ONR, *NS-TAST-GD-005. Guidance on the Demonstration of ALARP.* |
| [4] | ONR, *NS-TAST-GD-006. Design Basis Analysis.* |
| [5] | ONR, *NS-TAST-GD-007, Severe Accident Analysis.* |
| [6] | ONR, *NS-TAST-GD-010. Early Initiation of Safety Systems,* 2021. |
| [7] | ONR, *NS-TAST-GD-027. Training and Assuring Personnel Competence,* 2022. |
| [8] | ONR, *NS-TAST-GD-058. Human Facotrs Integration.* |
| [9] | ONR, *NS-TAST-GD-059. Human Machine Interface (HMI),* 2022. |
| [10] | ONR, *NS-TAST-GD-060, Procedure Design and Administrative Controls,* 2021. |
| [11] | ONR, *NS-TAST-GD-061. Staffing Levels and Task Organisation,* 2022. |
| [12] | ONR, *NS-TAST-GD-062. Workplaces and Work Environment,* 2022. |
| [13] | ONR, *NS-TAST-GD-064. Allocation of Function Between Human and Engineered Systems,* 2022. |
| [14] | WENRA, *Safety Reference Levels for Existing Reactors 2020,* https://www.wenra.eu, 2021. |
| [15] | WENRA, *Waste and Spent Fuel Storage Safety Reference levels. Version 2.2,* https://www.wenra.eu/sites/default/files/publications/wgwd\_storage\_report\_final.pdf, 2014. |
| [16] | WENRA, *Decommissioning Safety Reference Levels. Version 2.2,* 2015. |
| [17] | WENRA, *Radioactive Waste Disposal Facilities Safety Reference Levels,* 2014. |
| [18] | WENRA, *Safety Reference levels for Existing Research Reactors,* 2020. |
| [19] | WENRA, *Guiance Document. Issue 0: Probabilistic Safety Assessment of Existing Research Reactors,* WGRR Guidance Document Issue O | WENRA, 2020. |
| [20] | IAEA, *SSR-2/1. Safety of Nuclear Power Plants: Design, Rev.1. (2016) https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1715web-46541668.pdf.* |
| [21] | IAEA, *SSR-2/2. Safety of Nucelar Power Plants: Commissioning and Operation, Rev. 1, (2016). https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1716web-18398071.pdf.* |
| [22] | IAEA, *SSR-3. Safety of Research Reactors (2016). https://www-pub.iaea.org/MTCD/Publications/PDF/P1751\_web.pdf.* |
| [23] | IAEA, *SSR-4. Safety of Nucelar Fuel Cycle Facilities, (2017). https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1791\_web.pdf.* |
| [24] | IAEA, *SSG-3. Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants.,* https://www.iaea.org/publications/8235/development-and-application-of-level-1-probabilistic-safety-assessment-for-nuclear-power-plants, 2010. |
| [25] | IAEA, *SSG-2. Deterministic Safety Analysis for Nuclear Power Plants. Rev. 1,,* 2019. |
| [26] | IAEA, *SSG-4. Development and Application of level 2 Probabilistic Safety Assessment for Nuclear Power Plants.,* 2010. |
| [27] | IAEA, *SSG-20. Safety Assessment for Research Reactors and the Preparation of the Safety Analaysis Report, Rev. 1, (2022)..* |
| [28] | IAEA, *SSG-25 Periodic Review for Nuclear Power Plants, (2013). https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1588\_web.pdf.* |
| [29] | IAEA, *SSG-42. Safety of Nucelar Fuel Reprocessing Facilities, (2017). https://www-pub.iaea.org/MTCD/Publications/PDF/P1744\_web.pdf.* |

# Glossary and Abbreviations

ALARP As low as reasonably practicable

BSO Basic Safety Objective

CBA Cost Benefit Analysis

CCF Common Cause Failure

CNS Civil Nuclear Security (Office for Nuclear Regulation)

DBA Design Basis Analysis

EIMT Examination, Inspection, Maintenance and Testing

HEP Human Error Probability

HFE Human Failure Event

HPLV Human Performance Limiting Value

HRA Human Reliability Assessment

HSE Health and Safety Executive

IAEA International Atomic Energy Agency

LC Licence Conditions

NPP Nuclear Power Plant

ONR Office for Nuclear Regulation

PIFs Performance Influencing Factors

PSFs Performance Shaping Factors

PSA Probabilistic Safety Analysis

SAA Severe Accident Analysis

SAP Safety Assessment Principle(s)

SOE Safe Operating Envelope

SRL Safety Reference Levels

SSC Structure, System and Component

TAG Technical Assessment Guide(s)

TRC Time Response (Reliability) Curves

WENRA Western European Nuclear Regulators’ Association

# Appendix 1 – Assessment Expectations for Review of HRAs for Nuclear Power Plants

This appendix provides more specific and detailed guidance for assessment of HRAs for Nuclear Power Plants (NPP). This is presented in the form of a Table of Assessment Expectations. The Table presents a check list of items that Inspectors may consider when assessing the HRA aspects of the PSAs for nuclear reactors. It is only intended for guidance and by no means should be taken to imply that Inspectors have no discretion when choosing the scope and depth of the assessment to be undertaken. Neither is it the intention of this appendix to replace any aspects of the main body of this TAG or to prescribe specific methods and approaches for conducting HRA. Whilst written primarily for NPPs, the principles can also be read across, in a proportionate way, to other types of facility

| **Table A1-2.5 Human Reliability Analysis (HRA)** |
| --- |
| The methodology/ies selected for the HRA, and in particular for the evaluation of HEP, including the choice of human reliability data sources, is/are justified. |
| The types of human failure events (HFEs), (i.e., those basic events in the fault trees and event trees which represent the human-induced failures of functions, systems or components) that are included in the logic model structure are identified up-front. Important types of HFEs and their causes have not been omitted. |
| The identification is complete of pre-initiating fault HFEs and includes individual and common-cause misalignments and mis-calibrations.  If some potential pre-initiating fault HFEs are not included in the model, adequate justification for their omission is provided.  The modelling of pre-initiating fault HFEs events is correct. |
| HFEs have been modelled at the appropriate level for each accident sequence, e.g. alternative representations of the HFE have been considered such a single act or omission, HFE broken down into specific contributing error types that result in the HFE. Different error rates and dependencies might be associated with various human error types that could result in the HFE. Has the analysis has considered different ways in which a given action might be implemented? |
| The HRA considers HFEs that might occur during the normal PSA sequence and context as well as plausible deviations from the normal context. |
| If HFEs associated with initiating faults are embedded in the technical data used in the estimation of initiating fault frequencies for the Full Power PSA, justification is provided that these human actions have been adequately captured. |
| During low power and shutdown modes the analysis of initiating faults has considered events caused by plant failures, those triggered by operator interactions and those caused by internal and external hazards |
| A systematic examination of NPP procedures for changing configurations, equipment testing and maintenance procedures has been carried out to identify potential human errors during the execution of such normal procedures that do, or may lead to, initiating faults. |
| In the absence of complete/detailed facility specific data to support the identification of human actions leading to initiating faults, all assumptions made to form the basis for an analysis are identified explicitly and shown to be appropriate. |
| The HRA method selected can adequately represent the aspects of the NPP shutdown relevant to human reliability which may be different to when the reactor is operating at power e.g. long time windows for operator actuation, status of procedural guidance and training, familiarity with shutdown accident transients, levels of supervision, availability of indications/status of control room, difficulties in diagnosing events, increased workload etc. |
| Post-initiating fault HFEs include failures to carry out required actions in response to procedures, alarms and other cues and un-required human actions in response to situations that have been diagnosed incorrectly. The identification of these events is complete.  If cases exist where the HFE related to the detection/decision part of the human action has been modelled separately from the HFE/s related to the manual actuation part of the human action, the rationale for this is clear.  If some potential post-initiating fault HFEs are not included in the model, adequate justification is provided.  The modelling of post-initiating fault HFEs events is correct. |
| For each pre-initiating fault HFE, all the operational activities which could lead to the human error are identified (e.g. surveillance tests, calibrations, maintenance activities or operational realignments).  Any operational activities screened out are justified. |
| In the absence of facility specific information, for each pre-initiating fault HFE, any assumptions regarding tests, maintenance tasks or operational realignments that could lead to the human error are stated.  A process is in place to ensure that these assumptions are captured in the future development of testing, maintenance and operational procedures and strategies and completion of system designs. |
| For each post-initiating fault HFE which involves failure to respond to procedural steps, equipment failures, alarms or other cues, the cues are identified. |
| In the absence of facility specific information, for each post-initiating fault HFE which involves failure to respond to procedural steps, equipment failures, alarms or other cues, the assumptions regarding the cues available to the operator are identified.  A process is in place to ensure that these assumptions are captured in the future development of procedures and completion of design. |
| Occasions for misdiagnosis of the situation by the operators have been analysed systematically.  HFEs resulting from identified credible mis-diagnosis have been modelled correctly (e.g. human actuations due to mis-diagnosis that change the course of an accident sequence will normally be modelled in the event trees. Un-required switching off of systems due to misdiagnosis will normally be modelled in the fault trees). |
| The human reliability quantification method/s selected is/are suitable for the specific type of HFEs addressed with the method. |
| Specific human error contributors to each HFE are identified:  • The task analysis is complete: sub-tasks included as possible contributors to the HFE and the ones which are not included are identified. The rationale for the exclusion of sub-tasks is clear.  • The possible human failure modes included (i.e. commission, omission, etc.) are identified. |
| Facility-specific and HFE-specific influences of the factors required by the quantification model (Performance Shaping Factors, PSFs) are identified.  Facility-specific information obtained from observations made during walk-downs and simulator exercises, review of procedures, discussions with, and interviews and questionnaires to personnel, etc, is used to characterise the PSFs for each HFE. The sources of information are identified and auditable. The way in which this information is used is transparent. |
| In the absence of facility specific information, all the assumptions made to characterise the PSFs (e.g. quality of man-machine interface, quality and availability of procedures, level of training, degree of supervision, accessibility, etc) are described and justified. A process is in place to ensure that relevant assumptions are captured in the future development of procedures and completion of the design. |
| Time windows are correctly assigned; justification is given for the choice of events that mark the start and end of the time windows (cues and limiting times), dead times and time spent on other tasks are accounted for and adjustments made as appropriate. |
| The quantification of all the HFEs is transparent.  The quantification of all the HFEs has been done correctly and in accordance with the HRA method/s selected. |
| If the probabilities for some HFEs in the models have not been calculated using detailed HRA analyses (as above), an adequate justification for the generic (screening) values used is provided. |
| Dependencies between HFEs appearing in the same accident sequence are identified and accounted for.  The process by which the candidates for dependency were identified is transparent.  Any assumptions made in the dependency analysis are described and justified.  The determination of the degree of dependency is transparent and justified.  The method by which the conditional probabilities of dependent HFEs are calculated is clear.  The dependency analysis is adequate. |
| A list of all the HFEs included in the PSA, and their associated mean probabilities and uncertainty ranges is included. This list is traceable to all the supporting analysis. |

1. Dutyholder has been used throughout this TAG as a single term that includes Licensees and other duty-holders, Requesting Parties participating in a Generic Design Assessment (GDA), and any other organisation or individual involved in the development or application of the safety case. [↑](#footnote-ref-2)
2. An action is substantiated when it is demonstrated with evidence to be feasible and sufficiently reliable. [↑](#footnote-ref-3)
3. Human actions important to safety and administrative controls are commonly referred to as human-based safety claims. [↑](#footnote-ref-4)
4. A human error is an action or decision which was not intended, which involved a deviation from an accepted standard [↑](#footnote-ref-5)
5. A violation is a deliberate, but not malicious, deviation from a defined rule, procedure or standard. [↑](#footnote-ref-6)
6. Dependency is the degree to which one erroneous action can impact the reliability of subsequent actions, or where common factors can impact the reliability of several actions within a single fault progression. [↑](#footnote-ref-7)
7. Direct dependence is the degree to which one erroneous action can impact the reliability of subsequent actions within a single fault sequence progression. [↑](#footnote-ref-8)
8. Performance Shaping Factors (also known as Performance Influencing Factors (PIFs)) are aspects of the task design (including the ordering of task steps; number and role of people including supervisors, design of workspaces, equipment, procedures and training), which positively and negatively impact on task performance. [↑](#footnote-ref-9)
9. Use of operational experience data can give valuable insight into error modes, PSFs and operational difficulties, which can inform the qualitative analysis. However, its use in isolation to demonstrate adequacy or to select HEPs should be treated with caution, due to the potential for an under reporting of the failure rate. [↑](#footnote-ref-10)
10. An appropriate schema for the identification of task errors, their external mode and psychological mechanism should be identified and used by the dutyholder in a proportionate manner. [↑](#footnote-ref-11)
11. For new designs, where the goal should be less reliance on human performance and incorporation of passive design features, assessors should seek a justification as to why short timescale scenarios/actions persist. [↑](#footnote-ref-12)
12. Recent judgements by the UK courts have made clear that Sections 2 and 3 of the Health and Safety at Work etc. Act 1974 are not limited, in the risks to which they apply, to risks that are obvious. They impose, in effect a duty on employers to think deliberately about things which are not obvious. It is imperative that risk assessments go beyond obvious risks that could arise as a result of individuals acting outside their training and procedures. [↑](#footnote-ref-13)
13. Indirect dependency accounts for the impact that common factors (e.g. general high workload within a team, or broader organisational or cultural factors) has on the reliability of several actions within a single fault progression. It also provides a limit to claimed reliability recognising that errors that have not been predicted could become dominant, if the joint HEP is very low. [↑](#footnote-ref-14)
14. Bounding HEPs are generic probabilities used to model common tasks / actions (e.g. changing a glove on a glovebox, responding to a glovebox loss of depression alarm), where they can occur in multiple locations throughout a facility. [↑](#footnote-ref-15)
15. Screening HEPs are generic error probabilities that are not based on qualitative analysis of the task and the identification of the PSFs impacting task performance. They are generally used in early deign and safety case stages to inform where and which human actions make the largest contribution to risk. [↑](#footnote-ref-16)