ONR GUIDE			
Human Reliability Analysis			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-063 Revision 4		
Date Issued:	October 2018	**Review Date:**	October 2021
Approved by:	S Allen	Human and Organisational Capability Professional Lead	
Record Reference:	TRIM Folder 1.1.3.776. (2018/332541)		
Revision commentary:	Revision		

TABLE OF CONTENTS

Published 10/18

1. INTRODUCTION

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

2. PURPOSE AND SCOPE

2.1 The Office for Nuclear Regulation (ONR) has the responsibility for regulating the safety of nuclear sites in Great Britain. The SAPs for Nuclear Facilities [1] provides a framework to guide regulatory decision-making in the nuclear permissioning process. The SAPs are supported by Technical Assessment Guides (TAGs) which further aid the decision-making process.

2.2 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), which states that *"Human reliability analysis should identify and analyse all human actions and administrative controls that are necessary for safety"*. This guidance also assists with the interpretation and application of EHF. 5 (and its supporting paragraphs 449 – 452) that is closely related to 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.

2.3 As with all guidance, Inspectors should use their judgement and discretion in the depth and scope to which they apply the guidance provided in this TAG. This TAG does not provide detailed information on how to judge the technical adequacy of the various Human Reliability Analysis (HRA) or Task Analysis (TA) aspects assessed, nor does it prescribe specific methods and approaches for conducting HRA or TA. Inspectors should use their own knowledge and experience when considering the adequacy of a dutyholder's approach.

3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

3.1 The Nuclear Site Licence Conditions (LC) place legal requirements on the licensee to make and implement arrangements to ensure that safety is being managed adequately. The licence conditions provide a legal framework which can be drawn on in assessment.

3.2 LC 14, 15 and 23 are particularly relevant to this TAG:

a) LC 14 requires the licensee to make and implement adequate arrangements for the production and assessment of safety cases. Normally, the licensee's safety case will need to contain TA in Design Basis Analysis (DA) and also HRA where a Probabilistic Safety Assessment (PSA) is produced.

b) LC 15 sets out the requirements for periodic review and reassessment 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.

c) 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 the role and contribution of the operator to safety, which is analysed through both the probabilistic (PSA) and deterministic elements (DBA) aspects of the safety case, will contribute to this process.

3.3 In addition, LC 17 sets out the requirement for management systems which give due priority to safety and for quality management (QM) arrangements for all matters that affect safety. In this respect, Licensees are expected to establish an adequate QM process that is effectively applied during TA and HRA.

3.4 Safety cases, including TA / 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, 35 and 36, require safety documentation.

3.5 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.

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

SAPs

4.1 ONR's expectations concerning human reliability analysis 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".

4.2 Para 465 to 468 expand upon EHF.10 in relation to the types of safety case analyses HRA may need to be included within (e.g. DBA, PSA and SAA), the types of human actions that should be analysed, the selection and application of probabilistic data for human errors and consideration of dependency.

4.3 SAP EHF.10 is strongly linked with EHF.5 Task Analysis 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".

4.4 Paras 449 to 452 expand upon SAP EHF.5 in terms of the factors and demands that should be considered in task analysis the expected level of descriptive detail and use, and the need to apply task analysis to all actions and controls identified under Principles EHF.3 and EHF.4, so that the safety case demonstrates high confidence in the feasibility of achieving requisite reliability of these actions and controls.

4.5 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".*

4.6 Para 447 to SAP EHF.3:

States *"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".*

Related to EHF.3 is SAP ECS.2 concerning safety classification and its supporting 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." The methods are outlined in the paragraphs that immediately follow paragraph 164.

4.7 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".*

Para 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".*

4.8 In addition to the above, the other SAPs of most relevance to requirement for HRA/TA are:

4.9 SAP FP.4:

Which 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".*

4.10 Para 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..."

4.11 Para 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"…

4.12 Para 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…".*

4.13 SAP FA.5:

States *"The safety case should list all initiating faults that are included within the design basis analysis of the facility";* whilst Para 628 states *"initiating faults identified in Principle FA.2 should be considered for inclusion in this list,…".*

4.14 SAP FA. 9:

States *"DBA should provide an input to…the identification of requirements for operator actions".*

4.15 Para 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; and (h) potential dependencies between separate human activities (either by the same or by different operators)".*

4.16 Para 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".*

4.17 Para 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".

Other Fault Analysis Principles are also applicable to Human Reliability Analysis. Therefore, Inspectors should also refer to the advice provided in the PSA TAG T/AST/030 when making judgements on the adequacy of a dutyholder's HRA.

WENRA reactor safety reference levels

4.18 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 [2], 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.

4.19 Issue O1.5 on Probabilistic Safety Analysis requires human reliability analysis to performed, taking into account the factors which can influence the performance of plant staff in all plant states.

IAEA safety standards

4.20 The IAEA Safety Standards (Requirements and Guides) were the benchmark for the revision of the SAPs in 2006 and 2014 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.

4.21 The guidance in this TAG is also consistent with IAEA guidance:

SSG-3: Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants [3] states:

"A structured and systematic procedure should be applied for the identification of the human interactions that need to be included in the Level 1 PSA."

"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."

4.22 IAEA guidance on Deterministic Safety Assessment for Nuclear Power Plants [4] and Development and Application of Level 2 Probabilistic Safety Analysis for Nuclear Power Plants [5] are also relevant to this TAG.

5. ADVICE TO INSPECTORS

Introduction

5.1 This section of the TAG aims to provide guidance on the assessment of HRA produced by dutyholders. The guidance provided in this section is applicable to the assessment of HRA for all types of nuclear facilities. More specific and detailed expectations for review of HRAs for Nuclear Power Plant (NPP) are given in the checklist in Appendix 1 to this TAG. The guidance provided in this TAG and Appendix 1 reflects relevant good practice expectations for NPP HRA.

Human Reliability Assessment

5.2 The safety of nuclear installations often requires claims on human action. Where safety important human actions and administrative controls are required and their need is justified, the feasibility and reliability of the actions should be demonstrated qualitatively using task analysis. This qualitative modelling should be used to substantiate any human-based safety claims and the quantitative modelling of the probability of the associated human errors. It is considered necessary to carry out task decomposition and analysis of sufficient depth in order to understand what is being assessed, the demands and influencing factors on personnel and to assist with the

identification of reasonably practicable design options or improvements to support human reliability. If this is not done, the HRA risks missing factors that may be important to error. ONR therefore considers HRA to be more than just quantification of human error. It is this holistic task analytical process that ONR considers as HRA.

5.3 ONR expects fault analysis (comprising DBA, PSA and Severe Accident Analysis (SAA) as appropriate) to be performed to enable both a qualitative and quantitative assessment of the risk arising from plant design and operation. The fault analysis must account for the impact of human activities affecting safety in order for it to be considered complete and to ensure that adequate protection against faults is provided. Assessors should have confidence in the dutyholder's methods for adequately identifying safety important operator actions, demonstrating their feasibility, identifying influencing factors and error mechanisms, quantifying the error potential of the actions, and determining reasonably practicable improvements. Task analysis provides the necessary support to the HRA process for this demonstration of adequacy.

5.4 HRA/TA may also be required (with or without quantification) for the DBA, PSA and SAA aspects of a safety case. Regardless of the application of HRA, the guidance in this TAG applies.

HRA Methodology

HRA - General Expectations

5.5 Understanding i) the plant context as it actually is in reality and ii) the process of task analysis underlying the human error quantification, are key elements of HRA. This is a foremost expectation of ONR for a dutyholder's human reliability analysis. Task analysis provides a structured and systematic approach to understanding and examining the contribution of personnel to nuclear safety, substantiating the feasibility of the associated actions, understanding the errors that may occur and for informing the design of plant and tasks and identification of improvement options. Task analysis also plays an important part in ensuring that the fault schedule and analysis is complete, through a detailed examination of important human errors.

5.6 Inspectors may consider whether:

1) The need for and level of reliance on safety important human actions have been justified on As Low As Reasonably Practicable (ALARP) grounds.

2) The dutyholder's process for identification of safety important human activities covers all operational modes/states including maintenance, testing and calibration activities, fault and emergency response.

3) The dutyholder can demonstrate that all relevant safety important operator actions and their modes of failure are identified and modelled in their fault schedule and analysis.

4) Sufficient justification has been provided in the PSA and HRA as to why any bounding fault scenarios are sufficiently representative and challenging in HRA/Human Factors terms.

5) The dutyholder has carried out an Operational Experience Review (of existing or similar plants), including a review of simulator and emergency exercise data of key events and items relevant to pre and post-fault scenarios documented and referenced in the safety case. If no such events are discernible, a Critical Incident Review approach should be evident. This will provide confidence that

the HRA and its assumptions have sufficient bearing on the realities of the plant and that the HRA is not purely a 'paper' assessment of a generic plant.

6) For new and future plant designs, operational advice and/or simulator data has been used to inform the HRA.

7) Task analysis has been used to demonstrate the feasibility of safety important operator actions and to underpin the quantification of human error.

8) The task analysis focuses on those tasks fulfilling functions related to safety in order to ensure that general statements made by a duty holder of having performed a task analysis do not mask a lack of effort in this key area. Task analysis key focus areas are listed in SAP EHF.5 and its supporting paragraphs.

9) The process of task analysis has been used to qualitatively identify and analyse foreseeable violations and demonstrate the adequacy of any plant and organisational factors that are claimed to minimise violation producing conditions. It is not, however, a current expectation that foreseeable violations are identified and quantitatively modelled in the safety case due to limitations in the sophistication of current HRA techniques to quantify such events.[1]

10) The dutyholder has demonstrated that, where the HRA identifies equipment, task, organisational or procedural modifications which could promote more reliable human performance, these modifications have been implemented where it is reasonably practicable to do so.

11) The human reliability analysis produced by duty holders is clearly documented, transparent and auditable with coherent links to the safety case.

12) Key assumptions for human reliability and any issues/concerns raised during the qualitative and quantitative part of the HRA are clearly documented along with approach to integrating the assumptions and issues into the system design. The dutyholder's approach for verifying the assumptions during operations to ensure they are delivering the required human reliability and for resolving issues/concerns is also specified and traceable.

HRA - Identifying and Modelling Human Tasks and Errors [2]

5.7 The starting point for the HRA is the identification and understanding of those human activities that are important to safety and how these may fail. This process should employ task analysis to an appropriate degree and draw on the fault schedule, fault analysis (e.g. fault and event tree) and operational experience data.

5.8 Inspectors may consider whether:

1) Task analysis or a similar structured and systematic human error identification process has been used to identify and define all safety important human tasks, sub-tasks and associated errors.

2) The dutyholder has identified pre-accident human errors (including maintenance, testing and calibration activities, plant alignment activities), direct initiating event

[1] 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.

[2] The term Human Failure Event (HFE) is commonly used in NPP PSA, which may be a single human error or result from a number of specific human errors.

human errors, human errors during the course of fault sequences and post-accident human errors (omissions, detection, diagnostic and decision errors, commission errors etc. and common cause human failures).

3) The dutyholder's methods for the identification of human error take into account Operational Experience and simulator data.

4) The error identification process and HRA method adequately represent aspects of the NPP or other facility shutdown and start-up, which may be different to when the reactor or other facility is fully operational.

5) Opportunities to recover the effects of previous errors are identified including any potential for recovery errors to exacerbate a situation.

6) The dutyholder has considered plausible deviations from normal plant conditions or fault sequences that might cause additional human errors leading to exacerbated or additional fault sequences.

7) The dutyholder has identified (and analysed) the cognitive error potential of diagnosis and decision-making tasks. Adequate and proportionate cognitive task analysis has been carried out for safety important tasks/scenarios requiring decision-making and diagnosis. The analysis considers aspects such as the time-window, information sources, prevailing conditions, operators' thought processes and decisions at key steps in the task/scenario. This analysis has informed potential diversions and deviations from the desired course of action and dominant failure path.

8) The dutyholder has considered during software development, the management and evaluation of human errors.

9) The dutyholder has conducted a maintenance review, which identifies any activities where maintenance, testing or calibration error could be significant and which may not be revealed during re-commissioning/setting to work.

10) Any human errors have been assessed on the basis of preceding or similar studies. If this is the case and/or previous studies are to be used, then these should be reviewed by the assessor to ensure their continued validity and relevance to the current case.

11) The Dutyholder's task analysis demonstrates that operators can reliably perform and sustain claimed actions over timescales assumed in the safety case and under the prevailing conditions that may exist.

HRA - Identifying and Modelling Performance Influencing Factors

5.9 HRA should qualitatively examine the various factors that can influence reliable human performance. Assessors should check that the dutyholder has also factored these considerations into their estimate of human error probabilities. Operational experience, task analysis and other sources such as plant design information and procedures are required to identify and understand such Performance Influencing Factors (PIF)[3].

[3] Performance Influencing Factors (PIFs), also known as Performance Shaping Factors (PSFs), refer to influences on human performance arising from specific task demands and from psychological influences (e.g. stress, fatigue, degree of supervision, working practices, organisational factors etc.), together with factors such as the physical workplace, interfaces and environment (SAPs EHF 6 and 7) procedures and training (SAPs EHF 8 and 9) etc.

5.10 Inspectors may consider whether:

1) The dutyholder's method for identifying PIFs is sufficiently structured and comprehensive and the quantitative effects of these are properly integrated into the production of Human Error Probabilities (HEP).

2) The dutyholder's analysis has identified all the credible causes for human errors of interest in their safety case.

3) Hardware failures that may contribute to human errors (e.g. failures of alarms or indications, etc.) have been identified and included in the HRA.

4) The dutyholder has presented a robust justification in the HRA for any positive PIF effects. Inspectors should exercise caution about the validity of assessed quantitative impacts for these PIFs.

5) The dutyholder has presented evidence supporting any claims regarding the ability of re-commissioning, test procedures and independent inspection procedures etc. to detect and recover any maintenance, testing or calibration error. Measures have been specified to combat common-cause failures due to such errors.

6) Assumptions regarding the reliability of proof tests, acceptance tests or operational realignments that could lead to detection and recovery of a human error have been stated and their adequacy and validity demonstrated.

7) The dutyholder's analysis considers the likely dynamics of an evolving event and variation in factors that might apply during time phases of the scenarios being addressed. These might include any variations in PIFs that (e.g. different alarm patterns, instrumentation failures, different timing of events, growing impact of smoke from a fire, etc.).

8) The dutyholder's HRA considers the effect of human error (omissions, inappropriate or unexpected actions, etc.) on the circumstances affecting task demands and task performance and whether this can result in significant changes to the evolution of a scenario.

9) The dutyholder has examined the opportunities and options for error recovery and the potential for further human error, which could exacerbate a fault. The HRA submission clearly distinguishes between self-recovery and prompted recovery. The reason for including recovery actions in the HRA is specifically justified rather than assuming, by default that recovery potential is inherent within every HEP. This will enable dependence to be properly considered with respect to recovery.

10) The dutyholder has provided a suitable justification for the basis of timing estimates for post-fault scenarios and responses (including evacuation). Short timescale scenarios/actions (less than 15 minutes) have been thoroughly investigated or given a pessimistic HEP4.

11) Claims on extra human reliability for extended timescales to recover from a fault and the use of lower HEP values are supported by evidence. Such evidence would include information about the duty holder's accident management arrangements and shift changeover protocols an assurance that roles and responsibilities for accident management are clearly defined, that priorities for action will remain clear and compelling, that sufficient competent staff will be available and that repeated

[4] For new reactor designs, which are claimed to be less reliant on human performance and incorporate passive design features, assessors should seek a justification as to why short timescale scenarios/actions persist.

and diverse cues exist to prompt action before post-fault situations degrade further.

12) Task analysis has been used to identify improvements to plant design, task design and organisation to reduce the influence of detrimental PIFs.

HRA - Identifying and Modelling Dependence

5.11 As with the hardware related aspects of PSA, dependencies between human actions must be accounted for to avoid underestimation of risk. The potential impact of dependency between separate activities (either by the same or by different persons) should be assessed. The HRA should qualitatively consider the effect of dependency on reliable human performance. Assessors should check that the dutyholder has also factored these considerations into their HEP estimates.

5.12 Inspectors may consider whether:

1) The dutyholder has specified their rules for allocating dependence levels and the HRA explicitly states its basis for allocating dependence and dependence levels.

2) The dutyholder has identified and examined any direct dependence mechanisms between the tasks being considered in the HRA.

3) The duty holder has examined, as appropriate:

- Contingent operator actions on which other actions/errors may be completely dependent.
- Dependence between pre-initiator human actions/errors
- Dependence between initiator human actions/errors.
- Dependence between initiator human actions/errors and recovery actions/errors and between recovery actions/errors themselves.
- Dependence between post-initiator actions/error (and any recovery actions/errors).

4) The dutyholder has identified improvements to reduce dependence mechanisms/factors.

HRA - Quantification of the Analysis

5.13 Human performance can make a significant contribution towards overall plant risk; hence, it must be assessed within the safety case as accurately and effectively as possible. The PSA needs to determine combinations of basic events such as operator errors and equipment failures, which can lead to a fault sequence and determine its frequency of occurrence. An often important component of the frequency assessment is the estimation of HEPs. HEP derivation may also be necessary as an input to initiating event frequency assessment for DBA.

5.14 Inspectors may consider whether:

1) The dutyholder's approach to human error quantification is supported by suitable and proportionate qualitative analysis including the consideration of operational experience. The HEPs derived reflect this analytical approach and show the effects of all feasible PIFs.

2) The dutyholder has proposed single or combined HEPs of lower than 1E-05 in any single modelled fault tree event or accident sequence. This should be challenged on the basis that there are uncertainties and random events where modelling

cannot be achieved. Where a value approaching 1E-05 is offered, the dutyholder should provide a robust, modern standards qualitative substantiation to support such a value, and there should be a clear and rigorous demonstration of task feasibility and optimised conditions for human performance. ONR would not ordinarily expect to see reliance on human reliability claims of this order being made, as this would suggest inadequacy in the dutyholder's defence in depth strategy and an imbalance in application of the hierarchy of controls.

3) Any limitations associated with the scope, data source and any underlying assumptions of the duty holder's HRA quantification models and databases are clearly stated.

4) The quantification of all the HEPs and HFEs is transparent. The quantification has been performed correctly, is underpinned by proportionate task decomposition and analysis as is in accordance with justified HRA method/s selected by the dutyholder and quality checked.

5) The dutyholder has used novel, unfamiliar or 'in-house' analytical methods and models, and the assurance of their provenance and validity is provided.

6) The dutyholder's HRA quantification methods are appropriate for both the specific type of HFE/human errors being modelled and the tasks being addressed.

7) If the HEPs for some human failure events in the PSA models have not been calculated using detailed HRA, an adequate justification for the generic (screening) values used is provided.

8) For advanced designs or where new technology has been introduced to existing plants (e.g. digital interfaces, computer-based procedures, advanced human system interfaces, intelligent agents, soft controls, etc.), the dutyholder has substantiated the validity and applicability of the use of any HRA quantification technique. This is best done by reference to human performance trials with the particular interfaces of concern. For new designs it is reasonably practicable to collect such data as such trials will be taking place for operational reasons. Alternatively, a sub-set of scenarios should be quantified using another technique to determine sensitivity of estimates to advanced interfaces. (Note that much human error data which underpins current HRA quantification models predate current computer-controlled interfaces and are based on human interactions with analogue HSI and traditional use of paper-based procedures). Assumptions that digital-interfaces are (or will be) generally better than conventional interfaces will require evidence to support these assumptions.

9) Cutsets and HEPs correctly take account of any recovery actions and direct dependencies between fault initiation, fault recovery and other separate activities (either by the same person or different individuals). All HEPs (and dependencies) have been correctly captured, modelled and positioned in the fault and event trees.

10) If any cutsets contain error recovery factors of more than a factor of ten, the duty holder has investigated these in more depth to ensure that all dependencies have been captured in the analysis.

11) Significant maintenance, testing, calibration and mis-alignment errors have been specified and quantified.

12) Where human errors have been grouped or bounded, each of the errors should have the same effect on the system.

13) Where the dutyholder has used screening values in place of HRA modelling (e.g. based on an assumption that any quantification would result in very low estimates of HEPs) the following characteristics have been considered:

- There is no common-cause potential between the initial error and recovery actions and direct dependency has been modelled.
- Required instrumentation, equipment and personnel necessary for any recovery action are available and demonstrably unaffected by the initial error or fault.
- Recovery factors have been demonstrated to be feasible under the likely conditions that prevail as a consequence of the original error or fault.
- The claimed recovery actions are relevant to all the initial errors that may occur and will uncover the error.
- There is a compelling signal that an error has been made.
- Possible errors during recovery have been identified.

14) The dutyholder has not used Human Performance Limiting Values (HPLVs)5 as a short-cut for assessment understanding and effort.

15) Direct dependency has been modelled before the application of HPLVs.

16) Where HPLVs have been used, task analysis has been carried out to ensure that no additional errors or dependencies exist that should be separately modelled.

17) Any HPLV use has been justified and correctly combined into the fault and event trees.

18) The dutyholder has conducted a review of the human actions covered by any HPLVs that appear in cutsets to highlight any cases where human action or unrevealed dependencies may be reducing reliability and where potential improvements should be considered.

19) The dutyholder has used generic HEPs claimed to be applicable to a number of similar activities e.g. decommissioning glovebox size-reduction. In such cases, it should be ensured that all potential human failure modes bounded by the generic HEP have the same effect on the system of interest. The task and its context should be reviewed on a case-by-case basis to ensure that all the assumptions and PIFs used in the original estimate of the generic HEP are valid for the case of interest.

20) 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.

21) If the HEPs in a new PSA/HRA are better than for an existing one, the dutyholder has provided an explicit justification in terms of what has changed from a human factors perspective. This also applies for prospective (design stage) HRAs.

HRA - Sensitivity and Importance Analysis

[5] HPLVs provide an equivalent approach for dealing with indirect dependence in HRA, similar to the manner in which, common mode limiting values or beta factor models are used to limit optimism in the reliability of hardware systems. HPLVs account for knowledge and modelling uncertainties (epistemic uncertainty) associated with human reliability analysis. It is important to note that HPLVs are not HEPs; they are used to bound a HEP cutset and limit already modelled HEPs once direct dependence has been considered.

5.15 Inspectors may consider whether:

1) The sensitivity of the results of the HRA to uncertainties in the data and assumptions used in the models has been assessed.

2) The sensitivity of the overall safety risk to the individual HEPs or HFEs is clear. The dutyholder's HRA submission has explicitly identified and discussed the interplay of HEPs and the significance of the human error contribution to plant risk via sensitivity and importance analysis. This has considered the overall impacts of dependence and the important human cutsets. Where human error is identified as making an unacceptable or dominant contribution, appropriate measures have been taken to reduce the potential for such error, or to re-design the plant so that operator action is not required or that the consequences are less severe.

3) Those HEPs and their uncertainty estimates that have the most impact on the overall uncertainty of the risk results are identified and measures have been taken to reduce these.

4) The dutyholder has tested any proposed improvements to ensure that relevant human factors good practice has been followed and that the revised risk is ALARP.

5) Any task that has been identified as safety important and the top event fault frequency is sensitive to the HEP value, the duty holder has carried out a search for dependence between sub-tasks/events.

Note. Those SAPs relating to assurance of validity of data and models (AV1 – AV8) and the guidance provided in TAG T/AST/030 can also be considered applicable to HRA.

HRA - Additional Notes

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

1) 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.

2) Screening out a potential safety significant task on the basis of 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.

3) 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.

4) 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 duty holder may then claim that detailed HRA is not warranted. However, this approach requires assurance

that all human errors and possible dependencies have been identified in the first instance. 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. SAP EKP.3 sets an expectation that the second line of defence-in-depth should include operator control actions that correct abnormal operation before safety systems are challenged.

5) Approaches or claims made by a dutyholder showing that the risk BSO 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.

6) Time Response (Reliability) Curves (TRC) are sometimes used as a means 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.

6. REFERENCES

[1] Safety Assessment Principles for Nuclear Facilities. 2014 Edition, Revision 0. Office for Nuclear Regulation.

[2] Western European Nuclear Regulators' Association. Reactor Harmonization Working Group. WENRA Safety Reference Levels for Existing Reactors. WENRA September 2014. http://www.wenra.org

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Analysis for Nuclear Power Plants. Specific Safety Guide Safety Standards Series No SSG-3, IAEA, Vienna (2010)

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Assessment for Nuclear Power Plants, Specific Safety Guide, Safety Standards Series No. SSG-2, IAEA, Vienna (2010)

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 2 Probabilistic Safety Analysis for Nuclear Power Plants. Specific Safety Guide Safety Standards Series No. SSG-4-4, IAEA, Vienna, (2010)

FURTHER READING

INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3), IAEA-Safety Series 50-P-12, IAEA, Vienna (1996).

INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev. 1, IAEA, Vienna (1999)

INTERNATIONAL ATOMIC ENERGY AGENCY, Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants, IAEA-TECDOC-1511, IAEA, Vienna (2006)

INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic safety assessments of nuclear power plants for low power and shutdown modes, IAEA-TECDOC-1144, IAEA (2000)

INTERNATIONAL ATOMIC ENERGY AGENCY, Living Probabilistic Safety Assessment (PSA), IAEA-TECDOC-1106, IAEA, Vienna (1999)

INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design Specific Safety Requirements, Safety Standards Series SSR-2/1, IAEA, Vienna (2012).

7. APPENDIX 1 - ASSESSMENT EXPECTATIONS FOR REVIEW OF HRAS FOR NUCLEAR POWER PLANTS

Introductory Note

This appendix provides more specific guidance on the assessment of HRA 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 should generally expect to see when assessing the HRA aspects of the PSAs for nuclear reactors. It is only meant 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.

Table A1-2.5 Human Reliability Analysis (HRA)
The methodology/ies selected for the HRA, and in particular for the evaluation of human error probabilities (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 include 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 mis-diagnosis 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 Influencing Factors, PIFs) 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 PIFs 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 PIFs (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.

8. GLOSSARY AND ABBREVIATIONS

ALARP	As low as reasonably practicable
BSO	Basic Safety Objective
DBA	Design Basis Analysis
HEP	Human Error Probability
HFE	Human Failure Event
HPLV	Human Performance Limiting Value
HRA	Human Reliability Analysis
IAEA	International Atomic Energy Agency
LC	Licence Conditions
NPP	Nuclear Power Plant
ONR	Office for Nuclear Regulation
PIF	Performance Influencing Factor
PSA	Probabilistic Safety Analysis
QM	Quality Management
SAA	Severe Accident Management
SAP	Safety Assessment Principle(s)
SRL	Safety Reference Level
TA	Task Analysis
TAG	Technical Assessment Guide(s)
TRC	Time Response (Reliability) Curve
WENRA	Western European Nuclear Regulators' Association