Office for Nuclear Regulation

ONR GUIDE			
ALLOCATION OF FUNCTION BETWEEN HUMAN AND ENGINEERED SYSTEMS			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-064 Revision 4		
Date Issued:	December 2017	**Review Date:**	December 2021
Approved by:	Mike Richardson	Professional Lead – Human and Organisational Capability	
Record Reference:	CM9 Folder 1.1.3.978. (2020/265795)		
Revision commentary:	Rev4: Updated Review Period		

TABLE OF CONTENTS

1. PURPOSE AND SCOPE

1.1 The Office for Nuclear Regulations (ONR) has the responsibility for regulating the safety of nuclear installations in Great Britain. The Safety Assessment Principles (SAPs) for Nuclear Facilities provide 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.

1.2 The purpose of this TAG is to provide guidance to aid inspectors in the interpretation and application of the SAP EHF. 2, Allocation of Function (AoF). It also assists with the application of other SAPs which set out expectations with regard to human factors integration, EHF1.

1.3 This TAG is not intended to be a detailed technical guide, it provides broad expectations on key points that the experienced Human Factors inspector may wish to consider in relation to allocation of function. The aim of the TAG is to advise and inform ONR inspectors in the exercise of their professional regulatory judgement concerning balancing the human factors aspects of system design against the ALARP principle. As with all guidance, inspectors should use their judgement and discretion in the depth and scope to which they apply the guidance provided.

2. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

2.1 The Nuclear Site Licence Conditions (LCs) 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.

2.2 LC 14, safety documentation, LC 15 Periodic Review, LC 19 Construction or installation of new plant, LC 20 Modification to design of plant under construction, LC22 Modification or experiment on existing plant, LC 23, Operating Rules and LC 27 Safety mechanisms, devices and circuits are relevant to this TAG.

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

3.1 ONR's expectations concerning appropriate allocation of function are set out in a number of SAPs. References to AoF, either implicit or explicit, are noted throughout the SAPs and specifically addressed in the sections covering Key Engineering Principles (EKP. 3 to EKP. 5), Safety Systems (ESS. 8 and 13), Control and Instrumentation of safety-related systems (ESR. 1 – ESR. 4, ESR. 7 and 8), Human Factors (EHF. 1 – 10).

3.2 The primary reference is SAP EHF. 2, Allocation of function which states:

> *'When designing systems, dependence on human action to maintain and recover a stable, safe state should be minimised. The allocation of safety actions between humans and engineered structures, systems or components should be substantiated.*'.

3.3 Para 446 expands on EHF. 2:

> *'Where safety actions are identified in the administrative safety measures (EKP. 5 paragraph 145f) they should meet the guidance in paragraphs 155 and 156. Principles ESS. 8 and ESS .9 on safety system initiation are also relevant here*.'

3.4 SAP ERL. 3, Engineered safety measures is also important:

> *'Where reliable and rapid protective action is required, automatically initiated, engineered features should be provided'.*

3.5 Para 194 expands:

> *'For requirements that are less demanding, or on a longer timescale, administrative safety measures, ie those involving operator actions based on procedures, may be acceptable. The choice of the safety measure should take into account the hierarchy in paragraph 155 and the category of safety function to be delivered (see Principles ECS.1 and ECS.2).'.*

3.6 Other related SAPs:

Paras 450, 451 and 452 supporting SAP EHF. 5 Task analysis:

> *'The analysis should evaluate the demands these tasks place upon personnel in terms of perception, decision making and action. It should also take into account the physical and psychological factors that could impact on human performance'.*
>
> *'The analysis should be sufficiently detailed to provide a basis for developing user interfaces, procedures and job aids, as well as helping define operator roles and responsibilities, staffing levels, personnel competence and training needs, communication networks and workspace design. Further principles related to these topics are provided below.'.*
>
> *'The workload of personnel required to undertake these actions and controls should be analysed and demonstrated to be reasonably achievable. Where practicable, this demonstration should form part of the inactive commissioning of the facility. The workload of personnel and its impact on the effective completion of tasks important to safety should be reviewed in periodic safety reviews and as part of emergency demonstration exercises.'*

3.7 Other SAPs and their supporting text also make reference to the need for a process to identify and analyse human error. These include the following:

SAP EHF. 3 Identification of actions impacting safety:

> '*A systematic approach should be taken to identify 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.'.*

3.8 Para 447 supporting SAP EHF. 3 Identification of actions impacting safety:

> '*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.'*

3.9 SAP FA9 Further use of DBA:

> *'DBA should provide an input into the safety classification and the engineering requirements for systems, structures and components performing a safety function; the limits and conditions for safe operation; and the identification of requirements for operator actions.'*

SAP EKP. 3 Defence in depth:

> '*Defence in depth 'a nuclear facility should be so designed and operated that defence in depth against potentially significant faults of failures is achieved by several levels of protection.'*

SAP EKP. 4: Safety function:

> *'The safety function(s) to be delivered within the facility should be identified by structured analysis'.*

EKP. 5 Safety measures:

> *'Safety measures should be identified to deliver the required safety function(s).'*

ESS.8 Automatic initiation:

> *'A safety system should be automatically initiated and normally no human intervention should be necessary following the start of a requirement for protective action'.*

Para 646 to FA.10 Need for PSA:

> *''PSA should assist the designers in achieving a balanced and optimised design, so that no particular class of accident or feature of the facility makes a disproportionate contribution to the overall risk, eg of the order of one tenth or greater. PSA should enable a judgement to be made of the acceptability or otherwise of the overall risks against Numerical Targets 5 to 9 and should help to demonstrate that the risks are, and remain, ALARP.'*

3.10 The guidance is also broadly consistent with IAEA standards and guidance. The key relevant IAEA publication is Ref. 3.

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

3.12 The guidance in this TAG is consistent with the following harmonisation issues from the WENRA Reactor Safety Reference levels [Ref. 2], which represent good practices in the WENRA member states, are relevant and should be taken into account by the inspector:

- Issue E: Design Basis Envelope
- Issue F: Design Extension
- Issue G: Safety Classification of Structures Systems and Components

- Issue H: Operational Limits and Conditions (OLCs).
- Issue N: Contents and Updating of Safety Analysis Report
- Issue O: Probabilistic Safety Analysis (PSA).
- Issue Q: Plant Modifications.
- Issue T: Natural Hazards.

4. ADVICE TO INSPECTORS

4.1 Introduction

4.2 IAEA guidance (Ref. 3) states that 'the assignment of tasks between man and machine may be the most critical activity in the design of new process plant and major retrofits. It warrants a design approach that is commensurate in quality with high levels of plant safety and production performance sought from nuclear plant.' ONR supports this view.

4.3 Operators are involved in all aspects of operations in various ways and to differing extents, receiving information and making decisions based on this information and by direct and indirect interaction through manual and automatic controls. In automatic systems, this interaction may be less obvious, for example, setting or adjusting controls or through maintenance activities.

4.4 Typically, automation broadly includes automation of a function, system component or supporting level; this includes automation of control and cognitive functions traditionally carried out by people including diagnosis and decision-making. Automation is changing through use of intelligent systems to encompass tasks that have typically been controlled by operators. Examples include: analysis of off-normal conditions, situation assessment and response planning. Human factors aspects of such applications are considered in more detail in the HMI and Procedures Technical assessment guides; NS-TAST-GD-059 and NS-TAST-GD-060 respectively.

4.5 The balance of AoF is not a simple either/or situation. There are many permutations that can be considered, involving combinations of both static and dynamic allocation. There is therefore a continuum of operator control and the Dutyholder's decisions for AoF need to demonstrate the appropriateness of the allocation of tasks and functions.

4.6 The general principals for allocation of function are relevant to each stage of the lifecycle; the Dutyholder's AoF decisions are not restricted to the context of new nuclear power plants. Inspectors should consider whether an adequate AoF justification has been provided for:

- Design of all new nuclear facilities.
- Refurbishment or modification to existing installations.
- Periodic review of safety.

4.7 Historically, the allocation of functionality has been considered to be fairly straightforward, by allocating on the principle that humans are better than machines for some functions and vice versa. However, advances in technology mean that traditionally 'human' tasks can now be automated. The AoF criteria used to allocate functionality have therefore broadened to encapsulate advances in Human Factors

research. In addition, AoF decisions must be able to demonstrate appropriate consideration of the hierarchy of control and record and justify tradeoffs. For these reasons the traditional approach to AoF is considered to be overly simplistic and the degree to which functions are automated should be informed by a systematic analytical process that is integrated within the design process starting with the concept of operations and continuing throughout optioneering and design review. AoF should be influenced by the safety functional claims made in the safety case, consideration of the hierarchy of protection and Human Factors analysis.

4.8 General Expectations

4.9 Inspectors may consider whether:

- The Dutyholder has justified its decision for allocation of safety actions between people and automation; a process referred to as Allocation of Function (AoF).
- The Dutyholder's proposed design and modification of any system includes a specification of the way in which safety and other functions will be achieved, considering the principles of defence in depth and hierarchy of safety measures.
- The Dutyholder has provided a demonstration that the allocation of function takes into account all of the factors that influence effective and reliable *system* performance. Inspectors should apply particular scrutiny to decisions to assign functions to the operator which require:
    - Rapid of long term processing of large quantities of data.
    - High levels of accuracy of information processing.
    - High repeatability.
- High levels of reliability (see NS-TAST-GD-063).
- Reliance upon recovery in short timescales (see NS-TAST-GD-010).
    - Completion in hostile environments.
- The Dutyholder has demonstrated that where there is a potential for competing demands/constraints to influence the allocation of safety functions between humans and machines, a balanced consideration of both options has been through ALARP review. For example, where the justification requirements of IEC61508 (Ref. 6) are difficult to achieve, leading to new or increased claims on human action, the HF inspector should consult with the relevant Control, Electrical and Instrumentation discipline inspector regarding substantiation of reliability claims.
- The Dutyholder's design decisions made during the allocation of function analysis and development of its concept of operations were made using a balanced approach amongst what is technically feasible, what is appropriate for the safety of the plant, and human capabilities and limitations.
- The Dutyholder's allocation of safety function decisions are compatible with the principle of hierarchy of control as set out in SAP EKP. 5.

4.10 When accessing application of AoF by the Dutyholder, the inspector should consider whether:

- The Dutyholder has demonstrated that the AoF solution is compatible with concept of operations, staffing concept and capabilities of the end users.
- The Dutyholder has demonstrated an interdisciplinary approach to AoF. AoF is not a purely Human Factors domain; AoF decisions should be based upon input from the relevant engineering disciplines, operational personnel, safety case claims and assumptions and Human Factors principles. In recognition of this, the Dutyholder should provide an audit trail of the decision making process, explicitly outlining and justifying the rationale for trade offs between requirements in the ALARP process.
- The resultant AoF has been appropriately informed by DBA and PSA and Human Factors analysis.
- The Dutyholder has used the review of AoF to inform the assumptions and claims made in its HRA/PSA to ensure that performance shaping factors are accurately accounted for and the balance of risk between human and automated functions is justified.
- The Dutyholder has considered if relevant good practice is represented by the AoF in similar installations.
- There is contingency in the arrangements to allow for iteration when Human Factors analysis challenges the assumptions made during the initial AoF.
- The AoF has been used as input to the design of procedures and operator training needs/competence requirements.
- The Dutyholder has conducted a comprehensive Human Factors/ergonomics evaluation and testing/trials of the design and development of the AoF. This analysis has demonstrated that the AoF is effective in the context of the design philosophy and safety case claims and assumptions.
- The Dutyholder has integrated Human Factors/ergonomics best practice in all AoF areas and not just focussed on the more high profile systems.

4.11 **Procedures and Process**

4.12 The Dutyholder's arrangements should provide for explicit, proportionate consideration and justification to AoF. To demonstrate this, AoF needs to be formally represented in associated processes. In assessing AoF, Inspectors should consider whether:

- The Dutyholder's arrangements for design and modification call for consideration and justification of AoF. These arrangements should provide for:
    - Consideration of AOF during optioneering and throughout the continued development of the plant design and safety case.

- A process for identification of AoF requirements that covers all safety and operational functions necessary for all plant operational modes/states including maintenance, testing and calibration activities and normal operations, fault and emergency response.
- AoF as a specific item in the HFIP/design documentation. This should outline the approach and methods to be used and present detail of the mechanisms which will assure appropriate input into AoF decisions.
- Demonstrable application of the ALARP principle, especially where decisions are made not to automate actions assigned to individuals.

- The Dutyholder has a demonstrable audit trail which documents the decision-making process and the results of the Allocation of Function decisions including:
  - The changes in allocation introduced by the proposed systems.
  - The basis for such allocations.
  - The verification of the acceptability of the allocations.
- AoF is appropriately reflected in the Dutyholder's design arrangements, including the design justification reports.
- The Dutyholder can demonstrate competency in AoF within the Design Authority.
- The Dutyholder has demonstrated the adequacy of the AoF decision through testing, verification and validation throughout the design process.
- The Dutyholder has a process for monitoring system performance to proactively identify where AoF decisions need to be revisited.

4.13 **Concept of Operations**

4.14 One of the outputs from the AoF decision making process is a specification of the functionality of the required automated systems. The underlying goal is to deliver high quality system performance in terms of safety and reliability and to demonstrate that the tasks of the operator, and interaction with the chosen technology, are achievable and appropriate. Therefore, any proposed allocation should be assessed systematically against both Human Factors and control systems engineering criteria. Allocation of Function can be applied at two levels; global AoF which defines the intended operational concept and associated balance between operation interaction and automation at a high level; and a low task/subsystem/component AoF which considers and justifies the balance at a detailed level. It is possible for the balance of AoF at this lower level to be different from the high level operational concept.

4.15 When assessing the Dutyholder's approach to AoF at the global/systems level the inspector should consider whether:

- The Dutyholder's AoF is considered on a systems basis because, in the total system, it is humans who are in overall control and it is they who must take the decisions which will enable the system to meet its performance objectives and which will prevent or mitigate accidents.

- The Dutyholder has applied an iterative approach to AoF. For example, the safety case/PSA takes account of human actions in system operation and maintenance and will assign quantified values to them. Results of the PSA may indicate where performance requirements of a function exceed the capabilities of humans and automation or task redesign should be considered.

- The Dutyholder can demonstrate a clear understanding of the system requirements.

- The proposed concept of operations is compatible with the staffing concept and management systems.

- The ALARP process adequately accounts for factors such as through life feasibility; maintenance, repair obsolescence, training, procedures and makes allowance for these.

4.16 **Potential for loss of "situational awareness"**

4.17 By reducing the level of interaction with the system, automation may increase the risk that operators can no longer identify what the system is doing – that is they lose "situational awareness". This may degrade performance when the operator is required to carry out plant diagnosis, fulfil decision making tasks, and identify and respond to parameters that are out of specification. As a defence against loss of situational awareness, certain tasks might be allocated to the human operator in order that manual or cognitive skills which would otherwise be required infrequently are maintained. The inspector should consider whether:

- The Dutyholder has considered the potential for, and implications of, loss of situational awareness and provided adequate assurance that operators awareness of the current operational state will be maintained such that operators will detect and respond appropriately to pre-initiating faults and fault conditions.

- The Dutyholder's AoF has considered factors such as prolonged vigilance, boredom and fatigue.

4.18 **Task/sub system engineering Allocation of Function**

4.19 This is concerned with detailed assignment, evaluation and justification of specific system design options. It is noted that the AoF at this level may not be consistent with the higher level operational design intent.

4.20 The inspector should consider whether:

- The Dutyholder has given appropriate consideration to the task and task context. Particular attention should be given to allocation of tasks to humans on failure of automated systems to gain assurance that the claims can be supported.

- The Dutyholder has considered the negative impacts of automation. For example:

- System induced dependency.
- Health and safety concerns.
- Long periods of inactivity resulting in boredom.
- Loss of situational awareness.

- The AoF has been appropriately informed by task analysis and the Dutyholder can demonstrate that the AoF is iterated in response to analysis and design changes.
- The Dutyholder has demonstrated that the AoF is compatible with the operator's physical and psychological capabilities for all operations; maintenance examination, testing, operation of the plant.
- The chosen AoF is compatible with requirements for operator actions necessary to maintain compliance with operating rules.
- The Dutyholder has considered the role of each team member – it is important that operators feel that they have retained control over the system. Similarly they should feel that they are being productive and fulfilling a useful role. If these needs are not satisfied then it is likely that the human operator's overall performance will be degraded.
- The Dutyholder has considered the need for oversight of system performance by supervisors.
- The Dutyholder has considered whether the totality of tasks assigned to an operator when carried out under the worst possible conditions allow him to maintain an adequate level of performance. Allocation should consider the whole of the job rather than individual tasks and responsibilities. The benefits of training systems embedded in the HMI should be considered. Inappropriate sharing of tasks between operators should be avoided. Allocation should consider the role of each person in the system. The designer may have to take account of limitations in availability of operators and allow for flexibility in performing tasks.
- The Dutyholder has considered the overall workload in the AoF and demonstrated this is acceptable.

4.21 **Allocation of Function and the Safety Case Lifecycle**

4.22 There are specific issues relevant to the life cycle context that shape regulatory expectations. These are expanded upon below.

4.23 **Design of New Plant or Facility**

4.24 It is likely that any application for a nuclear site licence in regard to new power plants or new nuclear processes will involve substantially more automation than existing plants. However, it is not acceptable to propose automated functions simply on the basis of technical feasibility. The inspector should consider whether:

- The Dutyholder has adequately justified the proposed level of automation and demonstrated that it supports safety and operational

goals and is compatible with the capabilities and requirements of the affected individuals.

- The automation of these functions does not itself introduce potential for compromised human performance – for example, by compromising the operator's "situational awareness".

4.25 **Modification of Existing Plant**

4.26 In the context of refurbishment, the AoF process will normally apply to decisions about implementing additional automation. Thus, in modernisation, high-level plant functions are seldom changed, but new plant systems and interfaces can alter the role of personnel and so the potential for human error. Such automation can involve a process control sequence or it can be applied to the support of operator activities such as fault detection, diagnosis and decision-making. These changes are a deliberate and intended consequence of the modification.

4.27 Inspectors should consider whether the dutyholder has:

- Appropriately considered the impact of the proposed modification on the overall balance of AoF.

- Where relevant, the Dutyholder has compared its proposed AoF with the existing design when AoF is considered for plant upgrades and modification. Unlike completely new designs, it is not expected that AoF is started from first principles.

4.28 **Periodic Review of Safety**

4.29 In line with expectations of the periodic review of safety, the Dutyholder is expected to provide a substantiation of the current operational philosophy against modern standards. The inspector should consider whether:

- The Dutyholder has revisited the claimed demands on automated systems and the balance of protection given by these, the human-based safety claims and required responses of the human operators in regard to these automated systems.

- The Dutyholder has included a review of the current AoF against technological and Human Factors advances and demonstrated that the Allocation of Function is still appropriate and reduces risk to ALARP.

- Where the review identifies shortfalls in engineering, plant modifications have appropriately considered the potential for automation, and its reasonable practicability.

- The Dutyholder has considered the impact on task performance where AoF decisions change the demands upon the operator, for example increasing vigilance requirements, changing competencies or shifts the reliance onto the operator for complex maintenance.

5. REFERENCES

1 Safety Assessment Principles for Nuclear Facilities. 2014 Edition, Revision 0. ONR. www.onr.gov.uk/nuclear/saps/saps2014.pdf.

2 WENRA Safety Reference Levels for Existing Reactors. September 2014. Western European Nuclear Regulators' Association Reactor Harmonisation Working Group.

3 IAEA Tecdoc 668 – *The role of automation and humans in nuclear power plants.* IAEA, Vienna, 1992 ISSN 1011-4289.

4 NUREG 0711 (2004) *Human Factors Engineering Programme Review Model* NUREG-0711, Revision 2. Washington D.C. US Nuclear Regulatory Commission.

5 NUREG CR/0700 (2002) *Human-System Interface Design Review Guidelines*. NUREG-CR/0700, Revision 2. Washington D.C. US Nuclear Regulatory Commission.

6 IEC61508 *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*.