|  |
| --- |
|  |
| ONR Technical Assessment Guide  Allocation of Function Between Human and Engineered Systems |



ONR Technical Assessment Guide (TAG)

Allocation of Function Between Human and Engineered Systems

Authored by: Nuclear Safety Inspector

Approved by: Human Factors Lead

Professional Lead: Human and Organisational Capability

Issue No.: 5

Publication Date: May-23

Next Major Review Date: May-28

Doc. Ref.: NS-TAST-GD-064

Record Ref. No.: 2022/32281

Revision commentary

|  |  |
| --- | --- |
| Issue No. | Description of Update(s) |
| 5 | Issue 5.0 – The TAG has been re-structured to incorporate guidance on the allocation of function (AoF) process and is consistent with that described in BS EN 61839:2014.  Guiding principles in relation to the use of automation have also been extended. These revisions complement and provide clarification on the implementation of the existing guidance contained within the TAG. BS EN 61839:2014 has also been added to the supporting References for the TAG and is considered by ONR to be part of the body of guidance which forms Relevant Good Practice.  Additional explanatory text has been added to improve the usability of the TAG to better support regulatory activities. |

Contents

[1. Introduction 4](#_Toc137115726)

[2. Purpose and Scope 4](#_Toc137115727)

[3. Relationship to Licence and other Relevant Legislation 4](#_Toc137115728)

[4. Relationship to SAPs, SyAPs, WENRA Reference Levels and IAEA Safety Standards 5](#_Toc137115729)

[5. Advice to Inspectors 9](#_Toc137115730)

[6. Appendix 1 – AoF process 24](#_Toc137115731)

[References 25](#_Toc137115732)

# 1. Introduction

The Office for Nuclear Regulation (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 [1]. The SAPs are supported by Technical Assessment Guides (TAGs) which further aid the decision-making process

# 2. Purpose and Scope

1. The purpose of this document 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 about human factors integration, EHF.1.
2. This document 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 AoF. The aim of the document is to advise and inform ONR inspectors in the exercise of their professional regulatory judgement concerning balancing the allocation of function between the human and technology as part of system design. It also supports assessment of dutyholders’ submissions and their demonstration that risk is reduced to As Low As is Reasonably Practicable (ALARP). As with all guidance, inspectors should use their judgement and discretion in the depth and scope to which they apply the guidance provided.

# Relationship to Licence and other Relevant Legislation

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. 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, LC 22 Modification or experiment on existing plant, LC 23, Operating rules and LC 27 Safety mechanisms, devices and circuits are relevant to this TAG.

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

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, 9 and 13), Control and Instrumentation of safety-related systems (ESR.1 – ESR.4, ESR.7 and 8), Human Factors (EHF.1 – 12).
2. The primary reference is SAP EHF.2, Allocation of safety actions 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.’.

1. Para 446 expands on EHF.2:

‘Where administrative safety measures are identified to deliver safety functions (see Principle EKP.5) the guidance in paragraphs 155 and 156 should be followed. Principles ESS.8 and ESS.9 on safety system initiation are also relevant here.’

1. SyAP SyDP 3.1 Identification and Analysis of Security Tasks and Roles, Para 97, highlights the need to consider security in concert with safety.

‘The analysis should evaluate the demands these tasks place upon personnel in terms of perception, decision making and action. It should provide evidence to underpin the decision to allocate security functions to humans and should support the demonstration of a balanced design between human and engineered security measures avoiding an overreliance on the human to deliver security functions.’

1. SAP ERL. 3, Engineered safety measures are also important:

‘Where reliable and rapid protective action is required, automatically initiated, engineered features should be provided’.

1. Para 194 expands:

‘For requirements that are less demanding, or on a longer timescale, administrative safety measures, i.e., those involving operator actions based on procedures, may be acceptable. 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).’.

1. Other related SAPs - Paras 450, 451 and 452 supporting SAP EHF.5 Task analysis outlines supporting expectations:

‘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.’

1. Other SAPs and their supporting text also refer to the need for a process to identify and analyse human error. These include the following:
2. 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.’.

1. 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.’

1. Para 632 and 633 of SAP FA.6 Fault sequences:

‘The fault analysis should establish that adverse conditions that may arise as a consequence of the fault sequence [this includes any relevant internal and external hazards in the sequences] will not jeopardise the claimed performance of the safety measures and 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. SAP FA.9 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.’

Operator actions broadly fall into two categories:

The routine normal operator actions which are required to sustain compliance to limits and conditions of safe operation concerning supervision, surveillance and Examination, Maintenance, Inspection and Testing (EMIT) (where ESR.1 to 4 come in).

Operator actions which may be required to support a safety system acting in the event of a fault/abnormal operating condition arising and recovering the system back to normal operations (where ESS 8, 9 and 13 come in at level 2 and 3 of the defence in depth hierarchy).

1. SAP EKP.3 Defence in depth:

‘Nuclear facilities should be designed and operated so that defence in depth against potentially significant faults or failures is achieved by the provision of multiple independent barriers to fault progression.’

1. SAP EKP.4 Safety function:

‘The safety function(s) to be delivered within the facility should be identified by structured analysis’.

1. EKP. 5 Safety measures:

‘Safety measures should be identified to deliver the required safety function(s).’

1. ESS.8 Automatic initiation:

‘For all fast acting faults (typically less than 30 minutes) safety systems should be initiated automatically and no human intervention should then be necessary to deliver the safety function(s).’.

1. 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, e.g., 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.’

1. This guidance is also broadly consistent with IAEA standards and guidance. The key relevant IAEA publication is TECDOC 668 - The role of automation and humans in nuclear power plants [2].
2. 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. The guidance in this TAG is consistent with the following harmonisation issues from the WENRA Reactor Safety and Waste and Spent Fuel Storage Safety Reference levels [3]. These represent good practices in the WENRA member states, are relevant and should be considered by the inspector:

* Issue E: Design Basis Envelope for Existing Reactors
* Issue F: Design Extension of Existing Reactors
* 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 SV: Internal Hazards
* Issue TU: External Hazards

# Advice to Inspectors

## Introduction

1. IAEA guidance [2] states that ‘the assignment of tasks between [the human] 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. The process by which tasks are assigned to humans and technology during system design is known as Allocation of Function (AoF). It is an integral part of the optioneering process, where a decision between a human or technological or hybrid solution is to be made.
2. The concept of AoF is applicable to all licensed sites and all stages of the design process, all normal operational, fault, and accident conditions, and the full site lifecycle.
3. The functions performed on a nuclear licensed site fall into four main categories:

* Operational/Process
* Safety
* Security (Cyber and Physical)
* Safeguards

1. Additionally, AoF considerations are pertinent during the transportation of radioactive materials. For brevity, throughout this TAG, the term safety incorporates transport within its scope.
2. Operational/Process functions are those that deliver the commercial or product goals, e.g., produce electricity, reprocess fuel, and decommissioning hazard remediation.
3. Safety functions are defined [4] as a specific purpose or objective that must be accomplished in the interests of safety during normal operations and during fault or accident conditions.
4. Security functions are defined [5] as a specific purpose or objective that must be accomplished so that the overall cyber protection system or physical protection system outcome can be achieved.
5. Inspectors should be cognisant of the fact that security functions are derived from sector specific security legislation [6]. It is therefore important to ensure that inspectors from CNSS are involved in decision making relating to security related AoF.
6. AoF should consider allocation at both the macro and micro level of the system design. At the macro level, dutyholders may consider it advantageous to automate a high-level function (for example criticality control or decay heat removal). As the system design matures, it may not be feasible (or it may be advantageous) to allocate some of the lower-level functions to the human. Consideration at both levels is important because a technological solution often requires several supporting human actions to deliver the necessary operational and safety performance, and security outcomes. In considering AoF, dutyholders should recognise the way in which humans interact with technology. The following model of human interaction [7] shows the decision action process. Automation can replace all or some of these steps.

* Information acquisition
* Information analysis
* Decision and action selection
* Action implementation

1. The assignment of functions between humans and technology is not a simple either/or consideration. There are many permutations that can be considered, involving combinations of both static and dynamic allocation along with levels of automation which vary the level of involvement of the operator within the control loop.
2. The continuum of operator control requires dutyholders to demonstrate the appropriateness of the allocation of tasks and functions along with any wider implications to system and site safety.
3. AoF is also central to the process of optioneering where decisions between human or technological solutions are made. Inspectors are therefore advised to consider relevant guidance in relation to optioneering and the demonstration of ALARP [8].
4. Historically, due to the previously simplistic capability of automation, the allocation of functionality has been straightforward, by allocating on the principle that humans are better than machines for some functions and vice versa.
5. However, advances in the scope and sophistication of technology mean that traditionally ‘human’ tasks can now be automated. Given this, the application of simple ‘better than’ lists to derive functional allocation are unlikely to be sufficient to constitute good practice. This is because, the delivery of functions is often shared between humans and the technology. Examples include:

* The use of administrative controls to limit the range of crane movement, reinforced by a C&I protection system in the event of a human failure.
* Manually scramming a reactor rather than relying on the reactor protection system to do so.

1. ONR considers BS EN 61839:2014: Nuclear power plants - Design of Control Rooms Functional Analysis and Assignment [9] to form part of Relevant Good Practice in relation to AoF. This presents guidance on the process to be applied in determining AoF and as such provides a useful guide to inspectors when evaluating the dutyholder’s AoF processes. Caution is required however in applying this guidance, as, depending on several factors, which are discussed in detail throughout this TAG, a simplified, or more sophisticated approach, may be required to provide sufficient evidence to demonstrate that an ALARP AoF solution has been selected and implemented.
2. This BS standard also focusses purely on nuclear safety and therefore does not consider possible conflicts between, for example, safety and security. e.g., there needs to be a consideration of the balance of risk between the benefits of automating a function from an operational and safety perspective, and the potential to undermine that function by someone with malicious intent, either by physical sabotage or cyber-attack means.
3. The scope, level, and complexity of automation available to designers is increasing, supported by advances in C&I technology. Examples include analysis and diagnosis of off-normal conditions, situation assessment and response planning. Human factors aspects of such applications are considered in more detail in the Human Machine Interface and Procedures and Administrative Controls Technical assessment guides; NS-TAST-GD-059 [10] and NS-TAST-GD-060 [11] respectively.

## Procedures and Process

1. The dutyholder’s arrangements should provide for explicit, proportionate consideration and substantiation of AoF decisions.
2. Inspectors are advised to consider a dutyholder’s arrangements against the expectations set out in BS EN 61839:2014 [9]. This provides an appropriate process for derivation of AoF although dutyholders may choose to adopt alternative approaches, where they can be demonstrated to be suitable and sufficient.
3. One example of a suitable process based on that identified in BS EN 61839:2014 is presented diagrammatically in Appendix 1. This illustrates the key stages of the process and how it integrates with the wider nuclear safety and security plan and the design and engineering programme. Inspectors are also advised to consider AoF in line with ONR’s TAGs on Human Factors Integration [12] and guidance on optioneering
4. AoF cannot be performed in isolation of the wider design process and does not solely sit within the domain of Human Factors. It is important that suitable organisational arrangements and management systems are in place to deliver effective AoF. A summary of what constitutes effective arrangements is discussed later in this section.
5. AoF is comprised of four basic steps:

* Identification of operational/process, safety, and security, safeguards, or transport functions
* The development of allocation criteria
* Allocation of identified functions
* Verification and Validation (V&V) of the delivery mechanism for each function.

1. Further guidance on the regulatory expectations for AoF are provided below under the following sections.

* Guidance on the necessary organisational and management factors necessary for the AoF process to function effectively
* Guidance on the identification of functions
* Guidance on the selection of allocation criteria
* Guidance on the process of allocation
* Verification and Validation of the allocation decisio

## Organisational Factors

1. AoF cannot be performed in isolation. To be performed effectively, and to lead to appropriately considered and substantiated allocation decisions, it is necessary to assemble a multi-disciplinary team, which can (where appropriate) include the following disciplines:

* Nuclear systems engineering
* Systems analysis
* Safety Analysis (Including Fault Studies, Probabilistic Safety Analysis and Internal and External Hazards)
* Control and Instrumentation
* Mechanical and Electrical engineering
* Human Factors
* Protective Security
* Cyber Security
* Other function specific specialisms, e.g., chemistry, and criticality control
* Operations (where necessary including representatives from the training and procedure development functions)

1. A dutyholder’s AoF process should be integrated into the general design and ALARP optioneering process. Appropriate management controls (e.g., gated reviews) should be in place to ensure that the adequacy of AoF decision making is fit for purpose at each stage of the programme.
2. Inspectors are advised to confirm that a dutyholder’s AoF process is suitably integrated within relevant stakeholder groups and within relevant design and ALARP optioneering management systems.

## Functional Analysis and Identification

52. Permissioned nuclear activities may be comprised of thousands of discrete functions. These can be split into four main categories:

* Operational/Process
* Safety
* Security
* Safeguards

1. Inspectors are advised to seek confidence that a dutyholder’s AoF approach considers each of these functions proportionally, and recognises any interactions, dependencies, or conflicts between them.
2. Traditionally, the emphasis has been on Safety, but as automation has become more sophisticated, the interactions between each of these functions has the potential to be more complex. An increased focus on security has added to this complexity and has the potential to increase cross functional dependency and conflicts.
3. For new facilities or equipment, without pre-defined or inherited functions, dutyholders should identify the overarching functional goals and systematically de-construct these into subgoals and ultimately functions. This should be broken down to the level necessary to support the allocation of delivery by either humans, technology, or a hybrid solution.
4. The output of this functional analysis should describe the goal / function hierarchy and relationships, e.g., overarching goals at the top, system level functions in the middle, and the detailed control / monitoring functions at the bottom. The process of function decomposition can be typically stopped when:

* The function no longer contains a control function.
* The level of controlling individual parameters or actuators has been reached.

1. It should be possible to align the resulting functional analysis with one of the stages of the model of human interaction [7].

* Information acquisition
* Information analysis
* Decision and action selection
* Action implementation

1. Each function description (or groups thereof) should be appropriately informed by analysis sufficient to characterise the function to a level suitable to inform the allocation decision and derive design requirements.
2. A systematic process for goal / function derivation is proposed in BS EN 61839:2014 [9]. Inspectors are directed to this standard for further detail on process.
3. On current (or evolutionary new facilities), many of the goals and functions will be either, already defined, or inherited from pre-cursor designs. This in isolation does not demonstrate that all goals and functions have been adequately derived and inspectors are guided to confirm that the dutyholder has assured itself that any inherited goal / function description is accurate and complete. Nor does it demonstrate that the AoF is appropriate, although operational experience may be used to partly support such arguments.
4. The scope of the functional analysis should proportionally include the following:

* Normal operational/process functions, e.g., plant start-up / shutdown, normal process evolutions and examination, maintenance, inspection, and testing activities.
* All design basis events and faults described within the fault and safety analysis.
* All beyond design basis accidents described within the fault and safety analysis.
* Security functions and events described within the security plan.
* Safeguard functions.
* All plant locations – the process should not solely be limited to the main and secondary control locations.
* Through life feasibility, e.g., maintenance, repair, obsolescence, training, and procedures.

1. Inspectors are guided to focus their assessment on where the greatest safety, security, safeguards, and programme risks lie. For example.

* Functions that present the highest risk contribution.
* Where the design foreclosure risk is highest.
* Where the programme risk is highest, as would be the case for time critical implementations as part of hazard remediation on aging facilities.
* Functions that are performed frequently.
* Functions that, if automated, place the greatest challenges on the technology.
* Functions that, if delivered manually, place the highest cognitive and / or physical demands on the operator.

1. Inspectors are advised to confirm the adequacy of this scope, through reference to the safety and security analysis and design documentation (e.g., Fault and Protection Schedules, System Design Documentation, Safeguards Assessments, and Security Analysis).

## Development of the Allocation Criteria

64. The efficacy of an AoF process is determined by the criteria used to determine the allocation. Prior to starting an AoF process, the dutyholder should have established a suitable set of criteria that adequately capture the factors that contribute to reliable function delivery. The development of criteria prior to the allocation process is important to avoid retrospective bias.

65. These criteria should aim to take account of the nuanced and often dependent interactions between function types (operational/process, safety, safeguards, and security) and between the human and technology.

66. The criteria and the underpinning process should be sufficiently sophisticated to de-conflict any competing demands/constraints between the various functional requirements.

67. For example, an automated access control system may function to protect a vital area. In the event of a significant fault, time-critical access may be necessary to this area to manually deliver a nuclear safety function. Both these examples, assessed in isolation, would likely fail to identify the inherent conflict between the two competing functions.

68. Inspectors are guided to confirm that inter-function dependencies and conflicts will be (are being) appropriately considered and de-conflicted by the dutyholder.

69. Functional evaluation criteria should include, but not be limited to the relevant strengths and weaknesses of humans and technology. Inspectors are advised to challenge AoF processes that use only a limited set of ‘humans are best at’ / ‘technology is best at’ criteria. Where this is the case, inspectors are advised to guide the dutyholder to develop a more sophisticated suite of criteria that proportionally considers the following factors.

* Legal or regulatory requirements and expectations.
* Categorisation and Classification [4] considerations.
* The necessary safety or security classification of the human or technology based on the function category.
* Technology readiness levels (See Approach to Regulating Innovation [13] for further information)
* Dependencies or conflict between operational/process, safety, safeguards, and security functions.
* Strategic factors requiring time critical solutions due to aging and degradation.
* The impact on the operator of a technological allocation, including:
  + Technologically delivered functions generally require commensurate human actions relating to EMIT and fault recovery. These actions may be more challenging than those being delivered by the technology and may increase the consequence of failure or even reduce the wider system reliability.
  + The potential for the reduction of situational awareness during normal operations – where technology is functioning opaquely to the human.
  + The potential for the reduction of situational awareness in the event of a technology failure and/or hazard effects. The human is required to understand at what point in delivering a function did it fail, the potential extent and severity of hazards causing the function to fail, what parts of the system are still functional, what the corrective course of action is, or whether it can be achieved under hazard conditions.
  + The potential to increase risk taking behaviour in the false belief that the technology will intervene in all situations, including the assumption that the technology will be hazard resilient. Similarly, technological solutions can encourage operators to work to its safety limits. An important characteristic of any technological solution is that the operator has a clear understanding of the limits of the technology’s full range capability during normal and fault conditions, and that the technology fails ‘gracefully’ – that is clearly indicates the failure with sufficient time to step in to maintain the function.
  + A reluctance to stop using a technological solution in the event of a fault, for example, failing to switch from a screen-based interface to the supporting hard-wired systems when there is evidence of it presenting bad data.
  + Prolonged vigilance, boredom, and fatigue due to the automation of activities that can otherwise enrich a job.
  + Disproportionate trust in technology. There exists a technology bias, which means operators can disregard contrary indications if they disagree with a trusted system.
  + Assumptions that in the event of a technology failure (when detected) the failure is down to breakdown and unlinked to initiating event/s, which may not be noticeable at the time. For example, under hazard conditions (high local temperature, fires, high humidity etc), it may not be directly obvious what may have caused a failure. Further, the hazard may also put other systems or technology under strain e.g., they do not work as effectively.
  + Changes to roles and job designs with respect to moving from a control to supervisory function.
* The impact to the operator in assigning functions to be manually delivered, including
  + Environmental factors.
  + Cognitive impact – workload, situational awareness, stress, vigilance, response times, reliability, etc.
  + Physical workload, e.g., fatigue, injury, strength, and other anthropometric limitations.
  + Availability of the operators during normal and fault and hazard conditions.
  + Feasibility of complying with operating rules and instructions.

1. The criteria used are likely to be ‘weighted’ differently with respect to their importance to the AoF decision. Inspectors are advised to confirm that the relative importance of the allocation criteria is considered by the dutyholder.
2. The dutyholder should periodically re-visit its AoF processes and assessment criteria to ensure that learning from ongoing research into the relationship between humans and technology is used to inform effective AoF decision making.

## Function Assignment

1. Functional assignment follows once a suitable and comprehensive list of functions has been identified (or re-validated) and a set of appropriate allocation criteria have been established.
2. For new plants, which are evolutionary in nature, and thus may come with an inherited AoF, it is not appropriate to simply assume that these AoF decisions remain valid. dutyholders are expected to proportionately revisit these allocations to demonstrate that risks have been reduced to ALARP.
3. For older plants, where AoF decisions are historical and AoF may be being re-visited as part of a Periodic Safety Review, inspectors should seek proportionate evidence that AoF decisions are appropriately revisited to ensure the AoF determination manages risks to remain ALARP. Inspectors should also seek confidence that the dutyholder’s AoF process has been revalidated to confirm it remains fit for purpose.
4. IAEA TECDOC 688 [2] provides a helpful framework of allocation.

* Functions that must be automated.
* Functions which are better automated.
* Functions which should be given to humans.
* Functions which should be shared.

1. Functions that must be automated are identified via reference to the relevant legal requirements and codes and standards.
2. The remaining functions are assigned based on the allocation criteria derived earlier in the process.
3. There are several models of allocation level that can be helpful in characterising the human or technological solution prior to it being fully developed. Each allocation has benefits and detriments in terms of human and technology implications and limitations.
4. Inspectors are guided to seek confidence that the dutyholder has selected an appropriate framework for its AoF process. Examples are provided below purely for utility and inspector understanding, but others may be equally applicable. Inspectors are advised to ensure that the dutyholder’s chosen framework is proportionate to their application.

* Full local manual control.
* Remote manual control.
* Remote manual technology-mediated control – operator inputs are mediated by the technology, e.g., tele-operations where force or accuracy is amplified or where the technology intervenes to prevent exceeding parameters.
* Manually initiated sequenced automation – operator detects the need to act and initiates an automated sequence and receives confirmation of success.
* Advisory sequenced automation – the technology identifies the need to act and advises the operator of this need. The operator permits or carries out this action.
* Transparent full-automatic control – the technology acts but informs the operator when it starts and when it successfully completes.
* Opaque full-automatic control – the technology operates in the background without the operator being aware of it functioning.

1. The output of the AoF process should be documented along with a summary of why the AoF decision was made and which of the criteria contributed to the decision. The benefits of good record keeping at this stage are important should an allocation need to be revisited later in the project or in the lifespan of the facility.
2. The AoF decision should be integrated, or linked with, any safety, safeguards, and security analysis, and subject to the dutyholders categorisation and classification system. This may affect the AoF decision.
3. Once an allocation has been made, and the method of delivery suitably developed by appropriate disciplines including engineering, safety, safeguards, and security, it should be substantiated via appropriate use of verification and validation methods. The greater the risk importance associated with the function and the complexity of the means of delivery, the greater the evidence required to substantiate that function. For example, the validation of the AoF associated with the design of a new reactor control room, will require the dutyholder to conduct suitable and sufficient Integrated System Validation (ISV) trials. Integrated ISV may also be appropriate for other types of control room, depending on their scope and complexity.
4. Inspectors are advised to:

* Seek confirmation that: the output of the AoF process is suitably integrated with the relevant engineering, safety analysis, safeguards, security, and pre-operational development programmes; that the output of the AoF process has been integrated into the technology design specifications and the design of procedures and operator training needs/competence requirements.
* Confirm that, where functions have been allocated to the human, the dutyholder has specifically considered the impact of multiple functions assigned to individuals in terms of workload and feasibility of timing. The allocation should recognise the whole job impact, the conditions under which the job may be undertaken (e.g., hazards), and not simply focus on individual tasks and responsibilities.
* Confirm that, where functions have been allocated to the human, the dutyholder has taken account within its safety, safeguards, and security analysis of any limitations in availability of operators, the credibility of the task under all conditions, and has allowed for flexibility in performing tasks (or triggers a reiteration of the AoF process where availability / task reliability challenges are identified).
* Confirm that the allocation of functions to humans and technology has resulted in meaningful job roles for operators which support situational awareness and promote engagement and job satisfaction.
* Confirm that the dutyholder has specifically identified and resolved any conflicting functional allocations between the operational/process, safety, safeguards, and security functions and that these instances are suitably documented.
* Confirm that the dutyholder has considered the impact on functional allocations in transitioning between plant states in normal to abnormal operations. Failure to consider this may undermine a functional allocation because what is an appropriate allocation in one plant state, may not be in others.
* Confirm that the dutyholder has captured and suitably documented any supporting tasks necessary for the technology to deliver the function, i.e., EMIT activities, or post fault manual delivery of a function.
* Consider the iterative nature of this process and check that, where necessary, the dutyholder’s process and programme duration allows for an iterative approach. Inadequate programme consideration may increase the design foreclosure risk.
* Confirm that the dutyholder’s AoF process makes effective use of any safety, safeguards, or security analysis. Human actions in system operation and maintenance may have assigned quantified values. The results of the PSA can indicate where performance requirements of a function exceed the capabilities of humans and automation and what can reasonably be claimed in relation to their performance. This reduces the need to revisit the original functional allocation.
* Confirm that 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 [14] 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 the substantiation of reliability claims.
* Confirm that the dutyholder’s allocation of safety function decisions are compatible with the principle of hierarchy of control as set out in SAP EKP.5.
* Confirm that the dutyholder has provided an adequate audit trail of the decision-making process, explicitly outlining and justifying the rationale for trade-offs between requirements in the ALARP process.
* Confirm that 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.
* Confirm that 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.

1. Inspectors should consider whether an adequate and proportionate AoF justification has been provided for:

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

## Verification and Validation of AoF

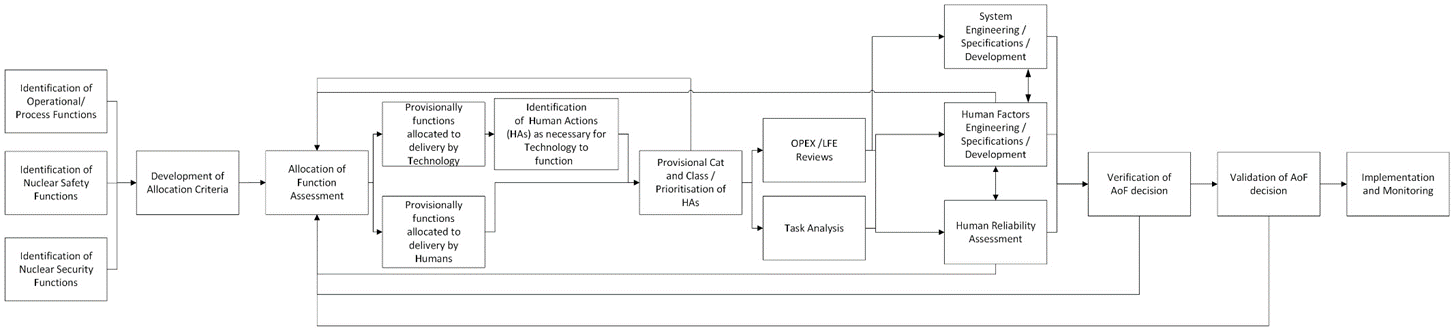
1. Once allocated, and the chosen means of function delivery developed to a degree of maturity (outside the scope of this TAG) to facilitate testing, the means of delivering the function needs to be verified and validated. This is to demonstrate that the AoF is effective in the context of the design philosophy and safety case claims and assumptions.
2. This process of V&V is not one that is unique to AoF and thus beyond the scope of this TAG. However, in the interest of utility, a summary of V&V in the context of AoF and Human Factors is outlined below.
3. There are two key types of Verification, Task Verification and Design Verification:

* Task Verification: The dutyholder has verified that the Technology or Task design is supported by the necessary features, e.g., instrumentation, controls, alarms, procedures, training.
* Design Verification: The dutyholder has verified that the technology or task design meets relevant good practice in relation to the relevant codes and standards.

1. Validation comprises a staged, or graded, approach to evidence gathering via performance testing of the technology or operators. Its aim is to demonstrate acceptable safety and operability against defined targets. This process may culminate in, for example, Integrated System Validation (ISV) Trials. ISV trials provide the final demonstration that system (technology, people, training, and procedures) reliability meets its targets. In the context of AoF, it provides evidence to substantiate that the AoF decisions are sound.
2. Beyond the expectations of a typical V&V process inspectors are advised to seek confidence that the dutyholder has:

* Sought operational experience and learning as appropriate for a particular allocation choice. Where necessary, and where the technologies being deployed are new or novel, this may require learning from outside of the nuclear sector.
* Actively identified functional conflicts between process, safety, safeguards, and security and suitably mitigated or deconflicted them.
* Avoided allocation bias and given due consideration to the principle of ALARP. Factors to consider include:
  + Allocation bias driven by convention from other high-hazard sectors.
  + Allocation bias driven by what is technologically possible, or a feature of a commercial system.
  + Allocation bias driven by the need to minimise through life costs. (e.g., bias towards the cheapest option rather than the ALARP option)
  + Allocation bias driven by implementation difficulty (for example, the difficulty in developing safety cases for software-based systems).
  + Allocation bias on the basis that the technology is not capable of reliably delivering a function, so it therefore must be achievable by an operator.
* Provided a demonstration that the allocation of function takes proportionate account of all factors that influence effective and reliable *system* performance. Inspectors should apply scrutiny to decisions which allocate functions to the operator which require:
  + Rapid or 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 [15]).
  + Reliance upon recovery in short timescales (see NS-TAST-GD-010 [16]).
  + Completion in hostile environments.
* Where the function is delivered by technology, its delivery should be designed in such a way that it adheres to the following (e.g.) risk reduction principles [7].
  + Automation systems should be comprehensible and explainable .
  + Automation should ensure operators are not removed from the command role where practicable to do so.
  + Automation should not negatively effect situation awareness.
  + Automation should not perform (i.e., the operator is totally unaware of the existence of the automation), or fail, silently.
  + Designers must assume that operators will become reliant on reliable automation.
  + Automation should be designed to fail ‘gracefully’ where practicable, such that in the event of failure, there is sufficient time for an operator to respond to the failure.

90 Once implemented, dutyholders should, where appropriate, monitor the effectiveness of the AoF decision to ensure that it meets the necessary performance criteria. The artificiality of V&V processes can mean that it is only in applied settings that some issues are revealed. Inspectors are advised to confirm that suitable monitoring is present or planned.



# Appendix 1 – AoF process

# References

|  |
| --- |
| ONR, “Safety Assessment Principles (SAPs) (2019/367414)”. |
| IAEA, “TECDOC 668 - The role of automation and humans in nuclear power plants”. |
| WENRA, “WENRA Safety Reference Levels for Existing Reactors (Revision 2020),” [Online]. Available: https://www.wenra.eu/node/86. |
| ONR, “NS-TAST-GD-094 Categorisation of Safety Functions and Classification of Structures and Components,” ONR. |
| ONR, “CNSS-TAST-GD-11.1 Issue 1.2 GUIDANCE ON THE SECURITY ASSESSMENT OF GENERIC NEW NUCLEAR,” ONR. |
| Legislation, “The Nuclear Industries Security Regulations,” 2003. |
| C. E. Billings, Aviation automation: The search for a human-centered approach., Mahwah, N.J: Lawrence Erlbaum Associates Publishers, 1997. |
| ONR, “NS-TAST-GD-005 Revision 11 Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)”. |
| B. S. Institute, “BS EN 61839:2014: Nuclear power plants design of control rooms functional analysis and assignment.,” 2014. |
| ONR, “NS-TAST-GD-059 - Human Machine Interface (2020/265758)”. |
| ONR, “NS-TAST-GD-060 - Procedure Design and Administrative Controls (2020/265773)”. |
| ONR, NS-TAST-GD-058 Human Factors Integration, ONR. |
| ONR, “Approach to Regulating Innovation https://www.onr.org.uk/documents/2020/onr-innovation-report-2020.pdf,” 2020. |
| IEC, “IEC61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems”. |
| ONR, “NS-TAST-GD-063 - Human Reliability Analysis (2020/265784)”. |
| ONR, “NS-TAST-GD-010 - Early Initiation of Safety Systems (2020/265704),” [Online]. |