SKI Report 99:10

Verification and Validation of Human Factors Issues in Control Room Design and Upgrades

Mark Green
Steve Collier

December 1999

ISSN 1104–1374
ISRN SKI-R-99/10-SE

SKI

SKI Report 99:10

Verification and Validation of Human Factors Issues in Control Room Design and Upgrades

Mark Green
Steve Collier

Institutt for energiteknikk
OECD Halden Reaktor Project
N-1751 Halden
Norway

December 1999

SKI Project Number 96193

Summary

Systems, facilities and equipment are periodically updated during a power plant's lifetime. This has human factors implications, especially if the central control room is involved. Human factors work may therefore be required. There is an extensive literature on human factors itself, but not so much on how it is verified and validated. Therefore, HRP and the Swedish Nuclear Power Inspectorate (SKI) commissioned a study. The objective was to review the literature and establish a knowledge base on verification and validation (V&V) of human factors issues. The report first discusses verification and validation as applied to human factors work. It describes a design process and the typical human factors topics involved. It then presents a generic method for V&V of human factors. This is built on a review of standards, guidelines and other references given in an annotated bibliography. The method is illustrated by application to some human factors topics.

Sammanfattning

System, utrustning och komponenter förnyas återkommande under en anläggnings livstid. Sådana förändringar är av betydelse med avseende på samspelet människa, teknik och organisation, särskilt om de berör det centrala kontrollrummet. Det behövs därför arbetsinsatser inom ergonomiområdet. Det finns omfattande litteratur om ergonomi, men inte så mycket om hur arbetsinsatserna verifieras och valideras. Halden Reactor Project fick därför i uppdrag av Statens Kärnkraftinspektion (SKI) att göra en studie. Syftet var att göra en genomgång av befintlig litteratur och etablera en kunskapsbas om Verifiering och Validering (V&V) ur ergonomisk synpunkt. Rapporten innehåller en diskussion om V&V och en beskrivning av design processen med typiska ergonomiska frågeställningar. En generisk metod för V&V ur ergonomiskt perspektiv presenteras. Metoden bygger på standarder, vägledningar och andra källor i en kommenterad bibliografi. För att visa hur metoden kan användas tillämpas den på några ergonomiska aspekter.

Contents

1 Introduction

This report collates and presents issues relevant to verification and validation (V&V) supplemented by notes on good practice. The contents are based on accessible standards, guidelines and other sources.
A generic process for review of V&V is developed and presented. This is applied to several human factors topics to illustrate how the suggested generic process could be used for specific human factors topics. The set of topics we have used should be understood as illustrative, rather than as a definitive list of subjects.
Statements, opinions, advice and coverage in this report represent the views of its authors.

1.1 Users

The main users and readers of this report are assumed:

To be familiar with general nuclear power terms, functions and operations.

To have access to the set of references upon which the report has been developed.

To have received some training in the concepts underpinning the report and in the use of the report.

1.2 Structure

Sections 2, 3 and 4 establish the terms and definitions for the work and characterise verification, validation and typical project structures. Section 5 then describes a generic process for V&V. The generic process focuses on control room upgrades, though it could be applied to any project that has human factors implications. These are the main sections of the report.
Section 6 following the generic V&V process describes some human factors topics that we believe any project is likely to address and then applies the generic V&V process to each of these human factors topics. These are illustrative examples of how to apply the generic V&V process to selected topics. Where there are issues specific to a topic, these are explained. Appendix A gives an annotated bibliography of the references reviewed for the report.

2 Context and Definitions

This section establishes a common set of terms, definitions and concepts for users of the report. It contains a discussion of the different uses of the terms 'verification' and 'validation' in the professional fields most likely to be met. It goes on to discuss human factors aspects of V&V and presents the definitions for both terms used by the report. Any other terms associated with the process of V&V are discussed and defined here.

2.1 Context

Understanding the context for this report requires an appreciation of:

The design process.

The V&V programme.

These are shown in Figure 1 and outlined in the subsequent sections.

2.1.1 The Design Process

The design and development process will vary considerably in detail between different projects. A process is therefore described which we believe is broadly typical of the stages undertaken when designing a new control room or modifying an existing one. Some description of this process is required, as it is necessary to make assumptions concerning to what the utility's V&V programme is applied.
The human factors topics typically addressed by a project are described in section 6 and in many of the references in Appendix A. Several references in Appendix A contain descriptions of both design processes and the human factors topics associated with them. The process for checking these aspects is a separate and independent process from V&V.

2.1.2 The Human Factors V&V Programme

As well as the design process itself, this report also needs to consider the way in which human factors aspects might typically be verified and validated. Such a consideration should include:

- A description of a typical V&V process including the scope for the consideration of V&V issues beyond the design process and into the facilities operational life.
- The elements found in such a process.
- The human factors aspects that could be addressed in a V&V plan.
- A description of current 'good practice' for these aspects.

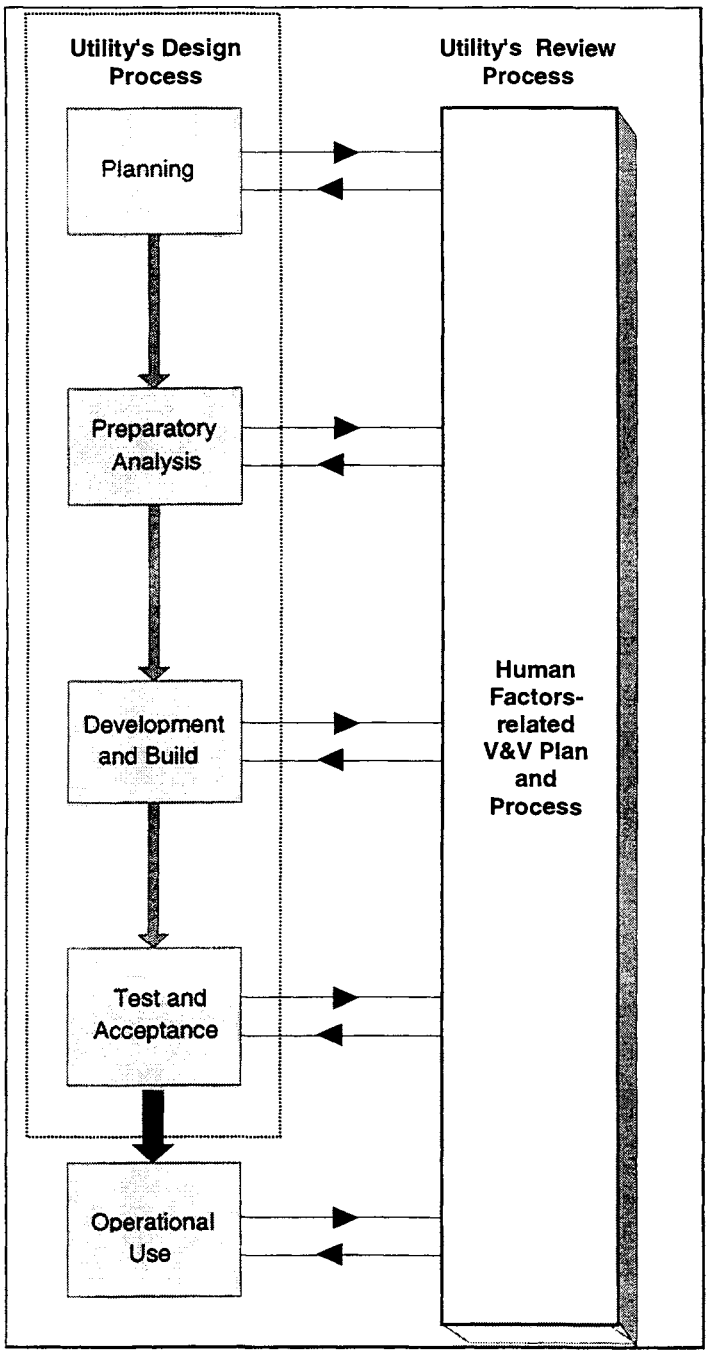

Figure 1. Main Processes Considered in the Current Work

2.2 Definitions

Numerous but sometimes conflicting definitions can be found for these terms across different fields, for instance, human factors, software engineering. Though the focus of this work is human factors, it is important to appreciate that differences exist between the term 'V&V' as used in software engineering, quality management, and human factors. Dictionary definitions of the terms vary but typical examples are:

Verify: to establish truth or correctness by examination or demonstration.

Valid: sound, defensible, executed with proper formality. *(Pocket Oxford Dictionary 1984)*

The verb to 'verify' means to show that something has been designed or constructed according to its specification. The word 'valid' means that the object that has been built is able to carry out the task for which it was intended. The suffixes '-ation' and '-ication' refer to processes or acts. 'Validation' must then refer to the process or act of showing that something is valid, and similarly for verification.
In the present context, then, we want 'verification and validation' to be understood as a process. The V&V process includes, for example, a documented specification, collection of data, analysis of existing and future systems, a comparison process, and documentation and resolution of differences.
The terms V&V possibly have different meanings within software engineering. For example EWICS-TC7 (1989)[1] define the terms as:

Verification: The comparison at each stage of a system's life cycle to determine that there is a faithful translation of one stage into the next.

Validation: The process of determining the level of conformance between an operational system and the systems requirement, under operational conditions. (EWICS-TC7, 1989)

These definitions, whilst they may be accepted and understood within software engineering, are the source of some confusion when brought outside this discipline and for this reason will not be considered further here, although they are close to our own use of the terms.
Quality management also has accepted processes and systems related to V&V. For example ISO 8402[2] defines V&V as:

Verification: Confirmation by examination and provision of objective evidence that specified requirements have been fulfilled.

Note 1. In design and development, verification concerns the process of examining the result of a given activity to determine conformity with the stated requirement of that activity.

Validation: Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled.

Note 1. In design and development, validation concerns the process of examining a product to determine conformity with user needs. (ISO 8402).

---

[1] EWICS-TC7 Guidelines published in 'Dependability of critical computer systems', Vol 2.Editor F. Redmil, Elsevier 1989. Cited in Dahll, G., and Kvalem, J.(1994) Guidelines for Reviewing Software in Safety Related Systems. Report prepared for Swedish Nuclear Power Inspectorate by Institutt for Energiteknikk, Halden, February 1994.

[2] Draft International Standard ISO/DIS 8402, ISO/TC 176/ SC1 (1991) Quality Management and Quality Assurance - Vocabulary. In ISO 9000 Compendium 3rd Edition (1993) International Organisation for Standardisation, Geneva, Switzerland.

The same standard also defines a process for the quality audits as:

> Systematic and independent examination to determine whether quality activities and related results comply with planned arrangements and whether these arrangements are implemented effectively and are suitable to achieve objectives. (ISO 8402).

It is also interesting that in psychology the 'validation' of a measurement means the establishment that it measures what it intended to measure. The parallel definition in the human factors of design would be 'Does the artefact, system, object, etc., actually do what it is intended to do?' This view of validation and verification is illustrated in Figure 2.

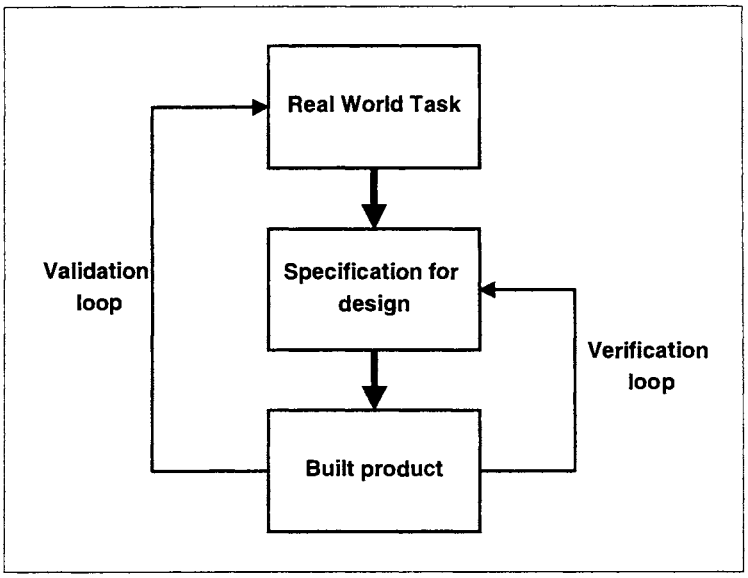

Figure 2. The Role of Verification and Validation

There are several more definitions of verification and validation in standards dealing with human factors issues. For example:

- Verification:

> The process of determining whether instrumentation, controls, and other equipment meet the specific requirements of the tasks performed by operators (from NUREG-0700 Rev. 1)

> The process of determining whether individual components meet the specified requirements. In this context, verification is a series of analytical checks of instrumentation, controls, displays, and other equipment against specific human factors criteria, engineering criteria and operating and functional goals. (IEC 964)

- Validation:

> (1) The process of determining whether the design of machine elements and the organisational design of human elements of a human-machine system is adequate to support effective integrated performance of established functions. (2) The capability of a system to check information entry items for correct content of format as defined by software logic. (NUREG-0700, Rev. 1)

> Validation, which should be carried out after completing the verification, is generally defined as the test and evaluation to determine that a problem solution complies with the functional, performance and interface requirements. More specifically, it is the process of determining whether the physical and organisational design for operations is adequate to support effective integrated performance of the functions of the control room operation staff. (IEC 964)

These definitions of verification and validation suggest that it is likely or natural that greater emphasis will be placed in the verification aspects earlier in the design process, and that later validation will dominate. This is illustrated in Figure 3.

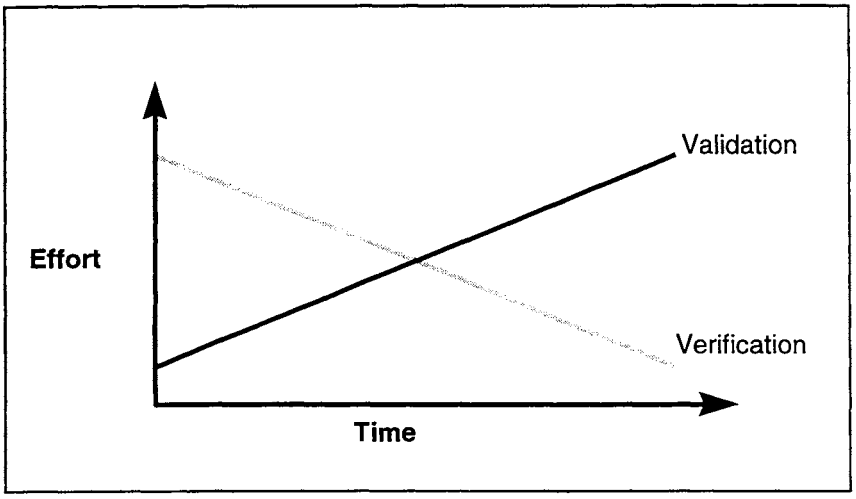

Figure 3. Relation between Effort and Time for Verification and Validation

However, validity or validation is at least as important as verification and should, as far as possible, be carried out early in the design process. Typical validation faults (adapted from Nielsen, 1993) could be:

- Design for the wrong users (or not all users).
- Design for the wrong tasks (or not all the tasks).
- Failure to include time constraints.
- Failure to include situational influences.

2.2.1 Definition of Verification

For the purposes of this report, we propose to use the definition of verification taken from the IEC standard 964. Verification is therefore defined as:

> The process of determining whether individual components meet the specified requirements. In this context, verification implies a series of analytical checks of instrumentation, controls, displays, and other equipment against specific human factors and engineering criteria and operating and functional goals. (IEC 964)

2.2.2 Definition of Validation

For the purposes of this report, we use the definition of validation taken from the IEC standard 964:

Validation, which should be carried out after completing the verification, is generally defined as the test and evaluation to determine that a problem solution complies with the functional, performance and interface requirements. More specifically, it is the process of determining whether the physical and organisational design for operations is adequate to support effective integrated performance of the functions of the control room operation staff. (IEC 964)

3 Characterisation of the Design Process

This section contains further discussion of a typical design process. This was previously outlined in section 2.1.1. It does not seek to define or stipulate one correct process but to present a summary of the typical high-level stages that such a process is likely to entail. There is also a brief description of the role and timing of human factors in the design process. Next, we discuss the design process and V&V work when the project is an evolutionary change or control room upgrade. A number of standards and references contained in Appendix A give systematic and comprehensive design processes. Finally, we discuss the changing nature of control room upgrades and the effect that this could have on human performance, and consequently on the kind of verification and validation that might be needed.

3.1 The Design Process

The design process has been characterised as comprising four principal sections: planning, preparatory analysis, development and build, and testing and acceptance. The adoption and demonstration of a comprehensive systematic design process is vital for the design result.
For smaller upgrades to existing systems, it may not be necessary to consider all aspects of the process in equal detail. However, the approach adopted should be sufficient to meet the requirements of the upgrade. See section 3.3 for a fuller discussion of this aspect.

3.1.1 Planning

In this stage the objectives for the system to be designed are defined and documented. In addition, the performance specifications are documented. Some of the tasks that may typically be undertaken at this stage are:

- Selection of the processes of designing the system.
- Outlining of the concept of the new system.
- Statement of the purposes of the new system as objectives.
- Definition of system and user requirements.
- If applicable, focus on the changes from an old system to the proposed new system.

3.1.2 Preparatory Analysis

This stage can be characterised as one in which the initial information gathering and analysis are performed for the design. Some of the tasks that may be undertaken at this stage are:

- Examination of concepts of the proposed system, i.e., feasibility.
- Definition of the functions that the system has to perform to meet its objectives and the performance specifications.
- Description of the major functions.

- Allocation of the functions to human and machine.

3.1.3 Development and Build

This stage is concerned with the development of detailed design specifications for the interface and the consideration of the interaction of the design with other elements of the system, i.e. training, documentation, etc. Typical tasks at this stage are:

- Documentation of detailed specifications.
- Building of prototypes.
- Refinement of design.

3.1.4 Testing and Acceptance

This stage is concerned with the final test and evaluation of the design to ensure that it is verified and validated. Typical tasks at this stage are:

- Final Verification — does the customer accept that the system has been designed, built, installed, etc. according to the agreed specification?
- Final Validation — is the system acceptable and suitable for the users?
- Human factors customer acceptance tests.
- Identification, recording and rectification of discrepancies. Any necessary changes are fed back to the development and build stage.
- Commissioning.

3.2 When to Apply Human Factors in a Design Process

In each of the design stages described above, several human factors topics can be identified that should be undertaken along with the engineering design, development and build work. Figure 4 identifies a typical set of these topics and relates them to the stages of the design process. As in Figure 1, verification and validation are shown as applying at all stages of a project, not only at the test and acceptance stage. Some V&V work on all human factors topics should be considered at all stages of the project. A fuller consideration of human factors topics and the application of a generic verification and validation process to these topics (or groupings of them) is the focus of section 6. It is important that these human factors issues are not considered as optional or supplementary, but rather as an integral and necessary part of the design process. Although the exact process of V&V will vary dependent on the scope and nature of the modification to be made, the principle remains the same.

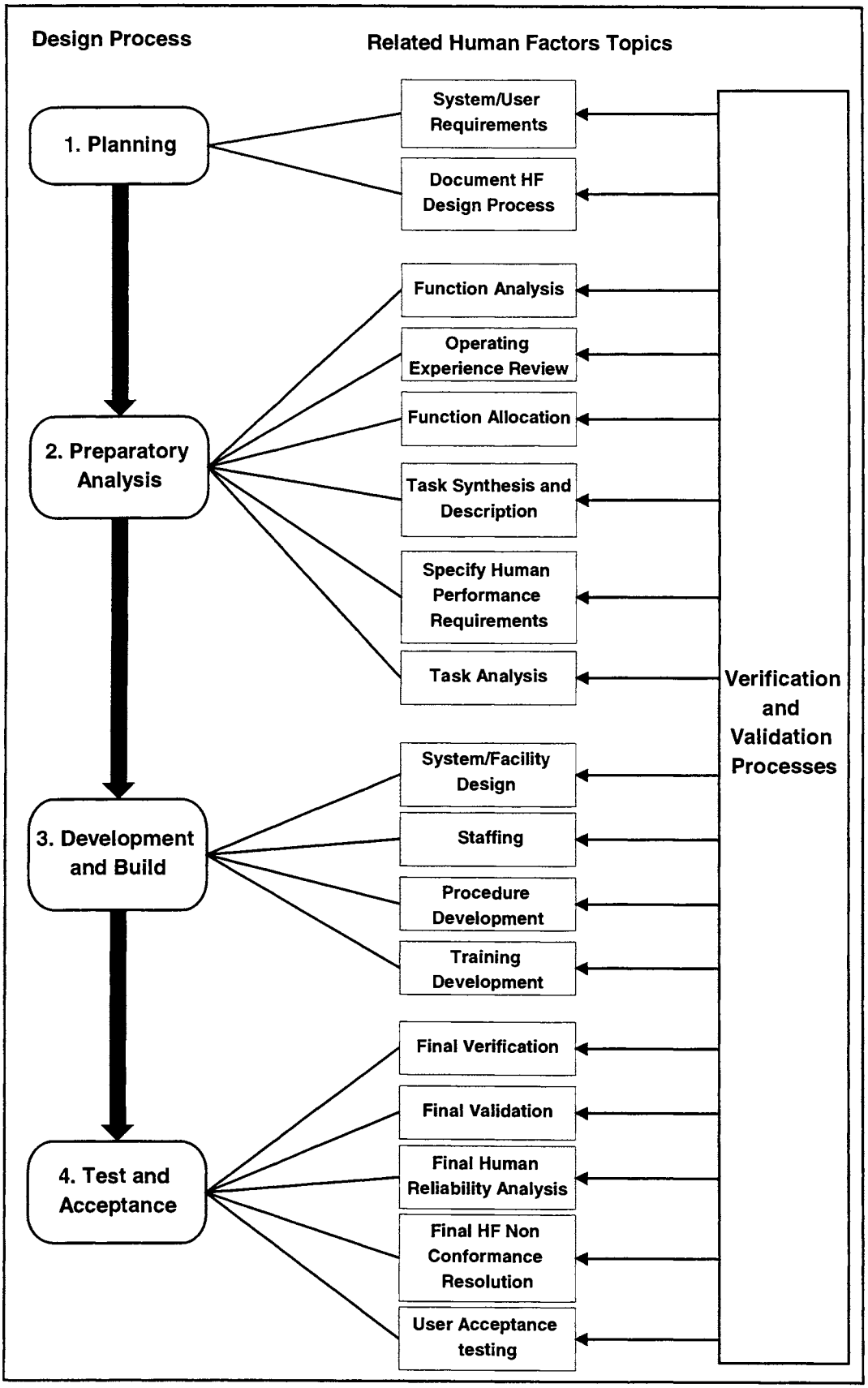

Figure 4. Principal Design Stages and their Associated Human Factors Topics

3.3 Upgrading Existing Facilities

A control system is a changing system. Due to operational experiences, regulatory demands, new technology and other factors, the system will undergo minor as well as substantial changes (International Atomic Energy Agency, 1995). The human factors V&V requirements for a smaller evolutionary change will be considerably different from those for a new advanced control room. Such evolutionary changes can result from a variety of sources including regulatory requirements, ageing of existing systems, introduction of new technology, insights gained from operating experience, etc. The literature gives little concrete guidance on how the V&V requirements for these sorts of changes should be determined.

For a new control room, the full range of V&V issues and requirements discussed in this report and the standards it references are applicable. However, for smaller evolutionary changes, V&V issues and requirements will differ and it is the extent and nature of the modification itself that will determine them. Typical control room evolutionary projects include the replacement or upgrade of process monitoring systems, re-organisation of hard-wired panel and desks, etc.

Evolutionary changes are acknowledged in the literature as an area where the V&V process is both important and needs to be tailored to individual projects. However, very little practical guidance is available. Must a comprehensive human factors and V&V programme be carried out for every upgrade, no matter how small? One possibility is that previous V&V work can be reused under certain conditions.

The use of existing data in the V&V of these changes can be based on arguments related to their degree of innovation and qualification by similarity. These arguments can justify the use of existing data and help to reduce the amount of V&V work. The new V&V efforts are focused on areas of change and their integration with the existing system. The V&V process itself must still have an acceptable framework supported by appropriate documentation. Final determination of what form of V&V is acceptable for evolutionary changes must be decided in each particular case.

3.3.1 Use of Existing V&V Information

For evolutionary changes, information often exists already, such as analyses from previous design documents, procedures, and operation experience. Together these can constitute an important pre-validated data set. This data set can be used to meet some of the requirements of the V&V process, although issues such as the degree of change and the quality of existing material must obviously also be taken into account. Consequently, IEC 1771 (1995a) notes that the V&V activities need to be tailored to the particular needs and circumstances of individual projects. The basic framework for carrying out a V&V (given in section 5) is, however, constant; that is, the stages of preparation, evaluation, and resolution are retained. The additional work that does or does not take place under these headings must be justified and documented.

The IEC 1771 standard draws attention to two important aspects when deciding the V&V requirements for projects of this nature. These are the 'degree of innovation' and the possibility of 'qualification by similarity'. The *degree of innovation* relates to those areas of innovation in the change and concentrates V&V activities on them. The degree of innovation varies along a continuum from a replica of an existing design, which

would require very little V&V, to an evolutionary design requiring selected V&V activities, to an advanced design required the full scope of V&V activities. For evolutionary changes, V&V activities can be concentrated on the areas of change and their integration with existing, proven, features of the design. (IEC 1771, 1995a)

Qualification by similarity relates to the extent to which a new design or modification contains features, including V&V, that are already proven. IEC 1771 (1995a, p. 53) suggests that qualification by similarity is applicable if it can be shown that "the differences between the old and the new systems or equipment do not affect performance or that performance is superior" (IEC, 1995a, p. 53). As a note of caution, it adds that:

> ...**more** than accident free operation of an existing system is required for a successful qualification by similarity argument. A review of system operation should be conducted that shows the absence of significant operational problems. (IEC 1771, 1995a, p. 53)

Besides this, the potential to affect or influence risk levels should be considered. Existing safety analyses can help to address this issue.

3.3.2 New V&V Information

In an upgrade, there is a need to verify and validate new and innovative aspects, including their interaction with the existing plant. IAEA-TECDOC-812 (1995) identifies a number of issues relevant to the V&V process for evolutionary changes, including:

- Appreciation of current and previous change programmes and their motives and philosophies.
- Appreciation of the possible effects of the change on other aspects of work and organisational factors.
- The effect of the changes on training requirements, simulators, procedures and other relevant aspects.
- The way changes will be introduced and whether parallel use of old and new system is desirable for V&V.
- The implementation of modifications in the plant simulator where appropriate V&V can take place.

Glenn and Niehoff (1985) provide a useful and practical description of how evolutionary changes to the control room were dealt with at Fort St. Vrain NPP in the USA.

3.4 The Changing Nature of Power Plant Design and Control Room Tasks

Changes in control systems and control room equipment can affect the role of operators and their tasks both during normal functioning and during emergencies. There are, for example, changes in the interface, tasks and functions allocated to the operator, including (NUREG-0711, p. 1-2):

- Greater use of automation.
- A shift of the operator's role from active involvement to monitoring, supervision, and backup of automated systems.
- Greater centralisation of controls and displays, both on a station basis and within the control room.
- Use of large displays in the control room that allow a shared space for viewing high-level or summary information and critical parameters.
- A shift of the operator's primary interface from direct interaction with components to interaction with a data-based system.
- Greater use of integrated displays and graphical displays.
- Greater use of information-processing aids and decision-support aids.

If the operator's role has changed in this way, it will be more difficult to apply the arguments given in the previous section: to argue for qualification by similarity or to claim that the degree of innovation is small.

These technologies and trends affect the design and equipment in both new facilities and existing control rooms. Therefore, there is a range of technologies and approaches to the man-machine interface at any one location, and a range of degrees of upgrading. These changes mean that any human factors programme, and V&V of it, must allow for a diversity of approaches to control and display, and must be particularly sensitive to new problems created.

New problems can arise because there is a potential to affect human performance, to create new types of human error and to reduce human reliability in new ways. Because these new effects on human performance tend to be of a different kind from those found in conventional control rooms, they are at first less obvious and less likely to be understood, or even recognised. The human factors programme must address these issues and resolve them in some way. Some of these new threats to human reliability are briefly discussed in NUREG-0711:

- Lack of Knowledge — Cognitive issues are emerging as more significant than the physical ergonomic considerations of control room design that have heretofore dominated the design of conventional interfaces, and indeed human factors as a subject.
- Changes in Function Allocation — Increases in automation have tended to result in a shift from physical workload to cognitive workload. As a result, there are dangers such as loss of vigilance, loss of situation awareness, and

eventually, loss of a full understanding of the processes as the operator is taken more and more 'out of the loop'.

- Changes in Cognitive Implications of Designs — Systems have changed in several ways. Information tends to be more pre-digested, information is resident on a workstation or computer system rather than physically located in a room, there is a greater quantity of information, and there is an additional burden of operating the interface equipment. These lead to a greater need to specify system requirements in cognitive rather than physical terms. This requires new techniques, such as cognitive task analysis, which are relatively undeveloped in human factors as a subject.

- Changes in Skill Demands — Although systems are increasingly automated, they also create new, usually highly skilled tasks for operators. Operators must understand and evaluate the performance of automatic systems, or even take over from them when they fail. It is difficult to see how this level of skill can reasonably be expected of operators, when the same automation has made their daily tasks more boring and monotonous.

These points make clear that the changing nature and equipment in control rooms itself changes the roles, functions and tasks of the control room and the staff within it. This in turn puts requirements on the kind of human factors work that is needed..
As a response to these problems, many bodies have begun to look more seriously at the implications of advanced control room systems. It is often difficult to set pass/fail criteria or to prescribe methods in advance for some of these new problems. There has consequently been an increased emphasis that utilities should give evidence of a design *process* and a V&V process that can stand up to scrutiny and create confidence that a design is satisfactory.

3.5 Sources of Confidence in a Design

When it comes to human factors, it is thought important (for instance, NUREG-0711, 1994) that:

- The design follows accepted human factors principles.
- The design supports the performance of the operators.
- The design supports the reliability of operators.

V&V of the human factors aspects of a design is just one source of confidence that a design is satisfactory. There are several sources of evidence for the efficacy of the human factors design (NUREG/CR-5908 Vol. 1, 1994, NUREG/CR-6393, 1996) as shown in Table 1.
Further confidence in a design can be gained by a detailed test programme of the actual plant and through successful operation of it. The record of operation can also be a source of validation early in the design process for the next similar design or upgrade (NUREG/CR-5908 Vol. 1,1994).

Table 1. Types of Information for Assessment of HFE Adequacy

Type of evidence	Minimal evidence	Best evidence
Planning of human factors activities	An HFE design team, a programme plan and methods for doing the work	A qualified HFE design team with all the skills and resources required, using an acceptable HFE programme plan
Design analysis work	function analysis, task analysis, assessments of alternative technologies	Results of appropriate HFE studies, analyses that provide accurate and complete inputs to the design process and V&V assessment criteria
Record of the design	Specifications and descriptions of designs	Designed using proven technology based on human performance and task requirements incorporating accepted HFE standards and guidelines
Verification and validation of the project	Compliance with HFE guidelines and project specifications, operation of the integrated system under actual or simulated conditions	Evaluated with a thorough V&V test programme throughout the project

4 Characterisation of the Verification and Validation Process

This section contains a more detailed discussion of the V&V process outlined in section 2.1.2, namely, a description relating the process of human factors V&V to the design process described in section 1. It documents:

- The overall purpose of V&V and at different stages in the design process.
- The advantages arising from V&V.
- The information requirements and the use of results from the V&V process.
- Their implication for other stages in the design.

Again, the section does not prescribe one exclusively correct process; it describes a typical role for V&V in the design process.

4.1 Background

The process of human factors V&V has three separate dimensions: the human factors aspect in the design process that the V&V covers, the process of V&V itself, and the detail in which a particular aspect is investigated, see Figure 5.

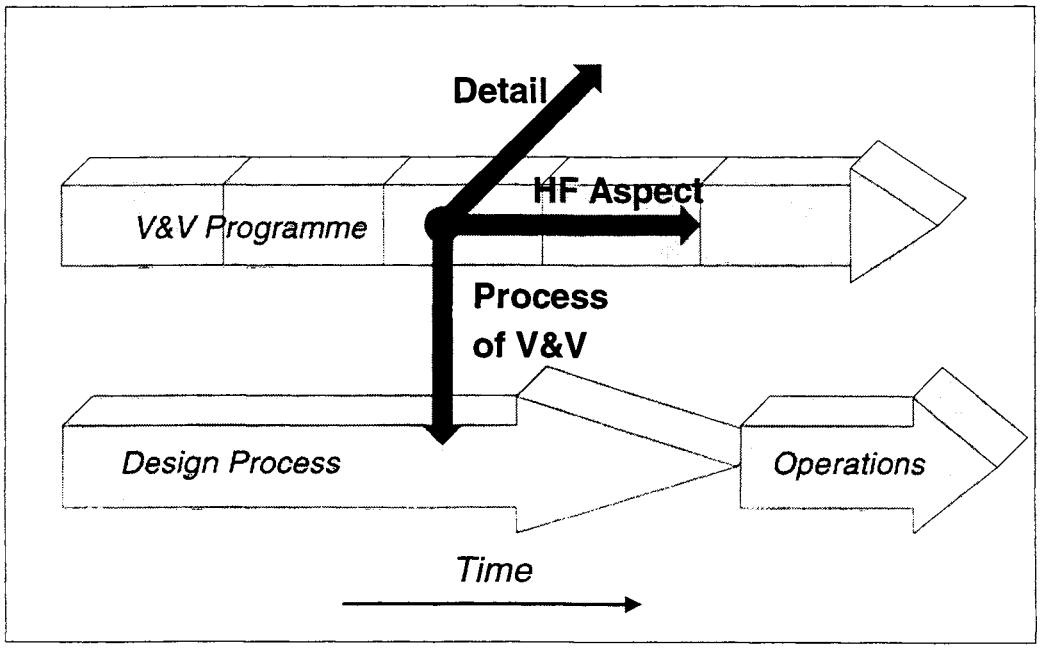

Figure 5. The Main Dimensions for V&V

The 'human factors aspect' dimension refers to those human factors aspects of the design to which V&V is applied. The 'process' dimension refers to the generic process applied to carry out V&V requirements and is independent of either the human factors aspect or the level of detail considered. The 'detail' dimension is the degree of detail for the V&V process applied. Both a small and a large modification may involve similar human factors aspects and the process of carrying out V&V will be similar, but the level

of detail for each aspect will not be necessarily as comprehensive for the small evolutionary change as for a larger upgrade.

There are several basic questions, related to the above dimensions, that help to clarify the purpose and process of V&V:

- Why should V&V be carried out?
- What is the process of V&V?
- How should that process be carried out?
- Who should apply the process?
- When should the process be applied?

The reasons for carrying out V&V are to:

1) detect design errors and to

2) provide evidence that
   - the system can be operated safely and
   - that operators can perform the necessary functions efficiently and effectively using the design provided.

Implicit here is the requirement for measurements of performance and for criteria to test the design against. For our purposes, we consider only human factors aspects, although technical and engineering aspects are also important.

What then is the V&V process and how is it applied? We consider it a series of tests, checks, and evaluations related to a particular human factors aspect of the design. We have adopted a generic framework based on that detailed in IEC 1771, that is, a three-stage process involving, preparation, evaluation and resolution. The main stages of the framework are independent of both the time they are used and the human factors topic they are applied to. Of course, the actual contents will vary but the framework itself will be constant. Consideration of who should carry out the V&V is discussed in section 5. It can be summarised as a team of personnel who are suitability qualified, with appropriate resources, who are independent of, but with access to, the design team.

In general, we believe that V&V activities should take place throughout the life of a project, rather than mainly at the end. Obviously, some V&V work has to wait until there are suitable outputs from the design process. Later in a project, when mock-ups and prototypes are available, these should be subject to V&V. However, earlier in the process it should be possible to do some V&V work. We feel that the benefits of V&V are at least as great early in the process as they are in later stages. This position is in agreement with IEC 1771 (1995a, p. 13) which states that

> It should be noted that this V&V activity [of functional design and detailed design] may be carried out at different stages of control-room design. Particularly for a new design, it can be seen as an iterative process, starting at a very early stage and being repeated periodically. This allows for design changes that result from reviews to be incorporated earlier in the systems. This results in a significant improvement of the overall design process. (IEC, 1995a, p. 13)

4.2 Planning for V&V

A V&V plan should be prepared early in the project and before the V&V work is carried out. It would be expected to contain, at a minimum, details of:

- The objectives for V&V.
- The mandate and terms for V&V.
- The relationship and interfaces of V&V to other elements both within and outside that of the project, for example, the design process and the quality assurance programme.
- The V&V team, its primary responsibilities, the authority of the team and resources available to it.
- A description of approach taken to V&V.
- How the process will be applied.

4.3 Basic V&V Process

The framework we have created for this report adopts the main V&V stages identified in IEC 1771 (1995a, p. 13) for verification and validation of a new control room, namely preparation, evaluation, and resolution. A full description of a generic process for carrying out V&V is described in section 5. The main components of this generic process as we have adapted it are:

1. Preparation — assembly of the elements required for the V&V process:
    - Identification of the performance and safety objectives for the modification or upgrade and development of the evaluation criteria. This should involve the documentation of the detailed criteria to be used for the evaluation.
    - Familiarisation with the concept or system to be considered including collection of all documentation related to the aspect under consideration and used in the design process. This documentation will be the basis for the V&V.
    - Identification of the functions, users, information needs, task interactions, etc. for the system from the source documents.
    - Selection of an appropriate evaluation methodology.
    - Identification of workspace and equipment required by the team in order to apply the selected evaluation methodology.
    - Definition of a schedule. This should detail the time requirements, relations and dependency between the tasks within the evaluation process.
    - Creation of an evaluation team. The team should be independent of, but have access to, the design team.

2. Evaluation — the appraisal or assessment of the human factors aspect:

- Process of evaluation. This should be carried out in line with the evaluation methodology identified previously and shall be systematic and documented.
- Record of evaluation. The evaluation results should be recorded as well as any deviations from criteria or the agreed methodology.

3. Resolution – of the identified deviations:
   - Evaluation of deviations and correction as required. The process for the consideration of these aspects should be systematic and documented.
   - Consideration of possible interactions of the deviations and corrections.
   - Documentation of process and outcome. The complete process should be adequately documented and recorded.

4.4 Timing of V&V within the Design Process

Firm guidance on when in the design process V&V is best applied, is typically sparse and very general in nature. In the past, there has been a tendency for V&V to be conceived as a series of tests and evaluations that are carried out at the end of the project after the design is completed. This view is still reflected in much of the literature. More recently, there has been general agreement that V&V should be more iterative and integrated into the design process. For example, Hollnagel (1985) describes verification as

> ...an organic part of the design process rather than something which occurs between the completion of the design and the release of the system for actual use (Hollnagel, 1985).

He identifies three reasons for this approach:

> Design iterations and Evaluation: Since the complexity of MMSs [man-machine systems] cannot be completely accounted for in the design basis the design process must consist of a series of iterations where the problems are decomposed into sub-problems and where solutions to these are found and verified. Such part-verifications of means, activities, and goals are necessary to ensure that the partial solutions work correctly and that they work together. From this perspective, the final verification of the whole system is the logical completion of a series of verifications that are an integral part of the design process rather than a separate exercise.
>
> Impact of evaluation results: Furthermore, if the verification only takes place after the design is completed it will be very difficult to introduce any substantial changes. Smaller changes of a cosmetic nature, such as deviations from established ergonomic principles can probably be accommodated. But barring catastrophic design flaws, other demands for changes are likely to be either postponed for later system revisions, or to be subsumed under training, operational support, instructions, etc. Human adaptability thereby serves as a buffer for design inadequacies, and provides the slack necessary for the system to function.
>
> Information requirements of the evaluation: Finally considering the verification throughout the design process will make it much easier to provide the required information. In order to carry out verification one must know specifically what the purpose of the system is. Such specifications are the result of design decisions, but if these are not properly documented, they may be difficult to reconstruct afterwards. Reasons that seem obvious at the time of decision may therefore have to be replaced by ad hoc reasons derived from a later analysis. This will not only make it more difficult

to carry out the verification, but also increase the uncertainty and ambiguity of the criteria. (Hollnagel, 1985).

Glenn and Niehoff (1985) and Stubler et al. (1993) endorse this approach of integrating an iterative V&V into the design process. Stubler et al. (Op.cit.) propose the use of lower fidelity test beds for addressing human performance issues much early in the design process to allow modifications to be made with minimal effect on the overall MMI system. They suggest the use of part-task simulators comprising both individual and partially integrated sets of prototype components and dynamic simulations of selected parts of the process. These they suggest should be performed as soon as they are available. This approach, in combination with the integrated system testing, will help to overcome Hollnagel's concerns.

The view of V&V as an integrated and iterative process is partially evident in the contents of recent standards and guidelines, although guidance as to exactly when and how often V&V should be carried out is less clear. For example, IEC 1771 states that:

> It should be noted that this V&V activity may be carried out at different stages of control room design. Particularly for a new design, it can be seen as an iterative process, starting at a very early stage and being repeated periodically. (IEC 1771, p.13)

However, despite the above statement the IEC standard only describes the V&V process being applied at two distinct phases in the design process: following completion of the functional design, and following detailed design, Figure 6. V&V of the functional design is concerned with the basic allocation of function between the operator(s) and the automation within the design and whether those tasks and functions are supported by the design. V&V of the detailed design concerns assuring the output from the functional requirements phase have been correctly incorporated into the design and assessment of the integrated control room. It should also be noted that the V&V process is not applied to single human factors topics but rather to related groups of topics or the results of a series of topics.

These two phases in the design process described in the IEC standard move away somewhat from the earlier tendency to test and evaluate at the end of the design. Nevertheless, V&V is still seen as a distinct and separate process applied to the design process rather than integrated within it. A similar approach is advocated in IAEA (1995).

NUREG-0711 (1994c) describes five distinct phases related to the timeline of the project:

1. *Human System Interface (HSI) Task Support Verification*: a check to ensure that HSI components are provided to address all identified person tasks.

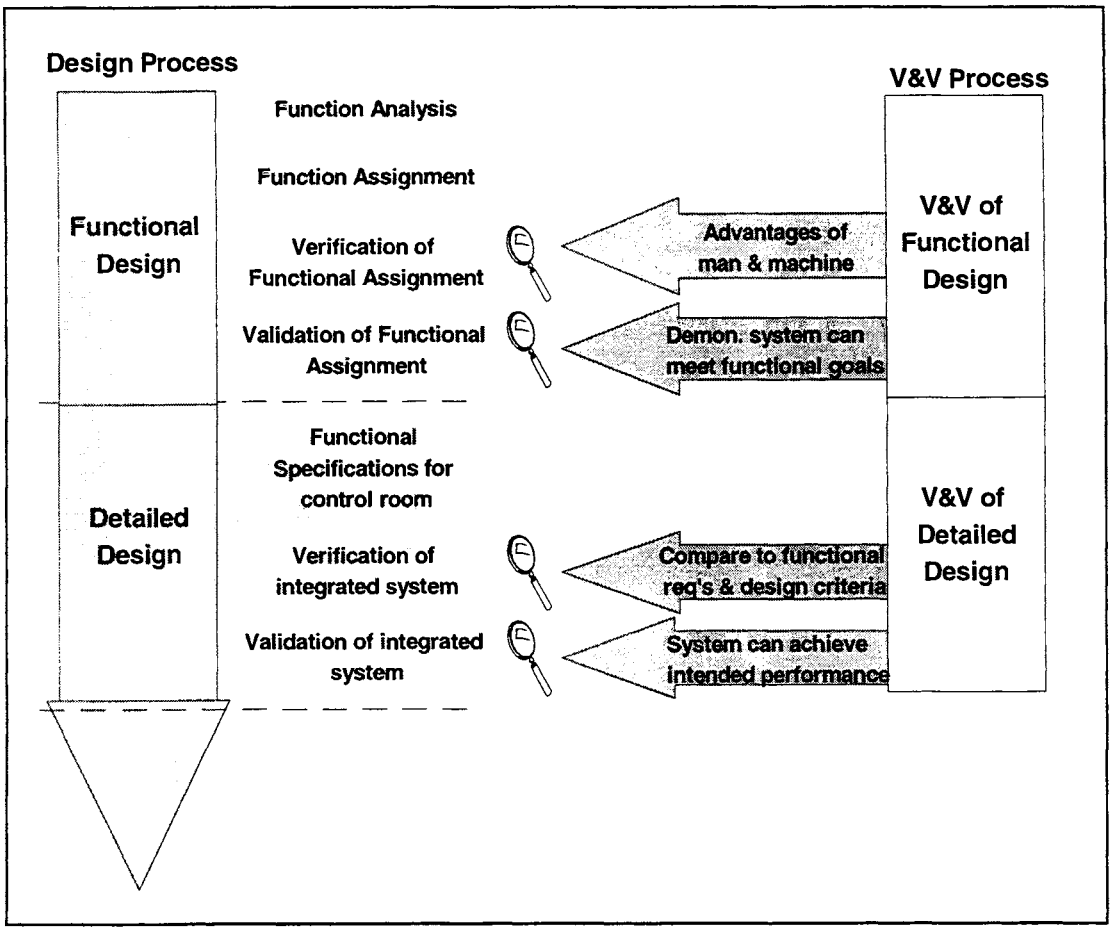

Figure 6. Timing of V&V activities in IEC 1771

2. *HFE Design Verification*: a check to determine whether the design of each HSI component reflects HFE principles, standards, and guidelines.

3. *Integrated System Validation*: performance based evaluations of the integrated design to ensure that the HFE/HSI supports safe operation of the plant.

4. *Human Factors Issue Resolution Verification*: a check to ensure that the HFE issues identified during the design process have been acceptably addressed and resolved.

5. *Final Plant HFE/HSI Design Verification*: describes the detailed design and performance criteria, ensuring that any remaining aspects are subjected to a suitable V&V method and that the in plant design corresponds to that described and specified by the design process.

The primary steps in this process are shown in Figure 7. It should be noted that individual stages relate to *either* verification *or* validation and not both.

V&V work can also take place in several different groupings of related human factors topics, in parallel, rather than solely in one large integrated system test. Testing of a group of related human factors topics together, without waiting for other aspects to be

completed, allows feedback and corrections to the design as early as possible. Groupings of human factors topics for the purpose of V&V work can be related to the timeline of the project, as described in IEC 1771 and NUREG-0711. Stubler et al. (1993) make the important point that "it is not the individual components themselves which should be V&Ved, but rather specific human performance issues." The issue of grouping of human factors topics is discussed in Section 6.

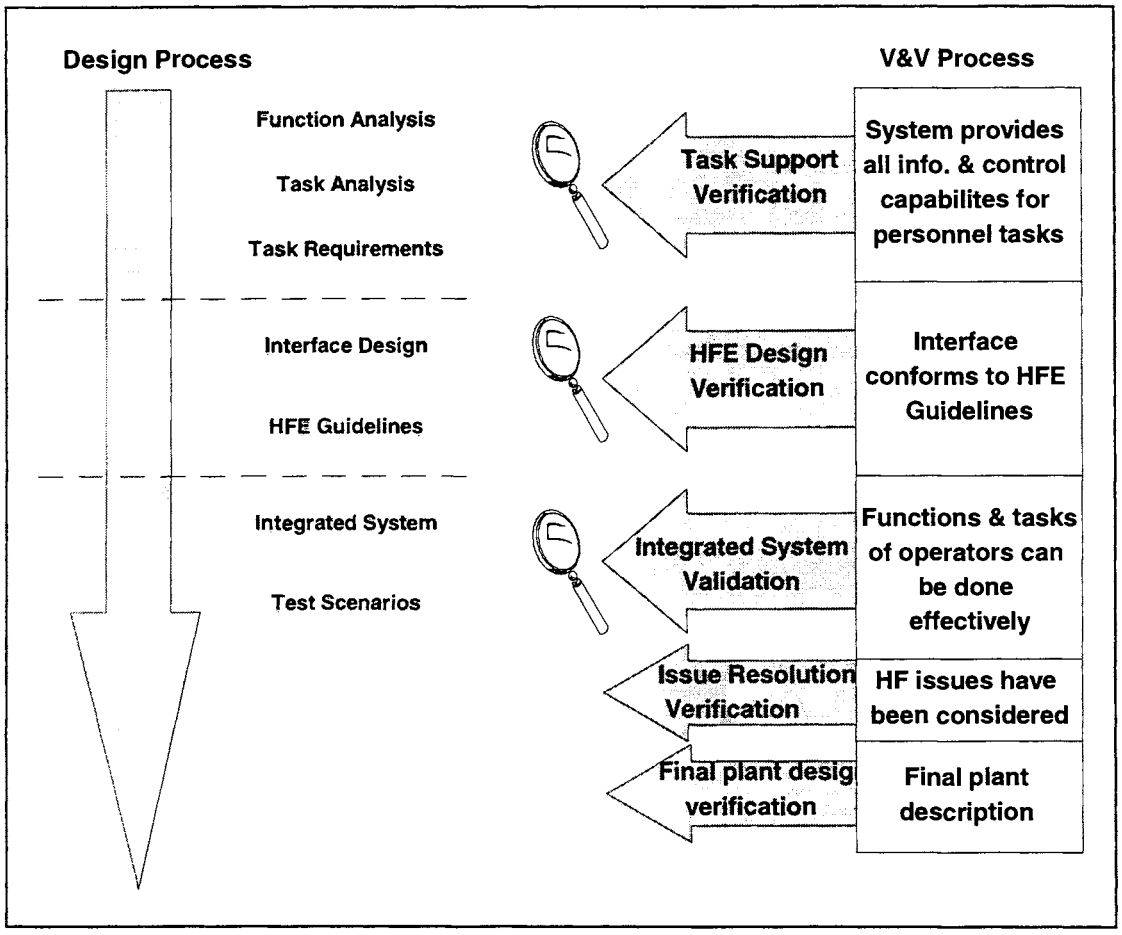

Figure 7. Timing of the Principal V&V Activities in NUREG-0711

5 Generic V&V Process

This section of the report describes a generic process for verification and validation. Firstly, the main reasons for developing a generic framework are outlined and the principal references identified. Separate sections on the generic processes for verification and validation itself are presented in sections 5.1 and 5.2.

The main reasons for the report adopting a generic approach to the process of V&V are:

- Applicability to different V&V processes.
- Applicability at different times in a project.
- Applicability to any human factors topic.
- Applicability at varying levels of detail.
- Points 2, 3, and 4 correspond to the dimensions used to characterise the V&V process in section 4.1, Figure 5.
- V&V of the human factors content of a project, the subject here, should not be confused with work on the human factors topics themselves. The process of verifying and validating, for instance, coding techniques used in an alarm system, is a different matter from the design issues in coding themselves. These issues should be addressed as parts of the larger human factors programme (NUREG-0711, 1994).

V&V of a project's human factors work should also be distinguished from the question whether tests and evaluations were themselves valid and reliable. NUREG 6393 (USNRC, 1996, p. 4-4) expresses the distinction in this way:

> The different uses of the terms 'validation' and 'validity' are potential sources of confusion. The term validation is used...to describe a process by which a NPP design is evaluated to determine whether it adequately satisfies the demands of the real-world operating environment. The term validity is used to describe characteristics of the methods and tools used in the validation process. (USNRC, 1996, p. 4-4)

That is to say, we can distinguish two things: a) whether a satisfactory programme for V&V of human factors was carried out, and b) whether the specific methods and measures used in human factors techniques and tests themselves were valid, reliable and generally following good practice. The latter question, especially the validity of methods and tools, is specifically covered in NUREG/CR-6393 (1996) and generally in a large volume of other human factors literature. It is not the subject of this report, although it is of course something that should be addressed (see sections 5.1.2 and 5.2.2).

The generic structure and the presentation of human factors topics within this report are presented as a set of questions. Each question is printed in Italics and is followed by explanatory text.

The generic V&V process contains the main stages identified in IEC (1995a), namely, preparation, evaluation, and resolution. We have filled out and altered this framework

by incorporating guidance and comments on the verification and validation process given in several other documents.

The documents reviewed for the project are listed and annotated in Appendix A. Of these, the most important for the present purposes were:

International Electrotechnical Commission (1989). *Design of Control Rooms for Nuclear Power Plants.* Geneva: IEC (International Standard 964. (1989-03)).

International Electrotechnical Commission (1995a). *Nuclear power Plants — Main Control Room — Verification and Validation of Design.* Geneva: IEC (International Standard 1771. (1995-12)). Supplementary standard to IEC 964.

U.S. Nuclear Regulatory Commission (1994a). *Advanced Human-System Interface Design Review Guideline: General Evaluation Model, Technical Development, and Guideline Description.* Washington: U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research (NUREG/CR-5908 Vol. 1).

U.S. Nuclear Regulatory Commission (1994b). *Advanced Human-System Interface Design Review Guideline: Evaluation Procedures and Guidelines for Human Factors Engineering Reviews.* Washington: U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research (NUREG/CR-5908 Vol. 2)

U.S. Nuclear Regulatory Commission (1994c). *Human Factors Engineering Program Review Model.* Washington: Nuclear Regulatory Commission Office of Nuclear Regulatory Research (NUREG-0711).

U.S. Nuclear Regulatory Commission (1996a). *Integrated System Validation: Methodology and Review Criteria.* Washington: U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research (NUREG/CR-6393)

U.S. Nuclear Regulatory Commission (1996b). *Human System Interface Design Review Guideline. Revision 1, Volume 1: Process and Guidelines.* Washington: U.S. Nuclear Regulatory Commission Office of Nuclear Regulation (NUREG-0700).

Glenn D.J. and Niehoff M.E. (1985). Control Room Design Change Verification at Ft. St. Vrain. In: *IEEE Third Conference on Human Factors and Power Plants*, Monterey, California, 23-27 June 1985, Edited by E.W. Hagan. Institute Electrical and electronic Engineers, New York, 1985, pp 109-114.

Stubler, W.F., Roth, E.M., Mumaw, R.J. (1992). Integrating Verification and Validation with the Design of Complex Man-Machine Systems. In: Wise, J.A., Hopkin, V.D., Stager, P. (1992) *Verification and Validation of Complex Systems: Human Factors Issues.* Berlin: Springer-Verlag (NATO ASI Series F: Computer and Systems Sciences, Vol. 110), pp 159-172.

Some of the most important standards for the project, and the inter-relationships between them, are shown in Figure 8.

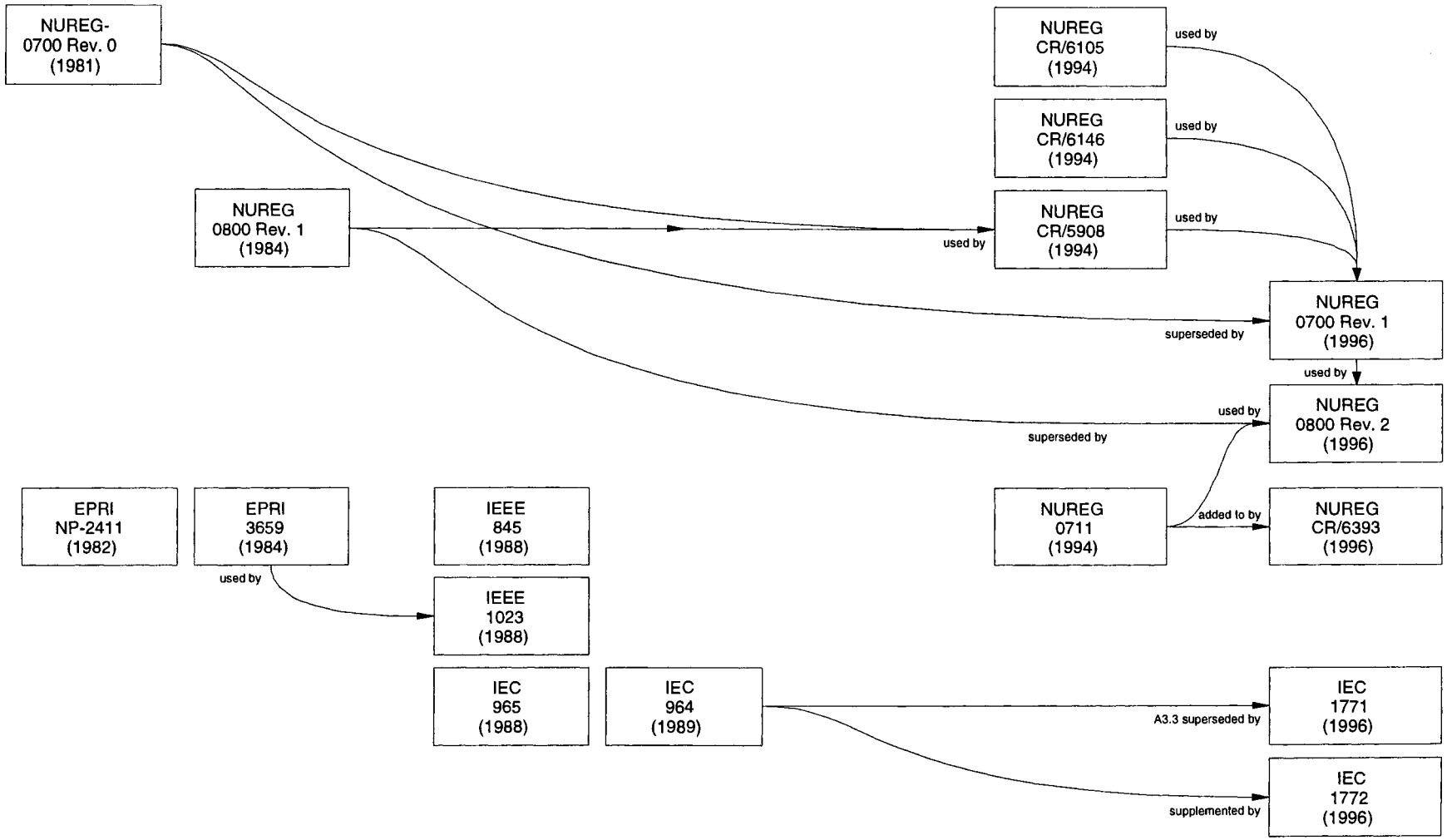

Figure 8. Relationships between Main Standards Influencing the Verification and Validation Process for Human Factors

5.1 Verification — A Generic Process

Verification is a kind of review or evaluation that shows whether something (e.g., a design, prototype or finished product) meets its specifications. That is, verification answers the question "Did the designers do what they said they would do?" Validation, on the other hand, shows whether something is effective, or "Does the system work?" (Stubler et al., 1993.). Both types of review are necessary because:

- It is possible to build something that meets its specifications but that is nevertheless not useful — it is verified but not valid.
- It is possible to build something that has some effectiveness but in which one cannot have confidence because it has not been shown to conform with a comprehensive specification — it is valid but not verified.

Generically (i.e., free of any reference to a specific human factors topic) a verification has several steps. A recent international standard (IEC 1771, 1995a) gives three main stages:

- Preparation.
- Evaluation.
- Resolution.

There is emphasis on the preparation phase to ensure good review results. The standard stresses that preparation should also take into account the information needs of human factors for control room design, so that reference material is available throughout the design process.

The sections in our own generic structure rearrange the structures within these headings and develop them further. Under each heading we include questions that suggest the kinds of evidence that could be asked for and the purpose behind each question. We now describe the three stages of preparation, evaluation and resolution relating to verification and the question set developed to investigate that aspect.

5.1.1 Preparation

5.1.1.1 Documents Used in Verification

Did the utility identify relevant source documents?

This question refers to familiarisation with the concept or system to be considered and documents that will be used for reference throughout a project. The utility's evaluation team should collect all documentation related to the topic under consideration and used in the design process. The documentation will be the basis for the verification process. The evaluation team should have access to members of the team that was responsible for design and documentation (IEC 1771, 1995).

A document structure should be developed, along with a review and approval procedure, with the outcome being the availability of documents to all design personnel. These provide guidance on all human factors issues. This helps to ensure uniformity of design by establishment of continuity and convention (Glenn et al., 1985).

The documentation should include material produced specially by the utility for a project, and more general information, such as standards, guidelines and human factors literature. The documents could include (based on IEC 1771, 1995):

- Normative documents.
- Human factors literature and guidance specific to the topic under review.
- Utility event reports.
- Failure analyses.
- Safety analyses.
- Incident and accident analysis reports.
- Feedback from experience with previous designs.
- Contract requirements.
- Systems descriptions.
- System specifications.
- Task analysis documents.
- Control room assessment.
- Generic control room design report.
- Panel or workstation drawings.
- Lists of acronyms and abbreviations.
- Descriptions of coding conventions.
- Man-machine interface style guides.
- Computer-processing specifications (e.g., alarm-processing).
- Procedures.
- Operator training manuals.
- Other documentation specific to the topic under review.

The documents used could also include human factors guideline documents, such as NUREG/CR 5908 Vol.2, 1994. There are disadvantages as well as advantages with the use of human factors guidelines or the style guides offered by software vendors. Firstly, conformance with guidelines does not guarantee that a system will be effective (valid). A check against the guidelines and other documents used by a project can only establish (verify) that the guidelines have indeed been followed. (This is a corollary of the fact that validation is necessary but not sufficient for testing a system.) Validation methods, such as evaluation of the dynamic performance, should be used in conjunction with evaluations against guidelines. Secondly, standard collections of guidelines may contain many topic areas that are not appropriate to a particular design review. An evaluation team need not use these.

Was the evaluation team given access to applicable documents prior to the beginning of verification?

Evidence needs to be presented that a utility's evaluation team had appropriate documentation. There should be no indication that a utility's evaluation team is being bypassed or isolated and is not being provided with relevant documentation.

Did the evaluation team have access to a human factors operating experience review?

One important source of information early in a project is an Operating Experience Review (OER) of human factors issues. The issues learnt from an OER provide a basis for improving the plant design at the beginning of the design process. Ways in

which the OER contributes to the human factors programme are shown in NUREG-0711, p. 3-1).

The resolution of OER issues can influence almost any human factors issue, such as training, staffing, procedures and equipment design. It can also contribute to V&V issues by indicating:

- Tasks to be evaluated.
- Event and scenario selection.
- Selection of Performance measures.
- Issues that need to be resolved in the new or evolutionary design.

5.1.1.2 Verification Team

Did the utility have a suitable evaluation team for the topic?

The evaluation team should be independent of the design team but should have access to it. The team may need to include experts from a variety of backgrounds appropriate to the topic. The independence of the evaluation team should not inhibit the communication with designers, who should be available for discussions and explanations.

Was the evaluation team suitably placed in the utility's organisation?

The team should have responsibility, authority and placement within the organisation to ensure that the commitment to human factors V&V is achieved (NUREG/CR-5908 Vol. 1).

Did the evaluation team have a suitable mix of disciplines?

The composition of the team will vary according to the size of the task or modification and the topic under review (IEC 1771, 1995). For instance, a review of alarm processing will call on experts differing from those used for a review of the control room environment. A basic technical team will usually include these areas of expertise, according to IEC 1771, 1995:

- Systems engineering.
- Architectural design and civil engineering.
- Systems analysis.
- Instrumentation and control systems.
- Information and computer systems.
- Human factors engineering.
- Plant operation and training.

The International Atomic Energy Agency (1995) gives a similar list for members of the design team. The evaluation team is likely to require the same knowledge and experience:

- Control room area and control panel facilities design.
- Instrumentation and control systems design.
- Digital information and communications systems design.
- Human factors engineering and cognitive science.
- Nuclear power plant operations and management.
- Nuclear power plant hands-on operations and maintenance experience.
- Nuclear safety requirements.

The specific areas of expertise represented should be based on the scope of the evaluation, however, operating experience is particularly important. The number of members of the team should be kept to a size commensurate with efficient work and communication. Expertise can be called in as necessary for human factors topics or areas of expertise not covered by the team (IEC 964, 1989).

Was the evaluation team independent?

The members of the team should have some independence from the designers. For instance, if a system being reviewed was produced by an I&C department then the team could be organised under the safety department.

The purpose of having an independent evaluation team is to help ensure an unbiased evaluation. Independence helps to ensure that:

- Systems are not tested against the same constraints and assumptions that they were designed against.
- There is less chance of an expectancy bias.
- The evaluation team does not have a vested interest in finding that everything is satisfactory.

5.1.1.3 Verification Resources

Did the utility supply suitable resources for the evaluation team?

This question refers to the resources, workspace and equipment required by the team to apply the selected evaluation method. There should be appropriate space for the evaluation team and any part-time consultants and specialists. There may be special equipment requirements (IEC 1771, 1995).

A full-scale mock-up is often very useful, not only for V&V (Glenn et al., 1985). There are several potential uses:

- Control Room (CR) audits and surveys.

- Task analyses and walk-through studies.
- CR improvements.
- Training.
- Input to a later full-scope simulator.

Were suitable working materials prepared?

The evaluation team should develop standard procedures, data sheets, etc. for conducting the review to systematise the effort (IEC 1771, 1995, p. 47). Types of forms and working materials that may be needed include:

- Documentation control.
- Component inventories.
- Control room components and features.
- Measurements - noise, lighting, heating.
- Questionnaire and interview records.
- Records of operator responses to specific tests (e.g., using a simulator).
- Human engineering discrepancies (HEDs) — to identify their location and nature so that follow-up action can be taken.
- Resolution of HEDs.

5.1.1.4 Verification Scope

Was the evaluation scope appropriate for the stage of the project at which it was performed?

At earlier project stages, only limited verification may be possible. Later, for example, when full scale mock-ups, simulators, etc., are available, more complete and comprehensive verification should be expected.

Did the evaluation include consideration of all appropriate scenarios?

There should be written description of appropriate operating situations, adapted to the chosen verification method and the stage of the project. These scenarios should be representative of the actual plant and should cover normal operation, a mix of multiple failure events and disturbances, and emergency conditions (IEC 964, 1989).

Did the utility include all relevant locations?

The focus of work is often the main control room. However, the design or design change may affect several other areas. It is important that these are included in the evaluation process. Affected areas could be (NUREG/CR-5908 Vol. 1):

- Auxiliary Shutdown Rooms and panels.

- Local Control Panels or stations.
- Other controls, switches, valves and breakers that are operated or consulted during normal, abnormal or emergency operations.

NUREG-0711, p. 11-2 also states that the general scope of the V&V should include all facilities defined in the project plan:

- Hardware having an MMI.
- MMI software.
- Communications facilities.
- Procedures (written or electronic form).
- Workstation and console configurations.
- Design of the overall work environment.
- Trained personnel.

Reviews have found that control points outside the main control room are often the source of human factors weaknesses. Therefore, the utility's human factors work and the V&V of this work should encompass these areas as well as the main control room.

5.1.1.5 Verification Schedule Development

Did the utility develop a suitable schedule for verification?

The evaluation team should be guided by a plan for human factors activities and V&V of them (NUREG/CR-5908 Vol. 1, Glenn et al., 1985). This should detail the time requirements, relations and dependencies between the tasks within the evaluation process and should extend throughout the whole project's duration. The schedule should be developed during the preparation phase of a project (IEC 1771, 1995). The schedule for verification should have an entry for each topic being reviewed, and the responsibilities and functions of the team members defined.

The verification plan can be adapted from similar plans used for software development. Suggestions for such a plan are given in IAEA (1996, p 34):

> The plan should document all the criteria, the techniques and tools to be utilised in the verification process. It shall describe the activities to be performed ... and each phase to show whether ... the requirements specification is met. The level of detail should be such that an independent group can execute the verification plan and reach an objective judgement whether the software meets its performance requirements.

The document goes on to say that the verification plan should address

- Selection of verification strategies.
- Selection and use of test equipment.
- Execution of verification.

- Documentation of verification activities.
- Evaluation of verification results.

5.1.1.6 Verification Objectives

Did the utility define specific objectives for the verification of a topic?

The general objective of verification is of course to establish that the design meets its specification. It is better for a utility to develop specific objectives for each topic under review. If this is done it will be easier for a utility to set itself specific pass-fail criteria designed to test these objectives and to evaluate whether these have been reached. For example, objectives for verification of the human factors topic 'Function Assignment' (IEC 1771, 1995) could be:

- To confirm that all functions necessary for the attainment of plant operational and safety goals have been identified.
- To show that the proposed assignment is in accordance with criteria.
- To show that all the relevant requirements for function assignment have been identified.

5.1.1.7 Verification Criteria

Did the utility develop criteria for the human factors topic?

Criteria should be defined for the evaluations of each human factors topic and for the objectives that the evaluation is intended to reach. This means that both specific issues need to be defined and the levels at which a design is judged to have passed or failed on to these issues. Experience has shown that it is important to define these early in the evaluation process (e.g., Glenn et al., 1985). It is not sufficient to have verification methods and objectives. There needs to be an evaluation too. NUREG 6393 (USNRC, 1996, p. 5–32) makes this point:

> A performance measure only describes performance...The goal of measurement is to allow a conclusion to be drawn...In order to judge the acceptability of system performance, it is necessary to establish criteria for the performance measures used in the evaluations. Performance criteria are the standards against which the integrated system performance is compared to judge its acceptability. (USNRC, 1996, p. 5–32)

The criteria can be derived from the source documents in use for the project, such as those given in IEC 1771 (1995):

- Any applicable mandatory regulations.
- Performance aspects.
- Safety principles.
- Availability and reliability requirements.
- Operator interface and display principles.

- Requirements from applicable standards, regulations and guidelines.
- Human factors literature.

or other specific criteria laid down by a regulator. USNRC (1996, p. 5–33 classifies performance criteria into several types:

- Requirement-referenced criteria — the comparison of the performance of the system to an accepted performance requirement.
- Benchmark-referenced criteria — the comparison of the performance of the system to a benchmark system that is defined as acceptable.
- Normative referenced criteria — the comparison of the performance of the system to norms established for the performance based on many system evaluations.
- Expert-judgement referenced criteria — the comparison of the performance of the system to criteria established through the judgement of subject-matter experts.

The criteria that are developed should include both technical aspects and human factors aspects. The criteria will need to cover the complete set of human factors topics that are relevant to a project.

The utility should have developed performance and safety criteria that relate to the topic under review. A utility will not be able to show that a topic has been verified until it can give evidence of an evaluation against these criteria. Obviously, if the objectives and criteria were not stated clearly in the first place, any V&V will at best be inconclusive.

5.1.2 Evaluation

5.1.2.1 Verification Method

Did the utility develop and document a suitable method for verifying a topic?

The utility should state how a topic was assessed. The methods and measures used themselves need to be reliable and valid. Advice on design and evaluation methods is available in several sources, such as NUREG/CR-6393 (1996), ANSI (1992). Appendix A contains annotations to show those references that we believe will be helpful in providing advice on test and evaluation methods.

5.1.2.2 Verification Process

Was the review process satisfactorily documented and traceable?

The method should be carried out in line with the evaluation methodology developed in section 5.1.2.1 and should be systematic and documented. Often, there will be requirements placed by the quality assurance standards in force for the project.

Were quantitative criteria defined and measured satisfactorily?

The review process should, as far as possible, include quantitative measures of the required features and performance.

5.1.2.3 Verification Results

Were the review results recorded satisfactorily, including deviations, non-conformities and assessments against criteria?

The results from the evaluation should be recorded, including any deviations from criteria or the planned methodology (NUREG-0711, 1994).

5.1.3 Resolution

Were satisfactory resolutions developed and recorded for all deviations and non-conformities?

There should be evidence that any deviations found in the evaluation (including failures to reach criteria and non-conformities) have been acted on. The process for the consideration of these aspects should be systematic and documented. All deviations may be evaluated for their potential effects and then addressed by the review process (Stubler et al., 1993). A decision then needs to be made and documented whether to:

1. Bring a deviation into compliance by modifying the design, selection of design alternatives, refinement of requirements, refinement of design criteria (IEC 1771, 1995).

2. Reduce potential effects through such means as procedure modifications, training, or

3. Allow a deviation to stand without change if it is found to have negligible impact on the system.

Were there checks for side effects of resolutions?

There should be evidence that the evaluation team has considered the possibility of side effects of any changes made because of deviations or non-conformities. For instance, a determination on human factors grounds that labelling in the control room needs to be changed may need to be reconciled with the prevailing plan for labelling and tag-numbering in the rest of the plant. It is important to ensure that on-going modifications do not conflict with other design issues and that they confirm the design basis (Glenn et al., 1985).

5.2 Validation — A Generic Process

The definition of validation is given in section 2.2.2. Validation is a kind of review or evaluation that tests whether something is effective. Verification, on the other hand, tests whether something (e.g., a design, prototype or finished product) meets its specifications. Verification may be necessary, but it is not sufficient without validation.

Another view of validation is that it addresses future conditions of use. The validation process should challenge the design and establish that the system will perform acceptably under a broad range of operating conditions. A validation process cannot prove that a design will work under *all* real world conditions (NUREG/CR-6393). Instead, a validation establishes through a comprehensive evaluation that a design is *not in*valid.

Validation should be an integral part of the design process. It is not a "fig leaf" designed to cover embarrassment that is applied at the end of a project (Stager, 1992). The objective should be to help during the design, not only to justify it at the end. Tests should be done as early in the design process as possible, to allow modifications to be made (Stubler et al., 1993).

Generically, a validation has similar steps to verification:

- Preparation.
- Evaluation.
- Resolution.

A variety of topics could be subject to validation, depending on how human factors topics are grouped. The question of the convenient grouping of human factors topics is covered in section 6. These could include those given in NUREG/CR-6393, 1996, p. 5-1 ff., those given in this report, those given in other standards, or any others required by a regulator.

We now describe the three stages of preparation, evaluation and resolution relating to validation and the question set developed to investigate that aspect.

5.2.1 Preparation

5.2.1.1 Documents Used in Validation

Did the utility identify relevant source documents?

Some documents may have been updated as a result of verification. Documents relevant to individual human factors topics may have been developed since earlier design stages or verification, such as control room floor plans, detailed screen designs, alarm messages, plant labelling, etc.

It should be noted that human factors as a subject is evolving. Observation of human factors criteria does not guarantee that a system is satisfactory (IAEA, 1995, pp. 72-73). This is one reason why validation is necessary as well as verification. For example, anthropometric criteria valid 20 years ago may not be valid now. Therefore, human factors source material may need to be reviewed and revised. Up-to-date sources, or revisions of previously acceptable sources, may be necessary.

Was the evaluation team given access to applicable documents prior to the beginning of validation?

The evaluation team should also have access to members of the team that was responsible for design and documentation.

Did the evaluation team have access to a human factors operating experience review?

Comments given in section 5.1.1.1 apply.

5.2.1.2 Validation Team

Did the utility have a suitable evaluation team for the topic?

Staff with detailed process knowledge and operating experience may be particularly important in validation, both in the design of tests and as test subjects.

Was the evaluation team appropriately placed in the utility's organisation?

Comments in section 5.1.1.2 apply.

Did the evaluation team have a suitable mix of disciplines?

Comments in section 5.1.1.2 apply.

Was the evaluation team independent?

Comments in section 5.1.1.2 apply.

5.2.1.3 Validation Resources

Did the utility supply suitable resources for the evaluation team?

Comments given in section 5.1.1.3 apply.

Were suitable working materials prepared?

Comments given in section 5.1.1.3 apply.

There may need to be an appropriate control room model that allows time-dependent dynamic characteristics to be evaluated. For a system whose concept is considerably different from conventional systems, a dynamic simulator is necessary for late stages of validation. Other choices, such as a full-scale mock-up, can be justified when either the difference is minor, or the validation is partial and earlier in the design process (IEC 964, 1989).

5.2.1.4 Validation Scope

Did the evaluation include consideration of all appropriate scenarios?

There should be a written description of appropriate operating situations, adapted to the chosen validation method and the stage of the project. These scenarios should be representative of the actual plant and should cover normal operation, a mix of multiple failure events and disturbances, and emergency conditions (IEC 964, 1989).

Scenario descriptions should cover the initial conditions, the proper sequence of human and plant responses and relevant symptoms. The expected paths to be

followed when operating the plant should be given to allow evaluation criteria to be addressed.

The scenarios should be realistic and cover environmental conditions that might affect human performance. Harsh environments may need to be simulated for tasks outside the MCR.

Was the evaluation scope appropriate for the stage of the project at which it was performed?

Comments in section 5.1.1.4 apply.

Did the utility include all relevant locations?

Comments in section 5.1.1.4 apply.

Validation may be limited at certain project stages by the recognition that certain parts (the control room, training programme, operating procedures, etc.) may exist only as drawings and specifications.

5.2.1.5 Validation Schedule Development

Did the utility develop a suitable schedule for validation?

Comments in section 5.1.1.5 apply.

5.2.1.6 Validation Objectives

Did the utility define specific objectives for the validation of a topic?

Comments in section 5.1.1.6 apply.

The utility should have developed performance and safety objectives for the topic under review. Generally, the objective is to establish that the system will perform acceptably, by showing that it meets performance requirements that have been established.

5.2.1.7 Validation Criteria

Did the utility develop criteria for the human factors topic?

Comments in section 5.1.1.7 concerning the development of criteria apply also to validation. The specific criteria will depend on the topic being reviewed. Some examples of objectives for which specific pass-fail criteria should be developed (from IEC 1771, 1995) are:

- The alarms, instruments and displays should be adequate to alert the operator to perform a required action.
- The controls and displays should be reachable and readable.
- The identification labels should be legible and complete without the need to resort to documentation.

- The indications should allow confirmation that actions have been taken or conditions cleared.
- The instrument scales and ranges should be appropriate.

The criteria may also depend on a regulator's experience as to what issues and objectives are practically important. It may be more difficult to develop criteria for issues that are more difficult to measure. Annex C of IEC 1771 (1995a) gives advice for studying the cognitive and information-processing aspects of designs

5.2.2 Evaluation

5.2.2.1 Validation Method

Comments in section 5.1.2.1 apply.

Did the utility develop and document a suitable method for validating a topic?

Comments in section 5.1.2.1 apply.

5.2.2.2 Validation Process

Was the review process satisfactorily documented and traceable?

Comments in section 5.1.2.2 apply.

Were quantitative criteria defined and measured satisfactorily?

Comments in section 5.1.2.2 apply.

NUREG-0711 (1994c, p. 11-4) suggests several performance measures for dynamic evaluations:

- Systems performance measures relevant to plant safety.
- Crew primary task performance, e.g., task times, procedure violations.
- Crew errors.
- Situation awareness.
- Workload.
- Crew communications and co-ordination.
- Dynamic anthropometry evaluations.
- Physical positioning and interactions

5.2.2.3 Validation Results

Were the review results recorded satisfactorily, including deviations, non-conformities and assessments against criteria?

Comments in section 5.1.2.3 apply.

5.2.3 Resolution

Were satisfactory resolutions developed and recorded for all deviations and non-conformities?

Comments in section 5.1.3 apply.

Were there checks for side effects of resolutions?

Comments in section 5.1.3 apply.

Did the evaluation team succeed in resolving issues, even when these arose late in the project?

Comments in section 5.1.3 apply.

6 Applications of the V&V Process to Human Factors Topics

Section 5 described a generic process for V&V of human factors. This section, after discussing the selection of the human factors topics to be considered, illustrates the application of the generic verification and validation process to some human factors topics.

We regard the particular human factors topics that need to be verified and validated as a pragmatic issue that will vary from case to case. In this report we have intentionally not explored all possible human factors topics in depth, recommended methods for carrying out work in these topics, or given pass-fail criteria for assessing work under these topics. However, we do feel it useful to illustrate how the generic V&V process could be applied to commonly occurring human factors topics.

In whatever way the design process is described, it will contain a number of human factors topics, each of which needs to be verified and validated, whether individually or in larger groups. In this report we have suggested human factors topics based primarily on the work of the International Electrotechnical Commission and the U.S. Nuclear Regulatory Commission, since the standards and guidelines provided by these organisations are likely to be the ones widely known within the industry.

The topics that we have selected should not be interpreted as a definitive listing, merely some of the topics that are likely to be substantially affected in any control room design or upgrade. If any further information on relevant topics is needed, the bibliography in Appendix A rates references for their relevance to the choice of human factors topics.

We have not given separate treatment in this section to some of the topics that appear in these references, in the interest of space and clarity. For example:

- 'Job Analysis' is discussed under 'Task Analysis'.
- 'Control and Display Design' is largely exemplified by reference to VDU displays rather than to more conventional instrumentation and controls.
- The location, environment and protection of the main control room are discussed under 'Space and Configuration'.
- The detailed arrangement of displays and controls is discussed briefly under 'Control and Display Design'.

We hope that the examples of verification and validation that are given are sufficient for the same pattern to be applied to these topics if desired.

There are a number of topics mentioned in many of references in Appendix A that are not covered at all in this section. Of these, three are mentioned here:

- 'Operating Experience Review': A review of human factors issues arising from operating experience is what we consider to be preparatory work and a source document for designs and reviews, including V&V reviews.

- 'Database of Human Characteristics': Similarly, a collection of information of human characteristics, standards, human factors knowledge, etc. is a source of information for design work rather than an object of the human factors V&V process. It is also one of the preparatory steps in the generic V&V process.
- 'Human factors issue resolution verification': We have not included this topic used by the USNRC because it has been treated as part of the generic V&V process rather than a human factors topic in itself.

The sections following give separate advice on the review of V&V for each of the remaining human factors topics. The presentation for each topic uses the question and explanation format given for the generic V&V structure. At the end of each section, we list any supplementary references for the specific human factors issue. These were not included in the V&V literature review in Appendix A and are intended to be illustrative rather than definitive.

The generic information previously given under each explanation has generally been omitted here. Instead, we have tried to illustrate how specifically to apply each question to the human factors topics under consideration. The generic explanations should be understood as continuing to apply to the specific topics.

On occasion, a question and explanation apply to both verification and validation. In these cases, the explanation given in the verification section will generally be more extensive but should be read as applying to validation also. For instance, the guidance given for the scope of verification in 'Function Analysis and Allocation' gives recommendations for the selection of scenarios and operating events. The comments apply equally to the selection of scenarios for validation.

6.1 Function Analysis and Function Allocation

Allocation of function has been defined as the

> ... assignment of responsibility for performing operations to human (i.e., operator) and/or machine in either exclusive or complementary ways so that functional goals are achieved. (IAEA, 1995)

The objective of the verification and validation of this human factors topic is to ensure (NUREG 0800 Draft Rev. 0, 1996) that:

- Important functions have been defined, including those important to plant safety.
- The allocation of function to humans and machines is appropriate.

Issues to be taken up in this topic are discussed in NUREG 0800 Draft Rev. 0, 1996 pp. 18.0-6.

Function analysis and function allocation (FA) both refer to efforts to identify and subsequently allocate tasks to people and machines. A FA activity by a human factors design team is to identify and document the functions that are allocated to the control system, the personnel, or a combination of the two. The purpose of this is to ensure that the allocations are optimised, without imposing unfavourable requirements on either person or machine (IEC 964, 1989).

The FA topic as we describe it here includes both an analysis phase and an assignment phase. Functional analysis is the identification and analysis of functions that must be performed to satisfy plant objectives. Function allocation (or assignment) is the assignment of functions to (NUREG 0800 Draft Rev. 0, 1996):

1. Personnel, e.g., manual control.
2. Systems elements, e.g., automatic control and passive, self-controlling phenomena.
3. Combinations of personnel and system elements, e.g., shared control and automatic systems with back-up.

The essential design steps in FA are:

- Analysis phase — the tasks to be performed by the designed system first need to be identified.
- Assignment phase — the tasks can then be allocated to machine, human or both. The basic goal of task allocation is to free operators from tasks they are not suitable for and to assign to operators those tasks for which they are most suited.

Job descriptions and staffing, etc., can then be established.

USNRC (1996c) states that acceptance of the function analysis and assignment should be based on conformance with review criteria, including:

- Identification of safety functions and processes.
- Identification of processes and functions that have been changed from the previous plant or system.
- Documentation of the technical basis for changed processes.
- A summary description of plant processes.
- A detailed narrative description of changed processes.

USNRC (1996b) gives an alternative method based on identification of plant safety functions and systems, identification and selection of operational events and function description.

The IAEA (1995, p. 56) notes that there are a number of factors influencing the identification and assignment of functions, including:

- Existing practices and procedures.
- Operational feedback.
- Regulations.
- Feasibility.
- Cost.
- Technical factors.
- Policy.
- Social factors.

The assignment of functions is verified at the functional design stage. This assignment is then validated to ensure that functional goals will be achieved. In the specification phase, the functional assignments are verified and validated. This ensures that they fulfil the design principles and technical requirements, and that the system in question really does support safe and reliable operation (IAEA, 1995).

It should not be forgotten that operators often have responsibility for other functions than just process supervision. Typical such functions are:

- Fire detection and fighting.
- Access control.
- Preparation for work permits.

IEC (1995a) notes that extensive top-down function analysis may not be necessary if functionality can be shown from existing documentation and if there are successful arguments for qualification by similarity. The V&V of functional assignment is relevant both to the design of new systems and to retrofitting projects, where the role of the operator will change (IAEA, 1995, p. 57). Any changes in function assignment and their integration with other functions should be verified and validated.

Improvements in the control room should be based on operators' real needs. The control room operational philosophy and operators' roles should not be changed without good cause. New systems should be the same as old systems where those are satisfactory. The new systems and functions should also be consistent with non-replaced control room systems (IAEA, 1995, p. 65).

6.1.1 Verification of Function Analysis and Function Allocation

The correct assignment of functions to person and machines should be verified (IEC 964, 1989). Verification of FA means the presentation of evidence that the allocation of function is in line with the criteria and specifications for function allocation developed for the project. The completeness of the assignment should also be verified.

6.1.1.1 Preparation

6.1.1.1.1 Documents Used in Verification

Did the utility identify relevant source documents?

All the documents listed in the generic plan could be of use during FA. For modifications rather than new designs, a subset could be used (IEC, 1995a, p. 17).

Analysis should be based on accurate information sources. Descriptions of plant systems, schematics, P&I diagrams, safety analysis reports, etc., Plant procedures, emergency response guidelines, technical specifications and personnel training materials will also specify functions and tasks (NUREG 0800 Draft Rev. 0, 1996, p. 25).

Lupton et al. (1991, p. 358, Figure 3) provide a good summary of several sources of documentation that could be used in functional design:

- Safety and licensing documentation — systematic reviews and analysis, safety goals and principles, operator response guidelines and event sequence diagrams.
- Control centre design documentation — previous control centre experience, human factors principles, design guides.
- Plant design documentation — production goals, performance specifications, initial plant description, process and instrumentation diagrams.
- Operations and commissioning documentation — previous operating manuals, initial operating policies and principles.

Was the evaluation team given access to applicable documents prior to the beginning of verification?

Accidents, reports, operating experience, previous alterations to equipment may give indications on where changes to FA need to be made. The design team may need explicitly to be given access to these, or helped with searches. The evaluation team needs access to these documents before verification begins.

Did the evaluation team have access to a review of human factors operating experience?

Operating experience may be a source of information, or at least of indications, that past allocations have not been entirely satisfactory and specific problems have occurred (NUREG 0800 Draft Rev. 0, 1996, p. 26). There may be instances where automation has not worked particularly effectively. There may also be tasks on older systems that can now be reallocated partially or totally to machines.

6.1.1.1.2 Verification Team

Did the utility have a suitable evaluation team for the topic?

Lupton et al. (1991, p. 361) suggest that a peer review to verify the completeness and correctness of the function analysis and function allocations.

Was the evaluation team suitably placed in the licensee's organisation?

Refer to the explanation in the generic process.

Did the evaluation team have a suitable mix of disciplines?

Lupton et al. (1991, p. 361) suggest that the evaluation team should include design, operations and safety staff.

Was the evaluation team independent?

Refer to the explanation in the generic process.

6.1.1.1.3 Verification Resources

Refer to the questions and explanations in the generic process.

6.1.1.1.4 Verification Scope

Was the evaluation scope appropriate for the stage of the project at which it was performed?

Refer to the explanation in the generic process.

Did the evaluation include consideration of all appropriate scenarios?

An examination of past operational records may reveal new operating situations, or variations on them, for which new or changed allocations need to be made. For instance, evolutionary changes in the plant may have created or changed tasks, procedures and emergency scenarios.

Operating events should address the systems and functions identified and reflect the full range of plant operations, emphasising abnormal and emergency situations (NUREG 0800 Draft Rev. 0, 1996, p. 26). Problems identified in the operating experience review should also indicate operating events to include.

USNRC (1996c, p. 26) recommends that the following events should be included as a minimum:

- Normal events, e.g., start-up, shutdown, refuelling, changes in operating power.
- Failure events:
- Instrument failure.
- MMI equipment and processing failure.
- Transients and accidents:
- Transients, e.g., turbine trip, loss of off-site power, loss of feedwater, loss of power to selected busses.
- Accidents, e.g., main steam line break, loss of coolant.
- Reactor shutdown and cool-down using remote shutdown system.

The selected events should be relevant to the overall scope of the project, i.e., the events should include the MMI components being modified or designed. USNRC (1996c) gives further criteria for selection of events.

Did the utility include all relevant locations?

New or changed function allocations may be needed in several areas, such as new local control panels, rearranged MCR facilities, auxiliary shutdown facilities, etc. Advances in instrumentation, display systems, operator support systems, etc. will have effects on FA.

6.1.1.1.5 Verification Schedule Development

Refer to the questions and explanations in the generic process.

6.1.1.1.6 Verification Objectives

Did the utility define specific objectives for the verification of a topic?

A utility should be clear about the purposes and objectives of a verification exercise. This will also entail the development of specific pass-fail criteria for these objectives so that it can be shown whether a design has achieved its objectives. The verification of function allocation should include objectives to confirm that (IEC 964, 1989):

- All the functions necessary for achievement of plant operational and safety goals are identified.
- The proposed function assignment is in accordance with criteria established for assignment, including completeness.
- All the constraints on each function are identified, including performance aspects, those derived from safety principles, availability principles and station operating principles, those derived from other standards and regulations (see IEC, 1995a, p. 17).

- Workstation configurations are adequate to support tasks. Verification consists of comparing the design to the requirements from function analysis, e.g., instrumentation, displays, controls, other equipment (IEC, 1995a p. 17).
- Requirements resulting from higher and lower functional goals merge under all operational modes without conflict.

A top-down approach is recommended to ensure that all operator functions and tasks are considered (IEC, 1995a, p. 15). This starts with a review of all plant functional goals, supporting systems, sub-systems and their functions.

6.1.1.1.7 Verification Criteria

Did the utility develop criteria for the assignment of functions?

A utility should test each of its objectives against specific pass-fail criteria where possible. IEC (1989) suggests that criteria should be based on:

- Complexity of decision-making within time limits.
- Importance of decision-making for plant availability and safety.
- Necessity for enhancement of operator's capabilities in decision-making activities, e.g., diagnostic monitoring and high-level mental processing.

Criteria are also given in Table A.3 of this standard.

Lupton et al. (1991, p. 360) suggest:

- Performance — priority, accuracy, precision, execution time constraints.
- Complexity — number and sequence of control actions.
- Solution flexibility — the need for alternative solutions and the degree to which pre-defined solutions are available.
- Information-processing and storage
- Environmental considerations — sensitivity and tolerance to external and environmental factors
- Cost — implementation cost and operational cost

6.1.1.2 Evaluation

6.1.1.2.1 Verification Method

Did the utility develop and document a suitable method for verifying FA?

Supporting function analysis should produce a hierarchy under which the top-level functions represent the most general objectives of the plant operating staff. The lowest level set of functions and sub-functions must be assigned to person or machine using a described method (IAEA, 1995, p. 54).

USNRC (1996c, p. 27) recommends that the function analysis should include the systems associated with each selected operating event. The control of these functions should be described, giving the type of control response required from personnel (e.g., discrete, continuous) location of control interfaces (e.g., MCR, local panel), and associated displays. When control is allocated to both personnel and plant, the role of each should be described.

Lupton et al. (1991, p. 359) suggest the information that should be gathered for each identified function:

- The goal to be achieved for each function
- Performance measures for the function
- Entry conditions and constraints
- Ongoing constraints
- The set of control actions required, including alternative actions for performing the function
- Preferred sequence of control actions to be performed
- Completion criteria
- Side effects of performing the function
- Messages and alarms generated by the function

This information is also useful for detailed design work on the man-machine interface.

IAEA (1995, p. 56) recommends grouping the functions resulting from a function analysis into:

- Functions that must be automated — e.g., functions requiring rapid performance, high repeatability, or where the consequences of error are severe
- Functions that are better automated — e.g., lengthy tasks, functions requiring high accuracy or involving a degree of risk to the operator
- Functions that should be assigned to humans — e.g., those that require humanistic or inferential knowledge or flexibility, those that include tasks in extreme abnormal or accident situation where automation is difficult or impossible
- Functions that must be shared between humans and machines — e.g., where automation is used to detect and annunciate plant conditions, process information for the operator to make judgements and control actions

6.1.1.2.2 Verification Process

Was the review process satisfactorily documented and traceable?

The method used must be fully documented. The objective of the V&V team is to establish here that this method was followed (IAEA, 1995, p. 54). Functional

analyses need to be documented in hierarchical form and descriptively. Function allocations should be explicitly documented.

Were quantitative criteria defined and measured satisfactorily?

Refer to the explanation in the generic process.

6.1.1.2.3 Verification Results

Refer to the questions and explanations in the generic process.

6.1.1.3 Resolution

Refer to the questions and explanations in the generic process.

6.1.2 Validation of Function Analysis and Function Allocation

In validation of FA, the evaluation team assesses the correctness of the assignment (IEC 964, 1989, p. 83) for ensuring the optimum performance of person and machine together. The functional assignment should be validated in the functional design phase of the project to demonstrate that the system in question will achieve the functional goals. The output of the functional design stage is an input to the detailed specification of the system (IAEA, 1995).

Lupton et al. (1991, p. 359) and USNRC (1996c, p. 28) note that function allocation can usually be accepted to be based on operating experience, but that the basis for function allocation should be examined when:

- Significant problems are found with established allocations.
- An upgrade to the MMI could change some roles or introduce new ones.
- The design of the MMI or underlying process differs from predecessors and thereby introduces new or modified functions.

If any of these changes or problems is present (or is likely to be introduced by a project) the validity of the design is in question and needs to be demonstrated.

6.1.2.1 Preparation

6.1.2.1.1 Documents Used in Validation

Did the utility identify relevant source documents?

Some documents may have been updated as a result of verification. Documents relevant to FA may have been developed since earlier design stages or verification. Care should be taken to use the most up-to-date documents.

Was the evaluation team given access to applicable documents prior to the beginning of validation?

Refer to the explanation in the generic process.

Did the evaluation team have access to a human factors operating experience review?

Refer to the explanation in the generic process.

6.1.2.1.2 Validation Team

Refer to the questions and explanations in the generic process.

6.1.2.1.3 Validation Resources

Did the utility supply suitable resources for the evaluation team?

The facilities may need to include mock-ups and part-task simulators.

Were suitable working materials prepared?

Refer to the explanation in the generic process.

6.1.2.1.4 Validation Scope

Did the evaluation include consideration of all appropriate scenarios?

IEC (1995a, p. 23) states that events chosen for assessment should be representative. They should include all normal, emergency and accident conditions and events caused by a representative combination of multiple failures leading to maximum operator workload.

Was the evaluation scope appropriate for the stage of the project at which it was performed?

A suitable series of representative dynamic events should be used (IEC, 1995a, p. 23).

Did the utility include all relevant locations?

Refer to the explanation in the generic process.

6.1.2.1.5 Validation Schedule Development

Did the utility develop a suitable schedule for validation?

Refer to the explanation in the generic process.

6.1.2.1.6 Validation Objectives

Did the utility define specific objectives for the validation of a topic?

Refer to the explanation in the generic process.

6.1.2.1.7 Validation Criteria

Did the utility develop criteria for FA?

IEC (1995a, p. 21) states that the general criteria for validation that need satisfying are that:

- The number of functional goals and the workload rate of the control room staff shall not exceed their capability.
- The assignment of functions to control room staff and local operators is acceptable. In particular, it should not require them to perform co-operative, mutually dependent tasks for the achievement of a function that is either time-critical or important for safety or plant availability.

6.1.2.2 Evaluation

6.1.2.2.1 Validation Method

Did the utility develop and document a suitable method for validating a topic?

IEC (1995a, p. 23) states that validation can be done essentially on the basis of documentation. It suggests that, for isolated questions, experimental tests can be done with operators. Annex A of the standard contains descriptions of ways to evaluate and quantify the performance of functions and operator's workload.

6.1.2.2.2 Validation Process

Was the review process satisfactorily documented and traceable?

Refer to the explanation in the generic process.

Were quantitative criteria defined and measured satisfactorily?

Annex A of IEC (1995) contains suggestions for quantifying operator performance and workload.

6.1.2.2.3 Validation Results

Refer to the questions and explanations in the generic process.

6.1.2.3 Resolution

Were satisfactory resolutions developed and recorded for all deviations and non-conformities?

IEC (1995a, p. 25) suggests that corrective actions may be needed on:

- Selection of design alternatives.
- Refinements of functional requirements.
- Refinements of design criteria.

Were there checks for side effects of resolutions?

IEC (1995a, p. 25) suggests that the evaluation team may need a *'review of impact of changes on previous function assignment.'*

Did the evaluation team succeed in resolving issues, even when these arose late in the project?

Refer to the explanation in the generic process.

6.2 Task Analysis

Task analysis is an important part of the human factors contribution to the design process. Its results are used for a number of purposes. These include evaluation of function allocation, staffing and job design, procedure development, and display and control layout. It typically builds on the information resulting from the function analysis and allocation of function by grouping related areas of the above together into meaningful groups or tasks. The operators themselves perform these, or the operators supported by automatic or semi-automatic systems.

> Task analysis involves the study of what an operator (or team of operators) is required to do in order to achieve a system goal. The primary purpose of task analysis is to compare the demands of the system with the capabilities of the operator. If necessary those demands are altered, thereby reducing error and improving performance. (Kirwan & Ainsworth 1992, p. 15)

Other sources describe the objective of task analysis as:

> ... to identify the detailed components of a task and its characteristic measures. (IEC 967, 1989)

> ... the evaluation of the performance demands on plant personnel to identify the task requirements for accomplishing the functions allocated to them (Drury (1987) cited in NUREG-0711 (1994))

Feher et al. (1996) identify the objectives of task analysis as being to:

- Identify and organise operator tasks to achieve a specific operational goal.
- Establish the inter-relationships and sequence between tasks in support of the operational goals.
- Describe the operational properties of each task including their assignment to specific personnel.
- Describe the information needs of operators who are to perform the defined tasks.
- Provide the information in an organised framework to designers of control rooms, procedures, and training programmes.

Guidance on the role and processes involved in task analysis include: IEC 964 Appendix A, NUREG-0711 (1994) p. 5-1, NUREG 0700 (1996) Rev 1, Vol.1 p. 25-31. Kirwan and Ainsworth (1992) discuss the role of various task analysis techniques in the design process.

Job Analysis

A job analysis will often be required, as well as a task analysis, as a basis for job design, especially where a new facility rather than an upgrade is being designed. If a job analysis is required, it should be verified and validated in a similar way to related topics, such as function analysis and task analysis.

A job analysis is used with the results of function analysis and assignment and task analysis as an information source for design of the control room staff structure, operating procedures and training programme (Berggren, personal communication). A job analysis should be conducted on the basis of the verified and validated function assignment and functional requirements. Function analysis, task analysis and job analysis, as major activities in functional design, have a significant influence on other topics.

A job analysis is also recommended by IEC 964 (1989). The analysis should clarify:

- Operator competence required
- Operational responsibilities of operators
- Non-operational duties of operators, e.g., reporting
- Operational interactions between operators
- Dialogues between operators and plant
- Communications between operators and plant personnel stationed outside the control room facilities

Job analysis begins with the identification of the number and characteristics of tasks assigned to person in a function assignment and the information on these in the task analysis. The number and organisation of operators can then be defined, taking regard of legal requirements and the normal practice of the utility. Lupton et al. (1991, p. 362) classify and describe a preliminary job analysis as part of their functional design methodology.

The results of a task analysis, function analysis and function allocation can be used in job analysis in several ways. Firstly, the content of jobs should be indicated by the analyses. Secondly, the skills of training required for jobs should be clearer. The analyses should also help with defining team responsibilities, relationships and communication requirements. Task analysis can also be used to help decide whether the definitions of jobs should be changed or enlarged, or where tasks need making into a more coherent job.

The collection of tasks assigned to an operator must allow the person to maintain an adequate level of performance under all circumstances. Conversely, operators should not be under-loaded. Previous function assignment must therefore take account of the whole job of an operator, not just individual tasks and responsibilities (IAEA, 1995, p. 57).

Tasks may be shared between operators in a group or in a team, but this should not be arbitrary. The role of each person must be defined. Where teamwork is required, communication and working structures will need to be considered (IAEA, 1995, p. 57). The job design can also affect training requirements: a change to existing roles may require retraining (IEEE, 1988, p. 13).

6.2.1 Verification of Task Analysis

6.2.1.1 Preparation

6.2.1.1.1 Documents Used in the Verification

Did the utility identify relevant source documents?

The evaluation team should have ensured that appropriate information sources for the task analysis were available. As task analysis requires the integration of information from many sources it is important that these are of an appropriate level of detail and breadth of coverage for the needs of the analysis. An example of the types of documentation that could serve as input to the analysis is presented in NUREG-0700 (1996), Rev1, Vol. 1 pp. 25-26. This also includes both plant system documentation and guidance on the various task analysis methods used. Information from operators serves a vital role in the development of many forms of task analysis and this aspect should be fully accounted for.

Was the evaluation team given access to applicable documents prior to the beginning of verification?

It should be demonstrated that all the appropriate, up to date information sources, were available to the evaluation team during the verification process.

Did the evaluation team have access to a human factors operating experience review?

Refer to the explanation in the generic process.

6.2.1.1.2 Verification Team

Did the utility have a suitable design and evaluation team for the task analysis?

The evaluation team should have the expertise to check several things: the selection of the task analysis technique, its application, the information sources, the recording and documentation, the use to which the information from the analysis will be put.

Was the evaluation team suitably placed in the licensee's organisation?

Refer to the explanation in the generic process.

Did the evaluation team have a suitable mix of disciplines?

The evaluation team should be composed of personnel with the appropriate expertise and experience to review these important aspects of task analysis process and results. For example, a combination of engineering, operational, and human factors expertise would be the minimum required to evaluate the task analysis. Specific requirements for experience in the application of task analysis techniques and appreciation of human information processing factors would be an advantage.

Was the evaluation team independent?

The evaluation team should be able to demonstrate its independence from the designers.

6.2.1.1.3 Verification Resources

Did the utility supply suitable resources for the evaluation team?

Task analysis is itself a resource intensive process, and a thorough evaluation of its processes and results no less so. The evaluation teams requirements for suitable resources to carry out the evaluation e.g. access to appropriate personnel, possible external expertise, appropriate time for the evaluation and the implications of its findings, should be demonstrated.

Were suitable working materials prepared?

The evaluation team should have a set of procedures, documentation, and processes for dealing with the verification of the task analysis. These should be complete, appropriate, and been demonstrated to have functioned.

6.2.1.1.4 Verification Scope

Did the utility include all relevant locations?

Whilst many of the tasks analysed will be located in the MCR, the evaluation team should have ensured that all locations and communication interfaces outside the MCR were also considered and included in the analysis.

Did the utility scope the evaluation appropriately?

The evaluation team should have ensured the task analysis was applied to an appropriate set of representative and important tasks. These should cover operations, maintenance, test, inspection, and surveillance across the full range of operating modes. (NUREG-0711 (1994) pg. 5-1)

6.2.1.1.5 Verification Schedule Development

Did the utility develop a suitable schedule for verification?

The evaluation team should be guided by a plan for human factors activities and V&V of them (NUREG-0711, 1994a, Glenn et al., 1985). This should detail the time requirements, relations and dependency between the tasks within the evaluation process. The schedule should extend throughout the whole project's duration. The responsibilities and functions of the team members should be defined. The schedule should be developed during the preparation phase of a project (IEC 1771, 1995a).

Did the utility develop a plan or schedule for verification of the task analysis?

The existence of that part of the plan making provisions for the verification of the task analysis should have been established. The evaluation team should have considered the appropriateness of the schedule and its provisions.

6.2.1.1.6 Verification Objectives

Did the utility define specific objectives for the verification of the task analysis?

A set of objectives specific to the verification of the task analysis process and results should be developed. These should reflect the capabilities of the technique(s) used and role that the results will have in the design process. For example, verification should establish that the task analysis has:

- Defined personnel task requirements, see NUREG 0700 (1996) p. 28-30.
- Included information from plant personnel to reflect operational needs and experience.
- Reflected an appropriate (to the level of modification) range of functions and events met, see NUREG 0700 (1996) p. 26-27.

6.2.1.1.7 Verification Criteria

Did the utility develop criteria for the task analysis?

Criteria for the verification of the process for carrying out the task analysis, and its results, should have been established by the evaluation team. The appropriateness and application of the criteria for accepting the task analysis as verified should be considered. The evaluation team should be able to demonstrate that the criteria developed have been applied and the analysis evaluated against them.

6.2.1.2 Evaluation

6.2.1.2.1 Verification Method

Did the utility develop and document a suitable method for verifying the task analysis?

The utility must state how the task analysis was assessed. Appropriate design guidance and methods for this should have been consulted. The method should be documented such that it is both fully described and justified.

6.2.1.2.2 Verification Process

Was the review process satisfactorily documented and traceable?

The correspondence between the methodology for reviewing the task analysis and how that review has been carried out in practice should be demonstrated and recorded.

Were quantitative criteria defined and measured satisfactorily?

The review process should have, if possible, developed quantitative measures for reviewing the task analysis.

6.2.1.2.3 Verification Results

Were the review results recorded satisfactorily, including deviations, non-conformities and assessment against criteria?

Evidence should be provided that all aspects of the review of the task analysis have been recorded and presented in a manner appropriate for its representation,

evaluation, and later use. The evaluation team should ensure that the records are clear. They should document each instance where the review methodology deviated from that prescribed or where the task analysis failed any of the criteria used in the evaluation.

6.2.1.3 Resolution

Were satisfactory resolutions developed and recorded for all deviations and non-conformities?

Refer to the explanation in the generic process.

Were there checks for side effects of resolutions?

The evaluation team would be expected to clearly demonstrate that the full implications of changing any part of the task analysis process or its results have been considered. For example, changes in a task, or its characteristics, might influence several other aspects such as personnel requirements, allocation of function, etc. The implications for these changes should be fully documented and traceable.

6.2.2 Validation of Task Analysis

6.2.2.1 Preparation

6.2.2.1.1 Documents Used in Validation

Did the utility identify relevant source documents?

Following verification of the task analysis documents or the task analysis may have been updated. These should be available prior to the validation of the task analysis.

Was the evaluation team given access to applicable documents prior to the beginning of validation?

It should be demonstrated that all the appropriate, up to date information sources, were available to the evaluation team during the validation process. Previous operating experience has an important role in establishing the scope, and need for task analysis and should have been accounted for where necessary.

Was the evaluation team given access to applicable documents prior to the beginning of verification?

Refer to the explanation in the generic process.

6.2.2.1.2 Validation Team

Did the utility have a suitable design and evaluation team for the task analysis?

The evaluation team should have the necessary expertise to conduct the validation tests at an appropriate level of fidelity.

Was the evaluation team suitably placed in the licensee's organisation?

Refer to the explanation in the generic process.

Did the evaluation team have a suitable mix of disciplines?

In addition to the needs for verification, extra operational experience is important for validating the task analysis; as is experience with the development and running of such tests in mock-ups and simulators.

Was the evaluation team independent?

Refer to the explanation in the generic process.

6.2.2.1.3 Validation Resources

Did the utility supply suitable resources for the evaluation team?

Dependant on the design stage, validation requires the use of resources and facilities of varying sophistication and fidelity. The evaluation team have been provided with

sufficient resources to ensure that validation exercises were carried out as early in the process as possible to an appropriate level of fidelity.

Were suitable working materials prepared?

Refer to the explanation in the generic process.

6.2.2.1.4 Validation Scope

Was the evaluation scope appropriate for the stage of the project at which it was performed?

The scope of the validation must be appropriate to the level of validation required. The evaluation team should have considered possibility to validate parts of the task analysis before the final integrated testing using table top techniques and later, using part whole mock-ups.

Did the evaluation include consideration of all appropriate scenarios?

The evaluation team should have ensured that validation of the task analyses was applied to an appropriate set of representative and important tasks from the area of operations, maintenance, test, inspection, and surveillance across the full range of operating modes. (NUREG-0711 (1994, p. 5-1).

Did the utility include all relevant locations?

Refer to verification.

6.2.2.1.5 Validation Schedule Development

Refer to the questions and explanations in the generic process.

6.2.2.1.6 Validation Objectives

Did the utility define specific objectives for validation of a task analysis?

A set of objectives specific to the validation of the task analysis process and results should be developed. These should establish that the objectives identified in the verification exercise have been validated, at a level of fidelity required for the design stage at which the validation exercise is being carried out. For example, talk-through, walk-through and low fidelity mock-ups can be used to validate task analysis earlier in the design process.

6.2.2.1.7 Validation Criteria

Did the utility set criteria for validating the task analysis under review?

The evaluation team should have established criteria for the validation of the task analyses. The appropriateness and application of the criteria for validating the task analysis should be considered. The evaluation team should be able to demonstrate that the criteria developed have been applied and the analysis evaluated against them.

6.2.2.2 Evaluation

6.2.2.2.1 Validation Method

Did the utility develop and document a suitable method for validating a topic?

Refer to verification.

6.2.2.2.2 Validation Process

Was the review process satisfactorily documented and traceable?

Refer to verification.

Were quantitative criteria defined and measured satisfactorily?

Refer to verification.

6.2.2.2.3 Validation Results

Were the review results recorded satisfactorily, including deviations, non-conformities and assessments against criteria?

Refer to verification.

6.2.2.3 Resolution

Were satisfactory resolutions developed and recorded for all deviations, non-conformities?

For each discrepancy identified, a documented record should exist detailing and justifying the action taken to rectify or accept the discrepancy.

Were there checks for side effects of resolutions?

The implications of the actions taken to rectify or accept the discrepancy should be considered and recorded.

Did the evaluation team succeed in resolving issues, even when these arose late in the project?

Refer to the explanation in the generic process.

6.3 Space and Configuration

'Space and Configuration' relates to the design of work areas, the grouping of operating areas, storage space, control panel arrangement, size, shape of and relationships between major items of control room equipment such as desks, chairs, panels and boards. (It does not cover arrangement of components within individual control panels and consoles, control and display device layout, interface designs such as graphical formats, etc. These are covered in sections on 'Control and Display Layout' and 'VDU Displays'.)

Even if an operator's immediate workspace is adequately designed in terms of displays, controls, and consoles, the entire working environment, holding people and machines, still needs to be arranged. Physical factors need to be considered, such as movement between items of equipment and the mobility of operators. The social relationships and team working of operators also need to be examined, since the physical arrangement can influence the effectiveness of communication, co-operation, problem solving, etc. Once designed and installed, a poor layout cannot easily be changed. Therefore, careful planning is essential prior to implementing a design.

The identification of basic plant functions (function analysis) and the subsequent review of their allocations (function allocation) serve as inputs to the early generation of a conceptual layout of a control room or other facility. The layout will show panels and workstations in an appropriate arrangement with a list of basic functions attached to each. Using this, the main concepts of the control room can be built up so that it can be further refined (IAEA, 1995, p. 59).

The design of the control room layout should take into account several factors, such as:

- The type of plant.
- The degree of automation.
- The manufacturers of the systems.
- The operational strategy.
- The operator team structure.

Generally, the layout corresponds to the operator team structure. Control room panels are generally divided into main systems, such as NSSS, BOP, safety systems, electrical systems, auxiliary systems. These are often divided into areas for 1) steady state power operation, shutdown, and early diagnosis during abnormal situations 2) NSSS auxiliary control boards 3) turbine-generator auxiliary control boards (IAEA, 1995, p. 28).

It is recommended that space considerations should be considered early in a project (IAEA, 1995, p. 65). There may be space consequences of modifications to data acquisition systems, computer rooms and the control room and there may also be effects on lighting, ventilation and other environmental requirements.

Brown et al. (1996) provide guidance for reviewing local control stations, including issues of space and configuration. These are multi-function panels, valves, switches,

breakers, displays, etc. that are operated outside the MCR during normal, abnormal and emergency operations.

Location, Environment and Protection

As well as the space and configuration within the control room, it may also be important to consider the location, environment and protection of the control room. Especially if a new facility is being designed, this may be sufficiently important for consideration as a topic for verification and validation in its own right.

If the project is a back-fit design, IAEA (1995, p. 65) recommends that implications for location, environment and protection should be studied in an early phase of the project. The design team should examine the effect on location, environment and protection of modifications to data acquisition systems and to computer rooms and the control room. If the effects on location, environment and protection are likely to be minimal, and it is possible to justify these aspects of the new design by arguments of similarity, then the subject may not warrant separate treatment.

Part of the human factors work in any design process should be to contribute to the selection and design of working locations, the physical environment, and the protection (LEP) given for human occupancy and use. The control room (or other facility) needs to be appropriately sited for its intended use and should meet safety principles. The environment should be provided in such a way that the operators can perform their tasks efficiently, comfortably and safely. In addition, there may be special requirements for verifying and validating operability in emergency conditions, including protection for hostile conditions. Such issues are not solely human factors concerns.

There will often be a common control room for multiple units at the same site, though separate control rooms have been developed at some plants. Some utilities have found that their operating staff members perform better if they are organised into teams largely dedicated to separate units (IAEA, 1995a, p. 28).

The specifications and designs of the location, environment and protection that should be subject to V&V are discussed in International Electrotechnical Commission (1989) A.4.2.2. Protection issues could include fire, radiation and hostile acts. International Electrotechnical Commission (1989) A.4.2.3 describes these.

According to IEEE (1988) LEP considerations include:

- Temperature, airflow and humidity — When conditions fall outside comfort zones, human performance is affected either by reduced comfort or, in the extreme, by physiological effects. In addition, low humidity control rooms can produce static electricity, which may disrupt instrumentation.
- Illumination— Certain kinds and ranges of ambient light are best suited to particular activities. Lighting problems such as glare, contrast or illumination variation can affect performance. Lighting provides illumination for tasks and may be varied for different purposes, such as reading gauges, avoiding glare and reflection on VDUs, reading procedures and drawings.

- Acoustics and sound — ambient sound can have direct physiological effects, such as masking, and performance effects, such as interference with warning signals and communications. It can also cause discomfort or hearing damage in the long term. Sources are human traffic in the control room, alarms, printers, paging loudspeakers, ventilation equipment.
- Workplace size, geometry and layout — Human performance can be affected in relation to the tasks being performed and the number of personnel involved in the area. Adequate space is needed to accommodate the expected number of personnel in the workplace, allowing for normal movement and traffic patterns. Workstations, panels, etc. need to be configured so that operators can reach required items and communicate with other staff.

The last of these are covered in detail in the present section. Additionally, habitability features, such as personal convenience, space, aesthetic considerations, safeguards against common hazards, etc. are specified to promote personnel comfort, morale and safety (IAEA, 1995, p. 40).

It may not be possible to verify some design aspects which come under the heading of 'environment', such as MCR lighting and noise, before the final stages of a project (USNRC, 1996). These may need to be verified and validated with the final installed design.

6.3.1 Verification of Space and Configuration

It needs to be verified that the control room has sufficient space. Equipment needs to be configured correctly in relation to other items and staff so that staff can perform adequately in normal and abnormal situations.

6.3.1.1 Preparation

6.3.1.1.1 Documents Used in Verification

Did the utility identify relevant source documents?

International Electrotechnical Commission (1989) lists some issues that create requirements that should be verified. Documentation dealing with these should be available to the design team and the evaluation team for verification:

- station's operating principles.
- assignments of functions.
- centralised or local control philosophy.
- supervision criteria.
- plant and technological choices.
- station operating authority and legal requirements.

Was the evaluation team given access to applicable documents prior to the beginning of verification?

The team may need access to architect's drawings, preliminary control room designs, plans of previous control rooms, etc.

Did the evaluation team have access to a human factors operating experience review?

The OER can suggest the need for modifications to layout or access to control equipment.

6.3.1.1.2 Verification Team

Did the utility have a suitable evaluation team for the topic?

Team members with drafting or drawing skills may be needed to build mock-ups or models. CAD skills may be needed for scale drawings, computer models.

Was the evaluation team suitably placed in the licensee's organisation?

Refer to the explanation in the generic process.

Did the evaluation team have a suitable mix of disciplines?

Refer to the explanation in the generic process.

Was the evaluation team independent?

Refer to the explanation in the generic process.

6.3.1.1.3 Verification Resources

Did the utility supply suitable resources for the evaluation team?

The evaluation team may need access to the tools used by the design team, such as mock-ups and models used to resolve access, workspace and related problems.

Were suitable working materials prepared?

Refer to the explanation in the generic process.

6.3.1.1.4 Verification Scope

Was the evaluation scope appropriate for the stage of the project at which it was performed?

Refer to the explanation in the generic process.

Did the evaluation include consideration of all appropriate scenarios?

Refer to the explanation in the generic process.

Did the utility include all relevant locations?

Space and configuration may be more likely to be inadequate in other locations than the central control room. For instance, locations where valves, switchgear, etc. are

manipulated manually, on rare occasions, are often found to have inadequate provisions for access and operation. This is especially true for maintenance operations.

6.3.1.1.5 Verification Schedule Development

Refer to the questions and explanations in the generic process.

6.3.1.1.6 Verification Objectives

Did the utility define specific objectives for the verification of space and configuration?

IEC (1989, p. 31) gives objectives for space and configuration:

- Space:
- The control room should have sufficient space to perform all necessary actions while minimising operator movement in abnormal situations.
- Configuration:
- The control room space and configuration should take into account constraints from, for example, station operating principles, function assignment, control philosophy, supervision criteria, plant and technological choices, legal requirements.
- The control room should have necessary operating areas for information and controls to perform the tasks assigned to operators in all operational and accident conditions.
- The operating area and equipment should be arranged according to human factors principles (A.4.3.2 contains requirements for grouping, size and shape).
- The arrangement should be structured to simplify system and component identification and to minimise the possibility of human error.
- The arrangement should be consistent for all operating areas.

6.3.1.1.7 Verification Criteria

Did the utility develop criteria for the human factors topic?

See previous question. A.4.3 of IEC (1989) contains criteria covering:

- Space for work areas.
- Grouping of operating areas.
- Control boards and arrangement.
- Size and shape.

Oborne (1987, p. 188 ff.) notes several considerations for which criteria should be developed, for example,

- Anthropometric considerations — passageways, space between equipment items.
- Movement considerations — gross body movement times between items.
- Visual considerations — visual contact between an operator, other items of equipment and other staff.
- Visual strain — especially in relation to the placement of VDUs.
- Auditory considerations — communication with other staff, proximity to noise sources.
- Personal space.

6.3.1.2 Evaluation

6.3.1.2.1 Verification Method

Did the utility develop and document a suitable method for verifying a topic?

Ministry of Defence, UK, (1989) gives several methods for carrying out design work that could also be used to verify that objectives and criteria have been met:

- Paper mock-ups — used to generate alternative layouts in two dimensions.
- 3-D mock-ups — used to evaluate clearance, fit, reach, sight-lines, etc.
- Scale drawings — used to depict initial detailed design.
- Full-scale mock-ups and models — the simplest mock-ups and models must be delivered as early as possible to have the greatest value.

Mock-ups and models are valuable throughout the whole design process to verify and validate designs. They also are useful for obtaining comments from future users, the client, etc. Computer models, both 2-D and 3-D may be of similar use to physical models, and may offer advantages in adaptability.

6.3.1.2.2 Verification Process

Was the review process satisfactorily documented and traceable?

Refer to the explanation in the generic process.

Were quantitative criteria defined and measured satisfactorily?

For example, criteria for spacing between major items, circulation space, etc. can be defined quantitatively.

6.3.1.2.3 Verification Results

Refer to the questions and explanations in the generic process.

6.3.1.3 Resolution

Refer to the questions and explanations in the generic process.

6.3.2 Validation of Space and Configuration

It needs to be established that the proposed design of the workplace and the layout of the systems within it function following their intended purpose. The purpose should be to allow staff to perform all necessary actions while minimising operator movement in abnormal conditions (IEC 964, 1989, p. 31).

6.3.2.1 Preparation

6.3.2.1.1 Documents Used in Validation

Did the utility identify relevant source documents?

Refer to the explanation in the generic process.

Was the evaluation team given access to applicable documents prior to the beginning of validation?

Refer to the explanation in the generic process.

Did the evaluation team have access to a human factors operating experience review?

For instance, an OER may reveal occasions during emergency situations or training exercises when:

- The control room space was inadequate for the number of personnel who need to use it.
- The emergency communications equipment was not located suitably relative to other equipment used early in an emergency scenario.

6.3.2.1.2 Validation Team

Did the utility have a suitable evaluation team for the topic?

Specialist skills may be needed to use and modify mock-ups and to evaluate whether models are able to validate a design.

Was the evaluation team appropriately placed in the licensee's organisation?

Refer to the explanation in the generic process.

Did the evaluation team have a suitable mix of disciplines?

The team may need some specialist skills to use and modify any mock-ups developed for the design and V&V work.

Was the evaluation team independent?

Refer to the explanation in the generic process.

6.3.2.1.3 Validation Resources

Refer to the questions and explanations in the generic process.

6.3.2.1.4 Validation Scope

Did the evaluation include consideration of all appropriate scenarios?

Some emergency scenarios may require equipment to be accessed that is not usually accessed during normal operations. For instance, automatic equipment may have to be manipulated manually in some failure scenarios. It is often these locations that are overlooked and that are inaccessible or difficult to work in, especially if the access required is for maintenance rather than operations.

Was the evaluation scope appropriate for the stage of the project at which it was performed?

At early stages, validations can be desktop exercises using models, computerised tools, etc. At later stages, full-scale mock-ups should be expected.

Did the utility include all relevant locations?

Refer to the explanation in the generic process. See also question above on scenarios.

6.3.2.1.5 Validation Schedule Development

Did the utility develop a suitable schedule for validation?

Refer to the explanation in the generic process.

6.3.2.1.6 Validation Objectives

Did the utility define specific objectives for the validation of a topic?

For example, the tests may wish to show that the space and configuration of a control room where extra equipment has been installed is still valid for the users.

6.3.2.1.7 Validation Criteria

Did the utility develop criteria for the human factors topic?

There is considerable scope for quantitative criteria, such as dimensions for circulation, sight lines and visual angle.

6.3.2.2 Evaluation

6.3.2.2.1 Validation Method

Did the utility develop and document a suitable method for validating a topic?

As standard, also see verification question.

6.3.2.2.2 Validation Process

Was the review process satisfactorily documented and traceable?

Validation should include scale drawings and other layout documentation where appropriate.

Were quantitative criteria defined and measured satisfactorily?

It should be possible to develop several quantitative criteria for space and configuration, such as clearances between major items, circulation routes. A validation test establishes whether these criteria are adequate in practice.

6.3.2.2.3 Validation Results

Were the review results recorded satisfactorily, including deviations, non-conformities and assessments against criteria?

Certain deviations can be recorded quantitatively, such as the dimensions for arrangement, spacing and sight lines. Other non-conformities may be qualitative.

6.3.2.3 Resolution

Were satisfactory resolutions developed and recorded for all deviations and non-conformities?

Refer to the explanation in the generic process.

Were there checks for side effects of resolutions?

For instance, changes to arrangements to accommodate the circulation of personnel may affect the sight lines of operators.

Did the evaluation team succeed in resolving issues, even when these arose late in the project?

If a full-scale mock-up or similar aid has been used from as early as possible, expensive changes are less likely to be needed. Conversely, a mock-up can be used to demonstrate certain weaknesses to sceptical project staff. Examples are poor sight lines, inadequate personal space, inability of two operators physically to share a display, possibility of inadvertent activation of controls by passing personnel.

6.3.3 Supplementary References

Brown, W.S., Higgins, J.C., O'Hara, J.M. (1996) *Local Control Stations: Human Engineering Issues and Insights*, Washington, DC: USNRC (NUREG/CR-6146)

Ministry of Defence, UK (1989) *Human Factors for Designers of Equipment. Part 4: Workplace Design.* Glasgow: Ministry of Defence, Directorate of Standardisation (Interim DEF STAN 00-25 (Part 4)/1)

Oborne, D.J. (1987) Ch 8: Workplace Design. In: *Ergonomics at Work.* 2nd Ed. New York: John Wiley.

6.4 Displays and Controls

This section covers the design of all types of displays and controls. However, with the increasing use of computerised support systems, integrated displays, large screen display devices, etc. in modern control rooms (or upgraded facilities) we have put particular emphasis in our examples on VDU displays. More conventional components, such as levers, switches, illuminated buttons, digital displays and gauges, can be designed, verified and validated with reference to the large amount of design information in standard ergonomics sources.

Design issues and guidance specific to NPP control rooms may override or extend general human factors information on controls and displays. For instance, important topics in their own right could be the design of VDU-based display systems, alarm systems, and control panels for nuclear plant. Therefore, wherever possible, documentation, guidance, specifications, etc., for specific systems should be used in preference to general information. For example, USNRC (1996b) contains guidance for advanced designs of control rooms, which may contain either hybrid designs, or totally computer-based monitoring and control systems. NUREG/CR-5908 contains procedures and guidance for reviewing computer-based HSIs, NUREG/CR-6105 contains guidance for reviewing alarm systems, and NUREG/CR-6146 has guidance for local control stations. USNRC (1996b) Department of Defense (1981) contains a large amount of design data for 'traditional' controls and displays. Note that dimensions and anthropometry in such handbooks may need to be validated for the population being designed for.

VDU displays themselves are the subject of several standards and textbooks, including IEC 1772 (1995b) which is a supplementary standard to IEC 964 and supersedes the information given in Appendix A of IEC 964 (1989). It presents design requirements for the application of VDUs in MCRs of NPPs. The standard is intended to apply to new control rooms. If it is applied to existing control rooms, care should be taken, as some assumptions may not apply.

IEC 1772 (1995b) assists the designer in optimising performance with VDUs that are used together with, or instead of, conventional displays. (The latter are covered here in the section 'Controls and Displays'.) The standard contains:

- Requirements for the clear statement of information needs
- Requirements for good presentation
- Methods for quick and easy access to information
- Design criteria

The standard refers to the design process given in IEC 964 (1989).

Arrangement and layout of displays and controls should be based on consideration and trade-offs of several principles. The first four of the examples below are from Sanders and McCormick (1992) and the remainder is based on Pheasant (1988):

- Importance — important components should be placed in convenient locations

- Frequency of use — frequently used components should be placed in convenient locations
- Functional grouping — of displays and controls that are functionally related in the operation of a system. For instance, electrical power distribution displays and controls can be grouped at the same location.
- Sequence of use — the arrangement can take advantage of frequently occurring sequences and patterns of use
- Check-reading — where several similar displays are to be scanned or monitored, arrange all indicators to be in the same alignment in the neutral or safe condition
- Labelling — all labels should be positioned in the same relationship to the components they describe
- Workload — distribute workload between both hands
- Separated relationships — where related controls and displays are physically separate (e.g., on vertical and horizontal panels) their arrangement should be as similar as possible

Verification of control and display layout consists of establishing that the design meets ergonomic criteria and principles established for control and display layout for a project. Since this is a comparatively well developed subject within ergonomics, the collection of human factors knowledge used for a utility's project will have extensive information on the subject.

Most of the examples that follow (applications of V&V to controls and displays) use VDU displays as examples.

6.4.1 Verification of Displays and Controls

6.4.1.1 Preparation

6.4.1.1.1 Documents Used in Verification

Did the utility identify relevant source documents?

There are specialist standards and ergonomic guidelines dealing with VDU displays. Proposed designs should be verified against the documents chosen for the project. The design documentation should identify the intended purpose and applications, principal users, failure criteria, system capabilities, information needs and application procedures and design and implementation (IEC 1772, 1995b).

Was the evaluation team given access to applicable documents before the beginning of verification?

Refer to the explanation in the generic process.

Did the evaluation team have access to a human factors operating experience review?

Refer to the explanation in the generic process.

6.4.1.1.2 Verification Team

Did the utility have a suitable design and evaluation team for the topic?

The evaluation team may need special skills, e.g., in the use of CAD tools for process mimics.

Was the evaluation team suitably placed in the licensee's organisation?

Refer to the explanation in the generic process.

Did the evaluation team have a suitable mix of disciplines?

Refer to the explanation in the generic process.

Was the evaluation team independent?

Refer to the explanation in the generic process.

6.4.1.1.3 Verification Resources

Did the utility supply suitable resources for the evaluation team?

For example, the evaluation team may need access to the CAD tools or other aids used to design mimics and displays. A practical example of verification is given in Annexe E of IEC 1772 (1995b).

Were suitable working materials prepared?

Refer to the explanation in the generic process.

6.4.1.1.4 Verification Scope

Was the evaluation scope appropriate for the stage of the project at which it was performed?

A VDU-based system brings together static and dynamic information; both aspects need to be verified. Repeated test should preferably be carried out over the full range of conditions on a full-scope simulator. This should take place at the construction stage, if available. It may be necessary to defer some tests to the commissioning stage (IEC 1772, 1995b, p. 41). There may need to be checks, for instance, that mimics designed on the development system have been transferred successfully to the delivery system.

Did the evaluation include consideration of all appropriate scenarios?

The verification should be carried out for a set of operational states including abnormal states and fault configurations (IEC 1772, 1995b, p. 27). Some information, or even complete formats, is helpful in all situations (That is, not scenario-specific.) These may be displayed continuously or included as constituents

of the most important format sets (IEC 1772, 1995b, p. 27). These should be verified as far as possible.

Did the utility include all relevant locations?

Refer to the explanation in the generic process.

6.4.1.1.5 Verification Schedule Development

Refer to the questions and explanations in the generic process.

6.4.1.1.6 Verification Objectives

Did the utility define specific objectives for the verification of a topic?

IEC 1772 (1995b) states that the VDU application system should be designed so that operators can perform their tasks correctly and promptly. Account should be taken of the relationship between the information presented and any associated controls.

6.4.1.1.7 Verification Criteria

Did the utility develop criteria for the human factors topic?

IEC 1772 (1995b, p. 27) states that the general verification criteria should follow the requirements given in 3.3 and 5.1 of IEC 964 and IEC 1771. There are also criteria in A.4.1, 4.4, 4.5 and A.4.5 of IEC 964 (1989).

6.4.1.2 Evaluation

6.4.1.2.1 Verification Method

Did the utility develop and document a suitable method for verifying a topic?

Example verification is given in Annexe E of IEC 1772 (1995b). The example suggests that the verification may need to consist of a series of tests:

- in a computer centre
- specified test sequences during implementation
- knowledge-based laboratory tests by the designer
- use of a full-scope simulator
- on site
- tests of all signals to the system
- supervising tests by commissioning engineers
- documentation of commissioning tests

6.4.1.2.2 Verification Process

Was the review process satisfactorily documented and traceable?

The design should document a clear definition of the purpose of the displays, their safety role and their basic performance requirements (IEC 1772, 1995b).

Were quantitative criteria defined and measured satisfactorily?

Refer to the explanation in the generic process.

6.4.1.2.3 Verification Results

Refer to the questions and explanations in the generic process.

6.4.1.3 Resolution

Were satisfactory resolutions developed and recorded for all deviations and non-conformities?

Refer to the explanation in the generic process.

Were there checks for side effects of resolutions?

Special attention should be given to consistency of information that is displayed at several locations at the same time (IEC 1772, 1995b, p. 27).

6.4.2 Validation of Displays and Controls

6.4.2.1 Preparation

6.4.2.1.1 Documents Used in Validation

Did the utility identify relevant source documents?

Refer to the explanation in the generic process.

Was the evaluation team given access to applicable documents prior to the beginning of validation?

IEC 1772 (1995b, p. 43) states that the validation should take into account the verification, especially the completeness of required functions, signals, formats and format sets.

Did the evaluation team have access to a human factors operating experience review?

For example, an OER may reveal where existing lighting designs have been found to give poor performance with newly installed VDU display systems, or where hierarchies of displays are confusing to navigate.

6.4.2.1.2 Validation Team

Refer to the questions and explanations in the generic process.

6.4.2.1.3 Validation Resources

Did the utility supply suitable resources for the evaluation team?

The validation team may need access to both the tools used to develop displays, and the process monitoring system used to present displays. (The latter may not have been available at the time of design.) IEC 1772 (1995b, p. 43) states that it may be beneficial to use a full-scope simulator as the main validation tool.

Were suitable working materials prepared?

Refer to the explanation in the generic process.

6.4.2.1.4 Validation Scope

Did the evaluation include consideration of all appropriate scenarios?

Key format-sets or information that is relevant in all scenarios should be validated as far as possible (IEC 1772, 1995b, p. 27). Validation should be carried out with representative operational scenarios, disturbed situations and accident conditions and information goals for different users of the system (IEC 1772, 1995b, p. 27).

Was the evaluation scope appropriate for the stage of the project at which it was performed?

The system (i.e., CAD package, drawings, and documentation) that was used to develop displays may need to be used for validation work early in a project. Later, validation will be necessary on the final VDU display system.

Did the utility include all relevant locations?

Refer to the explanation in the generic process.

6.4.2.1.5 Validation Schedule Development

Refer to the questions and explanations in the generic process.

6.4.2.1.6 Validation Objectives

Did the utility define specific objectives for the validation of a topic?

IEC 1772 (1995b, p. 43) states that the validation procedure should be concentrated on well-specified goals and the key formats of highest information content and abstraction.

6.4.2.1.7 Validation Criteria

Did the utility develop criteria for the human factors topic?

Validation criteria should follow the requirements given in 3.3 and 5.2 of IEC 964 (1989), IEC 1771 (1995a) and Annexe E of IEC 1772 (1995b, p. 27).

6.4.2.2 Evaluation

6.4.2.2.1 Validation Method

Refer to the questions and explanations in the generic process.

6.4.2.2.2 Validation Process

Was the review process satisfactorily documented and traceable?

The validation process should follow the requirements given in 3.3 and 5.2 of IEC 964 and IEC 1771 (1995a) and Annexe E of IEC 1772 (1995b, p. 27).

Were quantitative criteria defined and measured satisfactorily?

Refer to the explanation in the generic process.

6.4.2.2.3 Validation Results

Refer to the questions and explanations in the generic process.

6.4.2.3 Resolution

Were satisfactory resolutions developed and recorded for all deviations and non-conformities?

Refer to the explanation in the generic process.

Were there checks for side effects of resolutions?

Time delays caused by scanning or pre-processing should be reviewed, documented and assessed regarding consequences (IEC 1772, 1995b, p. 27).

Did the evaluation team succeed in resolving issues, even when these arose late in the project?

Refer to the explanation in the generic process.

6.5 Communications Systems

Communication system design influences the efficiency and effectiveness by which personnel exchange information. The focus is on communications between operators and personnel at remote locations, such as LTP operators (IAEA, 1995a, p. 41). Reasons for communication include exchange of advice, verification of information, exchange of instructions, gathering of information from remote indications and investigations of abnormal situations. Usually, information must be communicated quickly, without interference or distortion.

Communications systems typically include paging, telephones, radios, faxes and computer networks. A good system allows selection of who will receive and send messages, provides alerting for incoming messages and provides sufficient and suitable channels for exchanging information.

The major requirement is to satisfy the communication needs identified from task analysis and other operational requirements. There may also be other needs, such as personnel and security needs, requirements for site warnings, public address, etc., required by utility policies and procedures.

The main control room should be designed as the communication centre for the plant for normal operations and during the early stages of an accident (IEC 964, 1989, p. 45). Most of the equipment for communicating with locations off-site should preferably be located on a special communications panel or desk with extensions on the main control desk and panels (IEC 964, 1989, p. 128).

During back fitting, it has been experienced that modern communications systems may interfere with older electrical systems. Special care may therefore be needed in these situations (IAEA, 1995, p. 41).

6.5.1 Verification of Communications Systems

6.5.1.1 Preparation

6.5.1.1.1 Documents Used in Verification

Did the utility identify relevant source documents?

Human factors documents are available to help designers to define desirable signal characteristics, can characterise noise and speech interference and give advice on other design features and assessment methods (IAEA, 1995a, p. 41).

Was the evaluation team given access to applicable documents prior to the beginning of verification?

Refer to the explanation in the generic process.

Did the evaluation team have access to a human factors operating experience review?

Refer to the explanation in the generic process.

6.5.1.1.2 Verification Team

Did the utility have a suitable evaluation team for the topic?

Specialist help may be needed for certain assessments, such as speech interference.

Was the evaluation team suitably placed in the licensee's organisation?

Refer to the explanation in the generic process.

Did the evaluation team have a suitable mix of disciplines?

Refer to the explanation in the generic process.

Was the evaluation team independent?

Refer to the explanation in the generic process.

6.5.1.1.3 Verification Resources

Did the utility supply suitable resources for the evaluation team?

There may be specific equipment requirements, such as noise meters, which the evaluation team may require to confirm that the design objectives have been met.

Were suitable working materials prepared?

Refer to the explanation in the generic process.

6.5.1.1.4 Verification Scope

Was the evaluation scope appropriate for the stage of the project at which it was performed?

Early in a project, the evaluation team should check that the functional specification for the communication systems conforms to criteria and objectives.

Did the evaluation include consideration of all appropriate scenarios?

The verification should include scenarios that place constraints on communications systems design, for example, high noise levels, and high traffic load.

Did the utility include all relevant locations?

The utility may need to set communications criteria for adverse locations where background noise and acoustics are considerably worse than control rooms. Communications equipment may also have to be usable when wearing hearing protection.

6.5.1.1.5 Verification Schedule Development

Refer to the questions and explanations in the generic process.

6.5.1.1.6 Verification Objectives

Did the utility define specific objectives for the verification of a topic?

IEC (1989, p. 43 ff.) gives several objectives for communication systems. They should facilitate safe and efficient plant operation. Special consideration should be given to the design of systems to be used in accident or abnormal situations, or to communicate with emergency services. There should be non-verbal as well as verbal systems:

- Verbal communications systems:
- On-site communications — for general communication during operational conditions, for accident conditions, a public address system for on-site personnel under any plant conditions, and for use during maintenance.
- Off-site communications — for communicating with the station operating authority, emergency and government institutions, etc.
- Non-verbal communications systems, such as television monitoring systems, facsimile, data links.

6.5.1.1.7 Verification Criteria

Did the utility develop criteria for communication systems?

Ergonomic criteria should be developed for all communication systems, covering issues such as audibility, intelligibility, speech interference, the local environment in which the system is used, support for control room tasks, etc. For example:

- There should be an adequate number of telephones in the control room.
- There should be a direct wire telephone system for emergency conditions.
- The main control room staff should be able to communicate with personnel at any other unit with a separate control room at the same site.
- There must be off-site communications to emergency teams, radiation measurement groups, fire-fighting stations, local police, government, public agencies.
- Speech intelligibility over the communications systems should be adequate in the expected noise environment.
- Speech quality should be adequate.

6.5.1.2 Evaluation

6.5.1.2.1 Verification Method

Did the utility develop and document a suitable method for verifying a topic?

Refer to the explanation in the generic process.

6.5.1.2.2 Verification Process

Was the review process satisfactorily documented and traceable?

Refer to the explanation in the generic process.

Were quantitative criteria defined and measured satisfactorily?

Quantitative criteria that could be verified include noise levels, speech interference calculations, effects of hearing protection on communication, local acoustic conditions such as reverberation time.

6.5.1.2.3 Verification Results

Refer to the questions and explanations in the generic process.

6.5.1.3 Resolution

Refer to the questions and explanations in the generic process.

6.5.2 Validation of Communications Systems

6.5.2.1 Preparation

6.5.2.1.1 Documents Used in Validation

Did the utility identify relevant source documents?

Refer to the explanation in the generic process.

Was the evaluation team given access to applicable documents prior to the beginning of validation?

Refer to the explanation in the generic process.

Did the evaluation team have access to a human factors operating experience review?

An OER may show some occasions where earlier communications systems have been inadequate, for example, overload of telephone lines or radio equipment during emergency exercises, insufficient communications discipline.

6.5.2.1.2 Validation Team

Did the utility have a suitable evaluation team for the topic?

Refer to the explanation in the generic process.

Was the evaluation team appropriately placed in the licensee's organisation?

The design and evaluation teams may need contact with health and safety parts of the utility's organisation

Did the evaluation team have a suitable mix of disciplines?

The team may need competence in specialist areas such as sound measurement, speech interference assessment.

Was the evaluation team independent?

Refer to the explanation in the generic process.

6.5.2.1.3 Validation Resources

Refer to the questions and explanations in the generic process.

6.5.2.1.4 Validation Scope

Did the evaluation include consideration of all appropriate scenarios?

Scenarios that test the validity of the design should be selected, such as emergency conditions with high communications load, high background noise levels (e.g., steam dumping). Intelligibility testing should be carried out in realistic conditions if the

results are to be of practical value. For instance, protective equipment worn during emergencies may interfere with communications.

Was the evaluation scope appropriate for the stage of the project at which it was performed?

Paper and pencil techniques may be valuable in the early stages of a project. For example, they can be used to provide estimates of the frequency and duration of messages, to estimate traffic, and to make lists of communications required by law. At later stages, simulations and emergency exercises may be required to demonstrate validity.

Did the utility include all relevant locations?

For example, the control room may need to communicate with local control points during emergencies. Any auxiliary shutdown control points may also need adequate communications facilities in the event that the MCR is not habitable.

6.5.2.1.5 Validation Schedule Development

Did the utility develop a suitable schedule for validation?

Refer to the explanation in the generic process.

6.5.2.1.6 Validation Objectives

Did the utility define specific objectives for the validation of a topic?

For instance, validation studies could aim to show:

- The provided systems can handle the off-site communications requirements during emergencies
- The systems do not reach over-capacity during emergency situations
- Operators' workload is not unacceptably high due to unplanned communications with the control room during emergencies
- The systems remain usable during adverse environmental conditions, such as background noise, when using protective equipment

6.5.2.1.7 Validation Criteria

Did the utility develop criteria for the human factors topic?

The evaluation team should have shown that the communications systems criteria were adequate for emergency conditions tried in simulations. For example, was it shown that the number of telephone lines from the control room sufficient and that there were sufficient off-site communications links?

6.5.2.2 Evaluation

6.5.2.2.1 Validation Method

Did the utility develop and document a suitable method for validating a topic?

For example, a study of the expected frequency and duration of telephone calls during emergency conditions can help establish the need for communications equipment. Such studies can start relatively early in the design process, since many requirements such as legal requirements for off-site notifications, are already known. Later, validation during simulations and training exercises can show whether the facilities provided are sufficient.

6.5.2.2.2 Validation Process

Refer to the questions and explanations in the generic process.

6.5.2.2.3 Validation Results

Refer to the questions and explanations in the generic process.

6.5.2.3 Resolution

Were satisfactory resolutions developed and recorded for all deviations and non-conformities?

For example, there may be a conflict between requirements for hearing protection and the need to use communications equipment.

Were there checks for side effects of resolutions?

For example, an increase in the general volume of a public address system to render it audible in all situations may cause distraction or annoyance in some locations. When several communication systems coexist, there may be a problem of compatibility, consistency and system integration.

Did the evaluation team succeed in resolving issues, even when these arose late in the project?

A validation finding that there are insufficient communications channels, for instance, may be difficult to resolve if the problem is found too late in the project.

6.5.3 Supplementary References

Sanders, M.S., McCormick, E.J. (1992) Speech Communications. Ch.7 in *Human Factors in Engineering and Design*, 7th Ed. New York: McGraw-Hill.

UK Ministry of Defence (1991) Voice Communication. Part 9 in *Human Factors for Designers of Equipment*. Glasgow: Ministry of Defence, Directorate of Standardisation (Interim DEF STAN 00-25).

6.6 Procedures

> The purpose of NPP procedures is to guide human actions during task performance in order to increase the likelihood that the actions will achieve the task goal. (Barnes et al., 1996)

> The procedure development programme will result in procedures that support and guide human interaction with plant systems and control plant related events and activities. Human engineering principles and criteria should be applied with all other design requirements to develop procedures that are technically accurate, comprehensive, explicit, easy to use and validated. (NUREG-0711, 1994, p. 9-1)

Procedures and the process for their development should be subject to V&V in order to ensure that the final procedures are technically correct and present the information in the most effective and efficient manner. The basis for procedure development should include technical information, a writer's guide and a task analysis. Procedure development is also closely linked to the areas of job design, staffing levels, training, and integrated system testing.

6.6.1 Verification of Procedures

6.6.1.1 Preparation

6.6.1.1.1 Documents Used in Verification

Did the utility identify relevant source documents?

The evaluation team should have ensured that appropriate information sources for the development of procedures were available. These include the technical source documents for the contents of the procedure, and the human factors guidelines used for writing and presenting the procedure.

Lists of documents that form the technical basis for the procedures are presented in NUREG-0711 (1994) section 9.4 point 2, and in Barnes et al. (1996) Section 5.2.1 p. 5-2, 5-3. Barnes et al. also identify the regulatory and management bases for the procedures. NUREG-0711 (1994) section 9.4 point 3 identifies the basis for a human factors writer's guide.

In addition, the evaluation team should have established the documentary basis for the procedures design process itself, including the assumptions of the designers regarding the role and use of procedures. The important role of operational experience and lessons learnt should be established in this process. Documentary evidence for the application of this process should be presented.

Was the evaluation team given access to applicable documents prior to the beginning of verification?

It should be demonstrated that all the appropriate, up to date information sources, were available to the evaluation team during the verification process, e.g. results of function allocation, task analysis, etc.

Did the evaluation team have access to a human factors operating experience review?

Important feedback from previous operating experience should also be accounted for in the design of the procedures. This feedback should consider aspects such as format and layout, wording, diagram use, place keeping, use of multiple procedures. It should also include experience from the procedure development and maintenance system.

6.6.1.1.2 Verification Team

Did the utility have a suitable design and evaluation team for the topic?

Refer to the explanation in the generic process.

Was the evaluation team suitably placed in the licensee's organisation?

Refer to the explanation in the generic process.

Did the evaluation team have a suitable mix of disciplines?

Expertise in technical writing, document design, and graphical aspects (statistical and illustrative) could be included in the evaluation team.

Was the evaluation team independent?

The evaluation team should be independent of the procedure authors.

6.6.1.1.3 Verification Resources

Did the utility supply suitable resources for the evaluation team?

It should be demonstrated that the evaluation team's requirements for suitable resources with which to carry out the evaluation were met. For example the team may need access to appropriate personnel, external expertise, and appropriate facilities.

Were suitable working materials prepared?

Refer to the explanation in the generic process.

6.6.1.1.4 Verification Scope

Was the evaluation scope appropriate for the stage of the project at which it was performed?

The evaluation team should have ensured the verification process was appropriately applied to:

- Both technical content and human factors aspects of the procedures.
- The procedure presentation concept was documented and evaluated early in the design process.

- Draft copies of procedures were verified.
- Final versions of the procedures were evaluated in an integrated control room.
- The full scope of procedures was evaluated from the areas of operations, maintenance, test, inspection, and surveillance across the full range of operating modes. See NUREG/CR-6393 (1996), p. 5-11 and NUREG-0711 (1994), p. 9-1.
- For upgrading of existing facilities emphasis should be placed on emergency operation procedures, (IEC 1771, 1995a, p. 56).
- The assumptions and implementation scope for computerised presentation of procedures. For example the verification requirements for context sensitive computerised procedures will be greater than for more passive systems, see Barnes et al. (1996).

Did the evaluation include consideration of all appropriate scenarios?

Refer to the explanation in the generic process.

Did the utility include all relevant locations?

Procedures can be used outside the control room and/or co-ordinated with other 'field' or maintenance procedures. The use, interaction, and compatibility of procedures at these different locations and environment should have been considered

6.6.1.1.5 Verification Schedule Development

Refer to the questions and explanations in the generic process.

6.6.1.1.6 Verification Objectives

Did the utility define specific objectives for the verification of procedures?

The verification process should have documented specific objects suitable for procedures. Wieringa et al. (1992) suggest a number of objectives for verification including;

- The procedure should be accurate.
- The procedure should be written in accordance with appropriate standards (e.g., the writers' guide).
- The equipment labels and markings cited in the procedure should correspond with actual hardware.

6.6.1.1.7 Verification Criteria

Did the utility develop criteria for procedures?

The evaluation team should have insured that the two major principles involved in verification of procedures have been adequately considered: technical accuracy and written correctness. Criteria for verification of the procedure process and the procedures themselves should reflect these principles.

www.ski.se

STATENS KÄRNKRAFTINSPEKTION
Swedish Nuclear Power Inspectorate

POST/POSTAL ADDRESS SE-106 58 Stockholm
BESÖK/OFFICE Klarabergsviadukten 90
TELEFON/TELEPHONE +46 (0)8 698 84 00
TELEFAX +46 (0)8 661 90 86
E-POST/E-MAIL ski@ski.se
WEBBPLATS/WEB SITE www.ski.se