IAEA-TECDOC-1066

Specification of requirements for upgrades using digital instrument and control systems

Report prepared within the framework of the International Working Group on Nuclear Power Plant Control and Instrumentation

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

The IAEA does not normally maintain stocks of reports in this series.
However, copies of these reports on microfiche or in electronic form can be obtained from

INIS Clearinghouse
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria
E-mail: CHOUSE@IAEA.ORG
URL: http://www.iaea.org/programmes/inis/inis.htm

Orders should be accompanied by prepayment of Austrian Schillings 100,–
in the form of a cheque or in the form of IAEA microfiche service coupons
which may be ordered separately from the INIS Clearinghouse.

The originating Section of this publication in the IAEA was:

Nuclear Power Engineering Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

SPECIFICATION OF REQUIREMENTS FOR UPGRADES USING DIGITAL INSTRUMENT AND CONTROL SYSTEMS

IAEA, VIENNA, 1999
IAEA-TECDOC-1066
ISSN 1011–4289

Printed by the IAEA in Austria
January 1999

FOREWORD

The need to develop good specifications of requirements for instrument and control (I&C) systems applies throughout the world and is becoming more and more important as more I&C upgrades are planned. Better guidance on how to develop good requirements specifications will support safer, more effective and more economical refits and upgrades. The need for this was pointed out by the IAEA International Working Group on Nuclear Power Plant Control and Instrumentation (IWG-NPPCI). The first IAEA consultants meeting on the subject was held in Vienna from 17 to 21 March 1997 in order to exchange information on national experience in the development of I&C requirements specifications and to prepare an extended outline of the planned report.

This report is the result of a series of advisory and consultants meetings held by the IAEA in 1997 and 1998 in Vienna. It was prepared with the participation and contributions of experts from Belgium, France, Germany, Italy, the Republic of Korea, Sweden, the United Kingdom and the United States of America.

The scope of activities described in this report covers a methodology for the determination of requirements and the development of the necessary specifications and plans needed through the life-cycle of digital I&C systems. It is restricted to technical aspects. It indicates the subjects which specifications and plans need to include at different phases. The management of the contracts involved, the conditions of work and of payment, etc., are not discussed.

Special thanks are due to D. Welbourne (UK) who chaired the working meetings and co-ordinated the work. V. Neboyan of the Division of Nuclear Power was the IAEA officer responsible for preparing this publication.

EDITORIAL NOTE

In preparing this publication for press, staff of the IAEA have made up the pages from the original manuscript(s). The views expressed do not necessarily reflect those of the IAEA, the governments of the nominating Member States or the nominating organizations.

Throughout the text names of Member States are retained as they were when the text was compiled.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

1.1. STATEMENT OF THE PROBLEM

From experience at plants that have introduced upgrades of analog equipment and systems using digital equipment, there appears to be a large variability in the costs and problems encountered in implementing, operating and maintaining the upgraded systems. The source of many problems can be traced to the specifications for the upgrades. These specifications govern the basic requirements, design, development, installation and testing activities during the life-cycle of the upgrade. A systematic approach is needed to developing specifications which are comprehensive and which also maintains a focus on the highest project risk areas.

At present, there is no methodology, standard or guidelines generally accepted by the nuclear industry for preparing the various types of requirement specifications and plans for digital upgrades. This can be contrasted with the design and implementation on of computer software after the requirements have been defined. For software, there are many detailed and specific standards on the methodology and the detailed contents of the different specifications and design documents used in the life-cycle. For refits and upgrades, frequently the specifications of requirements for an analog system are reused and slightly modified to define the upgrade. This has often resulted in difficulties. In some cases, the documentation of the existing power plant may be inadequate for the complete definition of the requirements. Additional work may be required to determine features needed for the new equipment. Usually, digital equipment is needed with functionality different to or greater than the original systems. The specifications of requirements, manufacture and test must therefore include important requirements beyond the scope of the original analog equipment. Preparation of good specifications for a digital upgrade requires expertise in hardware, software, data communications, plant operations, networking and licensing.

The need to develop good specifications of requirements applies throughout the world and is becoming more and more important as more upgrades are planned. Better guidance on how to develop good requirements specifications will support safer, more effective and more economical refits and upgrades. A structured and disciplined approach to producing system documentation is now recognised as essential for new plant designs. New plant needs suitable QA support. The same approach should be followed for modifications and upgrades. The documentation for new plants may nevertheless not cover important requirements details. Guidance on the methodology and the specific points for inclusion in requirements at different phases of the life-cycle for instrument and control (I&C) systems should also be of value for new plants.

There is a need for guidelines on how to co-ordinate these subjects in the task of identifying the requirements and producing the relevant specifications and plans at each phase of the life-cycle, as comprehensively as necessary for that phase.

1.2. OBJECTIVES

The objectives of this report are:

- to provide guidance, without prejudicing the working practices of the readers and users, for subjects which the specifications of requirements for digital I&C systems should include at different phases of the life-cycle of a project;
- to outline, and later in the report to define more clearly, a methodology which minimises the risk of omitting important requirements from the specifications for digital I&C refits and upgrades;

- to ensure all elements of requirements which are needed in the various specifications are identified, so that they take account of significant influencing factors such as safety and utility preferences.

1.3. RELATIONSHIP TO OTHER WORK

Existing work or work currently in hand in the IAEA and elsewhere covers subjects such as:

- how to assess the need for refit;
- how to structure and undertake a modernisation project;
- how to determine the architecture of a computer-based system;
- verification and validation methods applicable to computer-based equipment;
- methods of software quality assurance;
- the state of the art in computer technology;
- the technology available.

These are discussed in documents which include IAEA references [1, 2, 3, 10, 27–32], and their references. The guidelines of this publication are intended to be read in conjunction with those of IAEA publications which provide more detailed guidance.

This publication does not repeat information provided by the reference documents but provides a methodology for identification of requirements.

1.4. SCOPE

This report describes a methodology for the determination of requirements and the development of the necessary specifications and plans needed through the life-cycle of digital I&C systems. It is restricted to technical aspects. It indicates the subjects which specifications and plans need to include at different phases. The management of the contracts involved, the conditions of work and of payment, etc., are not discussed.

A simplified reference life-cycle is defined for use in the publication, representative of the work needed for I&C systems. Influencing factors and constraints are discussed. Requirements elements are discussed, which can be expected to be included in specifications needed at the stages of feasibility, initial design, detailed design and implementation, testing and operation of the equipment. These are brought together in a description of the refit or upgrade process from initiation of a feasibility study to final operation and maintenance.

The elements of requirements which need to be identified at different phases of the life-cycle include, at the higher level:

- project requirements including scope of work, time-scale, support and services,
- system requirements including functionality and performance,
- implementation requirements including those for technology, software and engineering,
- qualification and testing requirements.

The activities and the input and output documents for each phase of the life-cycle are described in detail. For more detailed reference the information is shown as a table for each life-cycle phase, and in diagram form in Appendix I.

Other appendices give a suggested structure and document contents for requirement specification, a list of reference standards from US practice and from European Union practice and discuss the methodology for analysis of the I&C design for the requirements for a control room upgrade.

1.5. READERS AND USERS OF THIS PUBLICATION

The reader and user of these guidelines is envisaged as an engineer involved in planning or supervision of refit or upgrade work, or potentially in new designs. The engineer may be involved in the detailed work and may want to use the guidelines to check and confirm in more detail that the requirements applicable to the life-cycle stage are indeed covered, or to initiate work to discover the relevant requirements. The engineer is envisaged as working for a utility, at a headquarters group or on site, an architect engineer, design organization or consultant, or a site construction unit. The engineer may work for a supplier of equipment and software, for hardware production or software implementation, factory testing or site installation teams. The guidelines may be used for production of specifications and plans or for review and assessment of documents.

Although not directly aimed at engineers in a safety authority, the description of specifications and plans may be of importance for such engineers.

1.6. TERMINOLOGY

Terms used are defined in a descriptive way. The terms backfit, refit, retrofit, refurbish and upgrade are all similar and often interchangeable in normal English speech, and only have differences of shades of meaning. This shading is indicated and an example of the use is given in the Glossary.

The term 'utility' is used for the power plant owner, design organization and operator. In practice, the utility may engage an architect-engineer, agent or consultant to supervise, design and manage the refit or upgrade project. These organizations are intended under the term 'utility'.

The term 'sponsor' is used for any organization which is assisting the refit or upgrade by providing funds to pay for the project. A sponsor may be national government or a government agency, the utility finance department or shareholders, or an international organization. A sponsor will normally require full details of the project. A sponsor may require consultancy services or equipment and software quotations for the project to be provided by specific organizations.

The term 'supplier' is used for the organization responsible for the detailed design, manufacture and installation of the equipment and for the implementation of any software. In fact, the supplier may buy software and some equipment, or employ a software house, and may use the on-site utility services for some aspects of installation. The supplier is sometimes referred to as the 'vendor'.

The term 'project' is used to describe the total activity of the refit or upgrade work. In some cases the utility may use an agent or architect-engineer, or a major supplier of equipment to manage the project and co-ordinate the supply of several systems, if the total project covers more than one main function.

The term 'regulator' is used for the national body charged with approval of the project as sufficiently safe, in the context of a licence to operate a nuclear plant or facility. Other terms and abbreviations or acronyms are given in the Glossary.

2. BACKGROUND INFORMATION

2.1. CLASSIFICATION OF SAFETY OR OPERATIONAL IMPORTANCE

IAEA Safety Guide 50-C-D [4] establishes the concept of classification of nuclear power plant systems according to their importance to safety. It gives examples of the classification of the major systems of several types of nuclear power plants. Safety Guides 50-SG-D3 [5] and 50-SG-D8 [6] (currently under revision) apply classification to I&C systems. These guides establish the distinction

between the safety system and safety-related systems, which together form the systems important to safety. The safety system consists of the systems provided to ensure the safe shutdown of the reactor and heat removal from the core, and to limit the consequences of anticipated operational occurrences and accident conditions. Safety-related systems are systems important to safety which are not part of the safety system.

The principles of IAEA classification have been interpreted in IEC1226, which defines a method of safety categorisation. The standard identifies categories A, B and C for functions, systems, and equipment of I&C systems that are important to safety. The definitions of these categories are simplified as follows:

- Category A is assigned to functions, systems and equipment (FSE) which have a principal role in the achievement or maintenance of nuclear power plant safety (IEC1226 Section 5.2.1.).
- Category B is assigned to FSE which have a supporting safety role to systems of category A (IEC1226, Section 5.2.2.).
- Category C is assigned to FSE which have an auxiliary or indirect role in the achievement or maintenance of the nuclear power plant safety (IEC1226, Section 5.2.3.).

The remaining FSE are assigned to be "unclassified". IEC1226 annex A gives examples of typical functions for each category. This publication uses the categories of IEC1226 in grading the I&C systems for identification of the relative importance of different influencing factors to different aspects of the requirements through the life cycle of an I&C system. Individual countries may have other methods of identification and categorisation of FSE and items important to safety. These are defined through national and other standards. In those countries, this publication should be interpreted in a manner that is appropriate to the identification and categorisation process used in that country.

The English language terms used in safety categorisation are different in different nations, and the IAEA definition of 'systems important to safety' includes two separate system classes, which are the 'safety system' and the 'safety-related systems'. This differs from the terms used in US practice. Figure 1 illustrates some differences between international and different national practices. Decreasing importance to safety is indicated by movement to the right, and the vertical divisions are in qualitative terms.

Nuclear safety is not the only factor in determining the importance of an I&C system. It should be noted that IEC 1226 includes in category C some functions associated with more conventional concerns on personal and plant safety.

The utility may place a higher requirement on a system than that required by safety considerations alone. This may be due to availability requirements, the importance of the system to plant operation, or due to the unique nature of the system design. The utility may then require a high level of assurance of performance and reliability. This can be given if the system is treated as if it belonged to a higher safety category, and is subject to more rigorous requirements than otherwise. For example, a utility may decide to require a high level of V&V for a computer-based system that is of critical importance to plant operation, although it has low importance to safety. This can be achieved if it is treated as if it belonged to a higher safety category.

2.2. OVERVIEW OF THE DEVELOPMENT OF REQUIREMENTS

Section 2.3 of the report outlines a general method for preparing and issuing any kind of requirements specification document (such as basic requirements, detailed specifications, validation requirements, qualification, installation and test plans, as discussed in Section 6).

National or international standard	Classification to the importance to saf.			
IAEA	Systems important to safety			Systems not important to safety
	Safety system	Safety related system		
IEC 1226	Category A	Category B	Category C	Unclassified
France N4	1E	2E	IFC/NC	
European utility requirements (EUR) (time dependant)	F1A (Automatic)	F1B (Automatic and manual)	F2	Not classified
UK	Category 1	Category 2	Not classified	
USA (IEEE)	1E	Non-nuclear safety		

FIG. 1. Comparative safety classification and safety categories.

Section 3 discusses the life-cycle of a project, and identifies a reference life-cycle. The initial phases are at the overall level, and once the architecture is defined, the phases then show life-cycles for each system in the modernisation scope. The life-cycle then moves to the installation and site phases, considering the overall aspects. Many life-cycle requirements are given in various national and international standards, and software engineering experience has produced many recommendations for the information and work needed at different stages of the life-cycle. The life-cycle of a project is influenced by the decisions made on the documentation of requirements which govern the project at different stages. Good control and communications, and the reduction of the risk of misunderstanding, delays, confusion and project problems depends on this. The life-cycle is described in terms of activities, inputs, output requirements and output deliverables.

Section 4 describes the influencing factors which can affect a project, such as the utility attitude to digital I&C, the safety class of the equipment, the extent of replication of the systems being installed, the physical factors of layout and plant services available.

Section 5 describes the key elements of requirements which need inclusion in specifications for the stages of the life-cycle. Consideration of the progress of a typical project shows that there are many different types of secondary requirements defined at different times, according to the circumstances of the life-cycle stage. These detailed aspects are discussed in Section 6. The structure

of the key requirements has been developed from those identified in IEC1069. Tables I–X summarise Sections 3, 4 and 5 and provide guidance on subjects for inclusion in specifications of requirements at different stages of the project.

Section 6 describes a methodology for identification of requirements, as they are needed at different stages of the project. This section brings together the material on the types of requirement, the life-cycle stages and the influencing factors on the project, showing the major elements of the different requirements specifications and the suggested allocation in time and connections between the related documents. The main aspects discussed include functions, engineering of software and the HMI.

Additional information is included in the appendices. Appendix I shows in graphical form the flow of activities and documents, indicating also the typical documents to be produced and the organization which would provide it. Appendix II highlights some aspects related to the use of functional and task analysis in I&C design. Appendix III suggests a structure for requirements specification document, which is the key to the total upgrade project. Appendix IV provides a set of typical reference standards for a project. Clearly the user of this report must use his or her own experience and judgement in defining the requirements for a specific project. The material is offered as a guide and aide memoire for the user, based on the experience of the authors of this report. It is intended to allow as complete a set of requirements to be generated as practicable.

2.3. OUTLINE OF THE METHOD FOR DEVELOPING REQUIREMENTS

By considering the project phase which has been reached, the influencing factors and the elements of requirements together, the engineer can proceed step by step to consider each element in turn. The requirements relevant to the phase of the project must be considered with the influences on the project relevant at that phase, and each element of requirements can then be developed to as complete a state as possible.

It is important to identify requirements which cannot be properly defined at that time, for whatever reason. These should be shown as further work items until they can be resolved.

To some extent the process of defining requirements is open-ended, and documents which are too detailed may not add value to a product phase. Engineering judgement is therefore needed in defining the requirements, bearing in mind the readers and users of the document concerned. The author of the document of requirements may consider some detailed requirements unnecessary to define, in the interests of clarity of the overall document. Some details may be left to the discretion and judgement of the user of the document, to provide in accordance with good practice. But for category A systems, this discretion must be limited by reference to the applicable norms and standards for such equipment.

In the following, the requirements are assumed to be defined in a document. Although this will often be the case, at some stages they are usually defined as a computer information input process. Typical methods are an interactive graphical input to a computer system, or a software tool which requires systematic definition of top-level modules, detailed modules, and the links and interfaces between the modules. At some stages of the process, detailed databases may be formed as part of the definition of requirements. Some requirements are stated as plans, which define the time-scale, the quality assurance needed, the software V&V, the method of installation or other intended actions. In all cases, 'document' is used in the following for the method of recording the requirements.

The quotation and purchasing stage in the life cycle (see Section 3) is specifically important, because at that stage commercial aspects will interact with technical aspects. It is thus essential to

define at this time, as precisely and completely as possible, all the requirements that will govern relations between user and supplier throughout the following stages of the life-cycle, through to completion of installation and any warranty period. This requirement expression is referred to hereafter as the basic requirements specification (BRS), and its typical contents are outlined in Appendix III. The BRS will form part of the complete set of contract documents for the project.

2.4. METHODOLOGY

The methodology is described in Appendix I, by means of a diagram for each phase to show what is to be done, and from what inputs to define each document or plan as output.

The detailed process of identification of the requirements at a specific point can be described one step at a time as follows:

(1) At the phase of the project in question -

- identify the document type needed, which will state the requirements for the phase;
- identify the project QA control procedures over that document;
- obtain the correct drawing, document or other identification;
- obtain the correct authority for document preparation.
-

(2) Within the document structure -

- chose the element of requirements for development;
- identify from the element of requirements all detailed requirement subjects to be defined;
- identify the influences and constraints of most importance to this phase;
- develop a requirement statement accordingly;
- include the detailed requirement into the requirement documentation or record a further work item;
- repeat for all elements of the requirements.

(3) Within the document structure -

- identify any requirements which are incomplete, not known or otherwise uncertain;
- identify the extent of the lack of knowledge;
- include suitable text in the document to state this, as a referenced further work item.

(4) Using the draft document -

- initiate a check and review process according to project QA procedures;
- where practicable, initiate a formal verification of the requirements stated;
- where practicable, verify and validate the requirements by automated means.

(5) On completion of the document review and verification -

- correct the document to allow for agreed comments;
- obtain signatures and issue the document, according to QA procedures, for use on the project;
- follow up the further work items for resolution.

This process is then repeated for the next phase of the life-cycle, in order to develop the requirements needed for that phase.

The activities (Section 3), inputs, influences and constraints (Section 4), requirements (Section 5) and deliverables of each phase are shown in Tables I to X and in Appendix I, which summarise the total activity, as described in Section 6.

2.5. JUSTIFICATION OF THE SAFETY OF THE SYSTEM

The safety of the system to be installed in the plant must be justified, both in the mind and conviction of the utility, the designers and suppliers and also formally to the national safety regulatory authority.

Although the methods and practice of each country are different, some common principles can be given. These may be expressed as:

- there must be confidence in the people, the processes and the product,
- confidence must be demonstrated by documentary evidence,
- quality assurance can give confidence in the processes, and may extend to the staff and the qualification and testing of the product,
- documentary evidence must be open to audit,
- documents and responses to legitimate questions must be provided freely to the regulator,
- an overall summary document describing why the system will be safe is needed.

The overall process of justification of the safety of the system is called here the safety case. This consists of all necessary evidence to show that the system is safe, but is often also a term used for a specific summary document which gives references to remaining documentary evidence. A valuable guide to the practice followed in Canada, France, UK and USA for the safety case is given in 'Four party regulatory consensus report on the safety case for computer-based systems in nuclear power plants', published by the UK Health and Safety Executive.

Quoting from the above reference, the safety case is defined there (para 17) as:

> "... the licencee's documented demonstration that:
>
> (a) the correctness and completeness of the overall requirements specification has been justified in relation to the intended system function;
>
> (b) the system design has been developed to standards compatible with the safety importance of the application;
>
> (c) the delivered system satisfies all aspects of its requirements specification, and;
>
> (d) adequate means and arrangements are specified which ensure the required performance of the system throughout its operational life."

It can readily be seen that many points can arise from these principles, such as detailed examination of the set points of a trip system, detailed justification of the methods followed for operation and maintenance, and full documentation of the results of factory and site acceptance testing. The methods followed by all staff involved in a refit or upgrade project will need to take account of this, and should directly take account of the need and importance of safety. If this approach is followed, then the safety justification to the regulators will arise naturally, rather than being an imposed constrain on the project progress.

3. BASIC REFERENCE LIFE CYCLE

A clear life-cycle and methodology should be established for any modernisation project. A basic reference life-cycle is described below in terms of:

- initial and main activities to be performed in the individual phases,
- inputs to the phase activities,
- outputs from the phase activities.

The phases of the basic reference life-cycle simplify reality, and provides a common descriptive framework for this report. A suitable life-cycle for any specific project should be identified. The life-cycle should allow for the life-cycles of the drafts of IEC 1508, IEC 1513 and IEC 880 if applicable.

The modernisation project may concern one or several I&C systems of the NPP. Some activities are at the overall plant level, others are at the level of the individual I&C systems, and the life-cycle shows the relations between these. The life-cycle described separates the initial activities and the main activities of each phase; in many cases, these are an activity by the utility or his agent to initiate work (for example to issue a specification or agree a design), followed by activities by the supplier to undertake that work (for example to provide a tender against the specification or manufacture to the design). Qualification activities are necessary during the life-cycle, but are not specifically associated with any phase. They must be planned (phase 4), and must be completed before handover for operation. The FAT and SAT form part of the total requirement for qualification. The activities include:

- agreement of detailed system designs,
- agreement of detailed system planning information,
- development of specific equipment, (e.g. interfaces to other systems),
- software design, manufacturing and test,
- hardware design, manufacturing and test,
- development testing of specific equipment,
- manufacturing of standard components and modules,
- post-manufacture tests of standards components and modules,
- purchase and delivery of bought-out equipment and software,
- integration of hardware and software ready for the factory acceptance test.

3.1. OVERALL PROJECT PHASES

3.1.1. Project preparation and feasibility study

The initial activity is to develop the scope of the feasibility study. This may be done directly by the utility, and depends on discussion and review of the aims of the refit or upgrade, with production of a specification of the scope of the study required. This specification is normally issued to a supplier of nuclear plant design services, or an organization experienced in system engineering, when many systems are involved. In some cases the utility itself will undertake the study. The main activity is the production and reporting of the feasibility study which conclude the phase.

The activities needed include:

- reviewing the present I&C systems requirements documentation (or advising its development if not available) as input information for consideration of new systems,

- identifying the I&C functions, and associated systems & equipment belonging to the modernisation scope,
- identifying weaknesses and strengths of the existing systems, in their functionality, performance, dependability, operability and other key features,
- developing preliminary requirements for new systems, with special consideration of requirements that expand beyond those for the existing systems,
- developing conceptual design alternatives for the new systems,
- identifying the benefits of safety and operation expected from the work,
- developing estimates of costs for new system alternatives over the expected system life,
- developing estimates of benefits for new system alternatives over the system life,
- comparison of cost/benefits for new system alternatives,
- selection of recommendations for the optimum conceptual design for the new systems.

This phase is completed by issue of the feasibility study report, which should be reviewed by the utility, discussed and agreed. It should have clear recommendations and conclusions on the nature of the refit or upgrade and its scope. It is needed to justify and provide the basis for decisions by management and the sponsors of the extent of upgrade work.

3.1.2. I&C architecture and basic requirements specification

The initial activities depend on acceptance by the utility and its sponsors that upgrading and refits shall be done. The activities may include review of suitable products and suppliers, review of I&C, sensors and actuators, human factors review of a control room and consideration of safety improvements, fire and other hazards. These activities may be done by the utility, but generally will be done by a consultancy group experienced in system analysis and design. This group will work on behalf of, and in close consultation with the utility. Normally, for a major project, subject or topical review reports should be produced, as a preliminary to the main activities below. Appendix II gives guidance on the approach to analysis to identify requirements when these are not well defined.

The main activities are the development of design concepts and the development of the basic requirements specification. This specification will cover the general subjects described in Appendix III, and provides a comprehensive definition of the scope and nature of the total project. It is generally in several parts, with some reference documents, such as the reviews of the initial activities and standard specifications of good practice to be used by the supplier.

The activities needed include:

- providing the overall I&C systems architecture showing the systems and interconnections impacted by the modernisation project and an outline of the scope,
- specifying the basic requirements for functional, performance and dependability requirements of the I&C safety, automation and operator control systems,
- identification of the safety relevance of the I&C functions and categorisation of the I&C functions important to safety,
- allocation of the I&C functions and operator's tasks,
- developing the qualification strategy for the interconnected I&C systems.

The output of this phase provides documentation of the conceptual design and requirements needed for procurement activities for the new systems and serves as a design frame for the systems to be upgraded.

The phase is completed by issue of the basic requirements specification (see Appendix III and Section 4.1).

3.2. INDIVIDUAL I&C SYSTEM PHASES

3.2.1. Tender specification and purchasing of the individual systems

The initial activities are the specification of requirements for tenders for the individual systems. This may be done by the utility directly, or by his agent, who co-ordinates the total refit and upgrade.

The main activities are the suppliers' initial development of designs, time-scales and quotations.

The activities include:

- identification of suitable suppliers of the equipment and services needed,
- preparation and issue of invitations to tender, including the system specification and requirements and request for quotation,
- development of tender evaluation criteria,
- evaluation of tenders,
- selection of product and system supplier,
- agreement with the selected supplier of the scope, methods, options, details and plans for the project,
- revision of the basic requirements specification (or of other appropriate documents) to incorporate design, planning, cost, quality and other information from the bid evaluations, as the agreed contact document governing the project.

The phase is completed by selection of the supplier and by issue of a contract for procurement of the new system by the utility.

3.2.2. Specification of individual I&C systems

The initial activities are the identification of detailed system and software requirements for the individual I&C systems.

The main input is the contractual requirements from the supplier order, the basic requirement specification, the legal requirements from national laws and the requirements from national and international standards.

The main activity of this phase is the production of the I&C system specification and software requirements, completed by functional validation. The validation concerns only the specified functionality to ensure that the following phase of system realisation is not endangered by expensive reworks. Furthermore it should be confirmed that the I&C systems fault tolerance and response times meet the requirements from the earlier specification phase.

The activities are:

- specification of the I&C system architecture,
- specification of the functions to be performed by the I&C system,
- design of the application software (preferably by automated code generation),
- validation of the specified functions preferably by means of a validated plant simulator,
- check of system response time,

- definition of global system integration and installation plans,
- definition of system testing plans,
- definition of qualification plans for hardware and software.

Functional validation has to include the HMI, depending its direct impact on control room layout. If relevant plant operating procedures are impacted, validation of the HMI has to be considered even if the control room design is unchanged.

The phase is completed by issue of the system functional information, the software requirement specification and agreement on all planning documents.

3.2.3. System realisation

The essential prerequisite for the detail design is a validated set of functions for the I&C system. The results of the detail design phase are on one hand documents for the hardware manufacturing and for erection and installation for integration of the updated I&C system in the existing plant, and on the other hand documents for software production and verification. Part of the activity is to define VDU designs, alarm messages, sensor and actuator characteristics and other interfaces. This may be undertaken by the supplier, the utility or by others, with agreement of detailed data conversion processes to allow the information to be included in the system. The initial activities include:

- the hardware manufacturing documentation:
  - detailed hardware disposition,
  - junction lists, internal wiring lists,
  - power supply,
- the installation documentation:
  - cable routes and junction lists,
  - interface documentation to control room, process information system, transducers and switchgear,
- design of specific components, especially interfaces,
- the software detailed design documents,
- agreement of detailed system designs by the utility.

The main activities are the equipment manufacturing and erection of the I&C system in the test field, the detailed production and verification of all software and integration of the system operating and application software to the operable system. The manufacturing process is finished when the I&C system is ready to start the FAT.

The phase activities include:

- agreement of detailed system designs,
- software design, implementation and test,
- hardware design, manufacturing and test,
- development of specific equipment, (e.g. interfaces to other systems),
- development testing of project specific equipment,
- manufacturing of standard components and modules,
- post-manufacture tests of standards components and modules,

- purchase and delivery of bought-out equipment and software,
- integration of hardware and software ready for the factory acceptance test.

The phase is completed by successful integration of the system in the factory, ready for testing. For smaller systems or systems which are made up from components to be installed on site (such as instruments themselves) no factory test of the complete system may be appropriate, and all testing will be done on site.

3.2.4. Factory acceptance test

The initial activities are the detailed qualification tests, where these are needed separately from the FAT itself. This will be necessary for harsh environment tests of instruments, and it is usual for new modules to be subject to type tests at the limits of their specified environment and power supply variation. The software may need independent V&V, analysis or special testing in this phase.

The main activities are the tests of the FAT to detailed test plans prepared earlier (see Section 3.2.2). Typically, some of the qualification testing will be associated with this phase, e.g.:

- equipment qualification for its safety or safety-related role,
- software qualification and evidence needed for regulatory acceptance .

The activities include:

- final specification of requirements for FAT,
- FAT of integrated hardware and software (system validation),
- customer acceptance of FAT.

The phase is concluded by acceptance of the system for delivery to site.

3.2.5. Installation and setting to work of the individual system

The initial activities are for the supplier to develop an installation plan and to plan any installation tests needed.

The main activities are installation of the equipment and any installation tests needed.

The activities include:

- development of a suitable phased programme of delivery and installation,
- installation possible during normal operation,
- preparation for plant outage installation,
- installation needed during plant outage,
- simulator installation and testing, as needed,
- integration of the equipment and software,
- supplier's installation testing,
- review with the site staff of all site facilities, site services (elevators, cranes, equipment location and protection, temporary supplies etc.) and all installation areas needed by the supplier.

The phase is complete when the supplier has installed and set to work the systems, when he has performed his own testing and when he is ready for the site acceptance test.

3.2.6. Training and contract documents

The initial activities are for the utility to ask for training proposals and to agree a training programme with the supplier. This will need to cover both hardware and software.

The main activities are the training courses of the supplier, and the provision of all contract drawings, system manuals and handbooks necessary for the system operation and maintenance. The utility may have a preferred technical level and possibly a defined layout for system manuals. Specific handbooks and manuals may therefore be needed in addition to the supplier's standard provision, and a specific Section will always be needed to describe the system installed and its interfaces.

Training is usually conduced in parallel with the above activities of design and manufacture and covers activities such as:

- plant operator training,
- addition or change of VDU displays, alteration of computerised alarm or trip settings, modification of system calibration constants,
- system software load and QA procedures,
- system surveillance and calibration training,
- training for system maintenance and repair.

The phase is completed when suitably trained staff are available to the utility and all handbooks, manuals and contract documents are available.

3.3. PLANT RELATED PHASES

These final phases of the I&C basic reference life cycle are performed at the plant level because they concern the combination of I&C systems working co-operatively.

3.3.1. Site acceptance test and commissioning with plant

The initial activities are undertaken during the design and manufacture phase and are the production of detailed test plans and detailed commissioning tests and procedures for integration of the system with the plant itself.

The main activities are firstly the SAT itself, and then the commissioning of the system with plant. This will normally need some outage of the plant.

The activities include:

- site acceptance testing,
- checks of all plant cables to sensors and actuators,
- disconnection of any simulator equipment used in the SAT,
- connection of all plant sensors,

- connection of plant actuators,
- clearance of all significant utility reservations on acceptance,
- plant commissioning tests,
- initial supervised operation of the system with plant.

It is recommended to test integration and functional validation of the systems working co-operatively during the FAT, to give confidence of success in the SAT. It should be noted that the tests of the SAT may need to be more extensive than the normal FAT period will allow. All safety functions should be tested, whereas in the FAT only representative functions may be sufficient. The SAT may need a prolonged period of dependable operation (say six weeks) to give hardware and software confidence to the utility operations staff before operation with plant is possible.

The phase is completed in two phases, firstly by a satisfactory SAT and secondly by completion of commissioning with plant. Normally the SAT will be formally reported and the commissioning tests will be recorded in an auditable form.

3.3.2. System operation and maintenance

The initial activities are the development of operation and maintenance procedures, normally during the design and manufacture phases. Careful attention should be given to the development and QA procedures for software and for hardware modification, with appropriate levels of regression testing.

The main activities of operation and maintenance follow during the operation of the plant with the new system. These may require acceptance of the system by the safety authorities. The activities include:

- system manuals, handbooks and other documentation completion (see 3.2.5),
- supplier's spares recommendations and spares orders placed by the utility,
- delivery of spares required,
- software defect reporting procedures,
- software maintenance,
- hardware defect reporting procedures,
- hardware maintenance.

The removal from operation of the replaced system should be completed in accordance with defined plans. This often occurs as the new system is installed, but can occur later if there is to be parallel operation of both old and new system for a period of time.

The phase is ongoing and a completion point is not defined. Decommissioning is not considered in this report.

4. INFLUENCING AND CONSTRAINT FACTORS

4.1. INTRODUCTION

At each stage in the life cycle of I&C projects, various influences and constraint affect the requirements which must be defined. As an example, the safety role of equipment and the safety authority will influence the requirements for software V&V, and the need for a safety case. Again, the

experience of the utility with computer equipment will strongly influence the type of training needed. Constraints include the funds available and the planned outages of the plant during which installation can be done. The statements of requirements at different life-cycle phases therefore should take these influences into account. The influencing and constraint factors of concern are discussed in relation to:

- the project itself,
- the safety and operational importance of the I&C systems,
- the regulatory and licensing framework,
- the I&C systems integration,
- the process operation and HMI,
- I&C systems operation and maintenance.

The influencing and constraint factors should be taken into account from the feasibility study stage onwards and certainly from the early basic requirements specification stage, to limit scope and requirement changes later in the project and to prevent cost increases. Care should be taken to ensure that before contracts are placed, all requirements are developed sufficiently to allow a determination of the final contract price which is as precise as possible.

These factors are, generally, related to the chosen modernisation strategy and the utility approach and constraints. Some of these aspects are discussed in detail in Sections 4.2, 4.4, 4.5, 4.6, 6.2 and 7.2 of [2]. In the following, the major factors are outlined.

A reference structure for the basic requirements specification (BRS) document is provided in Appendix III, and used for convenience as a reference throughout this section. This structure will allow the necessary requirements of the utility to be integrated in a suitable form. The document structure given will need supplementary statements and documents to provide details relevant at different stages of the project. These will be references from the BRS. The BRS should be revised during the project, since the first issue cannot normally take account of the full nature of the refit work and of the equipment chosen, and unforeseen problems may appear. Other structures of requirement documentation may be appropriate, or may be the current practice of utilities or their agents. Whatever structure is used, the important elements must be addressed in the appropriate specifications for the phase of the life cycle. It is recommended that the structure is compared with Appendix III to identify any deficiencies in stating necessary requirements.

The BRS should include project, system functional, architecture and safety requirements, design, technology and other requirements for the new systems. The utility should ensure its production when placing a single direct contract for the total upgrade or refit project, or if a contract is to be placed for management of the procurement of the individual systems of the total upgrade. Either the utility or a supplier should write a corresponding document, with a reduced scope, for a refit of a single system. The more important requirements produced by the supplier are indicated in the tables. These include manufacturing build lists, software design requirements, installation requirements etc. No structure is suggested for these.

4.2. FACTORS ASSOCIATED WITH THE PROJECT ITSELF

4.2.1. Utility attitudes and general policy decisions

The utility's available technical design capabilities, background and support available to implement the refit or upgrade will influence the approach to the project. The utility (either directly or via its architect engineer or agent) may be familiar with modern approaches to safety and be confident in the application of new technology. It could then take a strong hand in the complete definition of technical requirements. If there is not sufficient familiarity or sufficient resources available, the utility

may wish the supplier to provide a comprehensive service of identification of requirements and of full design and implementation of the new system or systems. This will influence the scope and nature of responsibilities as well as the approach to new technology.

It is important also that the specific project should be carried out in the context of the overall policy of the utility towards I&C upgrade or refit. This should be performed taking into account:

- the number of NPPs the utility is operating in order to account for possible effects on other plants,
- the particular situation of the plant where the project is to be implemented (remaining lifetime, plant personnel skills),
- the final goal of project implementation (safety upgrading, operational improvement, reduction of maintenance and testing).

The utility attitude will influence the method of undertaking the feasibility study and the response. The BRS should be developed carefully to reflect the utility attitude and requirements.

4.2.2. Scope of project, scope split and interfaces definition

Scope and scope split definition are influences on the project at all stages from feasibility through design and realisation to implementation. Proper definition of interfaces will help to reduce the planning needs associated with the different phases.

Interfaces will exist between the different organizations involved and between the different I&C systems. Clear interface definitions are also essential to allow straightforward responsibility sharing between the utility and the suppliers or between the various suppliers. The scope split should be defined very carefully so that interfaces are easy to understand and easy to manage.

The scope of a project should be evaluated during the feasibility study and adapted to reduce interfaces when possible. The final scope adopted should allow for optimal:

- functional operation, maintenance and safety improvements,
- system integration within the overall I&C structure (see 4.5.3).

The maximum benefit from the project could be impaired by a "piece-for-piece" system replacement approach, although such a method could appear simpler and might involve less on-site interference.

Different degrees of modernisation, i.e. from limited refits to partial or large upgrades, also strongly influence the number and nature of the required specifications. This applies especially in the areas of system integration within the plant (see 4.5) and HMI (see 4.6).

The project scope will influence the information and document flow at interfaces, which should therefore be well defined and formalised in the BRS. This is of special importance if several different contractors provide equipment within the total project. Examples include cables laid by a separate contractor to the equipment supplier and software supplied by a separate organization or by the utility.

At the system design stage, scope split will influence information exchanged at the interfaces with the existing plant. The requirements should therefore include details of:

- information tagging, electrical signal standardisation, signal failure conditions (in Section 6 of Appendix III),

- erection and installation activities and associated responsibilities (in Section 2.10 of Appendix III),
- commissioning test provision and activities (in Section 2.10 of Appendix III),
- periodical testing provisions (in Section 2.2 of Appendix III).

Figure 2 illustrates the organizations which normally lead the activities at each phase of the project, and their relative degree of involvement.

4.2.3. Schedule and phasing of the project

The time schedule of the project itself and the way this schedule fits within overall planning of plant outage (or system erection in case of a new plant) has a big influence on the detailed design and the development of the detailed plans for manufacture, installation and test. The future plant outage schedule should be considered. The project should balance short refuelling outages and any extended outages where inspections or other work is planned, which allow more extensive installation and commissioning work.

The equipment systems should be integrated in suitable groups to maximise work and testing possible in the factory and to reduce to a minimum site erection and testing time needed. Possible actions to reduce the time needed for the project should be considered. For example:

- standardisation of cabinet sizes, cable entry and cabling method (see Section 2.7 of Appendix III),
- installation of cabinets before delivery of modules, with phased sections of the FAT,
- hardware techniques such as plug-for-plug cable replacements, cable preforming,
- software techniques such as double verification of configuration data, with flexible methods of data correction,
- use of simulators for I&C software validation (see Section 2.11 of Appendix III).

Proper design of interfaces (see above) also helps to reduce the planning needs at test and verification stage on site.

4.2.4. Project budget versus cost

The availability of a given budget is a basic influencing and constraint factor. It may influence the choice of technology and the extent of modernisation. It may influence the time-scale, for example design work may be done early with a delay until funds are available for the manufacture of the equipment.

The attitude of any sponsor organization to the extent of the refit or upgrade and the choice of contractors may be of great importance and may strongly influence the project. The scope split and the details of the documentation of requirements will depend on the attitude and requirements of a sponsor.

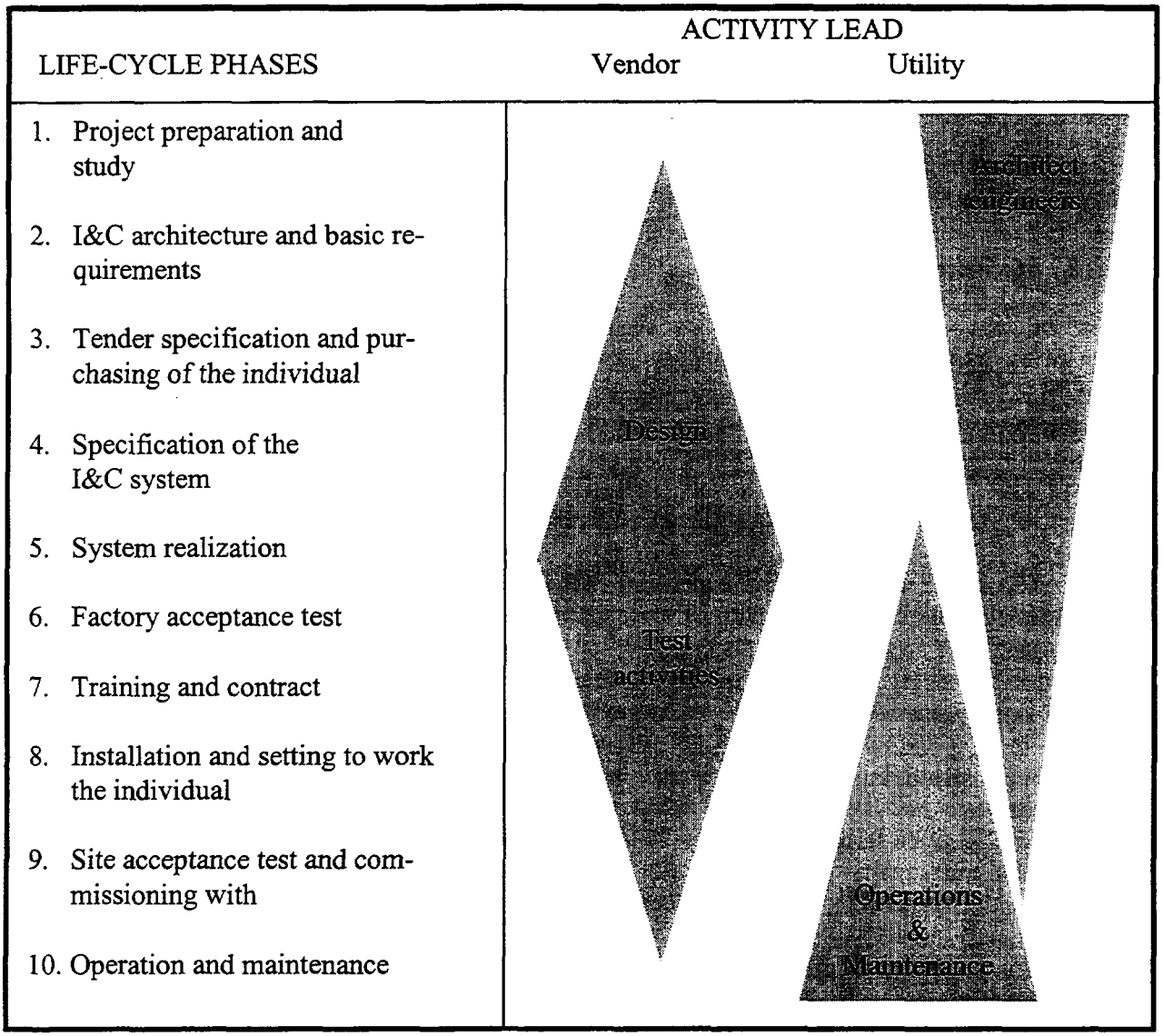


FIG. 2. Organizations which normally lead the activities at each phase of the project, and their relative degree of involvement.

4.3. FACTORS LINKED TO SAFETY AND OPERATIONAL IMPORTANCE

4.3.1. Safety classification

The safety classification of the I&C systems within or affected by the project is a major influence on requirements. Safety category will affect the requirements for applicability and gradation for rules, norms and standards (see Sections 2.2 and 2.4 of Appendix III).

Safety category influences requirements for:

- system hardware qualification,
- system and application software qualification,
- the system required reliability, probability of failure and frequency of spurious action,
- system redundancy, changeover and standby functions,
- the QA programme for the project,

- the isolation needed at interfaces between systems (in Section 2.2 and 2.6 of Appendix III),
- the periodical testing capabilities (in Section 2.2 of Appendix III),
- the extent and type of FAT and SAT, including software V&V.

The impact of the project on the plant technical specifications (such as safety limits monitored by the operators), which have safety importance, should also be examined carefully.

4.3.2. Operational importance

Considerations of operation of the plant could lead to requirements on the systems (in Section 2.2 of Appendix III). A system of high operational importance may need the same attention to definition of its functionality and performance and to quality as a system with safety significance (see Section 2.1).

4.4. FACTORS ASSOCIATED WITH REGULATION AND LICENSING

Regulation and licensing experience and attitudes have a strong influence on system requirements. Some safety authorities are experienced in newer technologies, others will still be developing their approach. There is therefore some uncertainty in defining the requirements for work needed for licensing support. So far as practicable, the regulatory assumptions and the work needed for the safety justification should be defined in the BRS (see Section 2.4 of Appendix III).

When specifying the applicable rules, norms and standards, it is of importance to describe also the precedence ranking that should apply in case of contradiction or overlapping between listed documents. A given standard could also be adopted only for requirements on a specific topic, i.e. with limitations and suitable interpretation. A detailed description of the licensing aspects of an I&C modernisation project can be found in Section 8 of [2].

It is important to plan for the production of all documents taking the requirement for safety justification into account. In particular, if the US approach of NUREG 0800 Section 7 is followed, special documents may need to be produced.

4.4.1. General national or international applicable rules, norms and standards

Some nations do not have established preferred norms and standards, but require that a coherent and internationally accepted set of standards is applied. As references, Appendix IV gives a grouping of representative standards applicable to US, European and international standards. Software standards in particular are being developed rapidly. It is therefore important that the standards applicable to the project are considered carefully. They should be read and referenced systematically to ensure a consistent approach representing good and recognised practice.

The implications of the general national rules and legislation on workers' health and safety, physical protection, electrical installation design, radiation safety, etc. must be taken into account

In accordance with the national regulatory framework all applicable national and international documents should be listed, to cover the aspects of:

- I&C systems design, realisation and modification,
- hardware and software qualification,
- I&C systems commissioning and periodical testing,
- HMI design, verification and validation, as far as applicable.

4.4.2. Applicable QA & QC programs

QA/QC relevant norms and standards (typically IAEA Safety Series No. 50-C/SG-Q [14] and ISO 9000 series) and project specific requirements should be indicated. Relevant requirements for safety classified equipment include:

- ten year or life-time records of specifications and manufacturing drawings,
- traceability of materials,
- traceability of functional requirements through documentation,
- special methods of hardware modification and change control,
- special methods of software modification and regression testing.

4.4.3. Licensing support

The supplier's support for documentation and activities that are needed during the licensing process with the safety authority should be defined. Associated requirements should be stated (see Section 4 of the BRS.). It is important to remember that the licensing related activities could start at feasibility study stage and will last even after the systems have been put in operation. The extent of support needed from the supplier for the production of safety case information should be considered carefully.

4.5. FACTORS LINKED TO I&C SYSTEMS INTEGRATION

The I&C systems integration approach influences the interfaces to the installed plant, the power supplies and services, and the interfaces to other new systems. Comprehensive systems integration, well planned and undertaken fully, is vital to the success of any refit or upgrade project. The requirements for designs should aim to minimise this work consistent with the goals of the project. The system integration influences the amount of work needed for modification of the existing plant layout and auxiliary systems.

A detailed discussion of specific limitations and constraints can be found in Sections 7.4 and 7.5 of [2]. Some major factors are outlined below.

4.5.1. Layout aspects

Existing and proposed equipment layout influences the requirements for:

- civil work needed,
- addition of false floors for computer equipment,
- floor loading and hold-down points for equipment,
- space available for equipment,
- access routes for installation,
- workshop areas for installation,
- workshops for maintenance of computer and other equipment.

The introduction of additional I&C cabinets should be done in a way which avoids a large amount of civil work. The distribution of the new or refit cabinets in different plant areas to those being replaced should be considered, provided that the environmental conditions in each location are those which are needed. Close liaison between the supplier and the utility is needed. In the case of

lack of available space, areas not previously considered for I&C equipment may be exploited, such as switchgear rooms, provided suitable environmental control is possible.

If the upgrade scope includes the control rooms, their available floor and panel areas impose basic constraints on the location of new components. Generally, the introduction of digital systems and the use of VDUs reduce the need for space compared to traditional analog solutions. This factor will be important in partial upgrading, when further components (e.g. VDUs) are to be added within the existing control room layouts. Space will be needed for the computer equipment which operates the new VDUs, and this may be constrained to be within a cable distance of about 20 metres.

Other factors to be considered include:

- existing HVAC system configuration and capacity,
- existing passive and active fire protection system configuration and capabilities,
- physical independence and separation of sections of a system,
- HELB concerns and equipment qualification (Section 2.7 of Appendix III),
- environmental conditions to be taken into account (Section 2.5 of Appendix III).

The existing normal and worst case environmental and EMI conditions in the relevant plant areas are important factors for the definition of the degree of protection or of qualification needed for I&C components and cabinets and for their location in the plant. This is influences layout as a constraint.

4.5.2. Electrical power supply

The available electrical power systems (AC and DC switchboards and distribution boards, redundancy and independence, diesel back-up, battery source capacities) are influences and constraints to be taken into account during I&C system basic functional analysis and architecture definition. Related impacts must be stated (see Section 2 of the BRS).

The specific characteristics of the existing I&C systems power supplies should be taken into account during detailed I&C system design to ensure proper operation when needed. Associated figures and requirements should be incorporated (see Section 5 of the BRS). These include:

- nominal and degraded voltage and frequency limits,
- harmonics ratio,
- supply interruptions,
- supply priority during reactor trip conditions,
- conditions during battery lowest charge and charging periods,
- voltage dips and spikes.

Suppliers of proprietary equipment are often not aware of the voltage and frequency extremes experienced on a power plant, and they should be informed of these carefully.

Clearly, new supply distribution boards or sources will be costly but may provide the simplest interfaces.

4.5.3. Integration within the overall I&C structure

The existing overall I&C structure influences the requirements for integration of the new systems. At the basic functional analysis stage, requirements will be influenced by the need for smooth integration of the new systems within the existing I&C structure. This can lead to alteration of the scope and limits of the project:

- to provide for a more coherent final I&C structure,
- to get clearer interfaces,
- not to impair coherency or feasibility of further possible I&C modification.

During the detailed I&C system design phase, integration influences the requirements both for physical and for time-based installation links between the different I&C systems. These should be reviewed to identify requirements for:

- time constraints and phasing in time,
- isolation and separation,
- cables,
- interface physical locations.

4.5.4. I&C integration within the control rooms

The feasibility study should require the control room integration to be discussed. This will influence the requirements in the BRS. The detailed design should identify the method of integration into the control room, paying attention to human factors and operator acceptance, and to the preservation or improvement of fire separation and fire limitation means. Constraints may arise, especially in the case of limited refits, due to the obsolescence of existing components in the control room panels. In these cases, the acceptable sizes of the new components (e.g. auto/manual control stations) should be such as to fit with no component modification into the existing panel arrangements.

The physical integration of new equipment into a control room should be done only after close consultation with the operating staff, their acceptance of the changes, training in the use of the equipment, and amendment of operating instruction manuals where relevant. These requirements should be reflected in the relevant specifications.

4.6. FACTORS LINKED TO PROCESS OPERATION AND HMI

Generally, refits have an impact on the arrangement of control rooms and on plant procedures. The factors linked to plant operation and HMI aspects should be carefully considered, since they are directly related to plant safety and reliability. An important constraint arising from control room upgrades is the need to allow for human factors and operators attitudes. This applies both at the elementary level such as colours of lettering, language and style and also at the advanced level such as allowing for the potential task analysis of the control room. Human factors analysis may result in alterations of layout. These factors are most important for a complete upgrading of the control rooms. However, their effects should not be neglected even for limited upgrading or partial refurbishment.

The feasibility study should identify the operating staff roles, the major effects of operation and HMI requirements on the project. The BRS should include the requirements arising from these (see BRS Section 2).

Specific aspects related to operational HMI are discussed in Sections 6.5, 6.7 and 6.8 of [2]. In the following, some major factors are outlined.

4.6.1. Control room and operating staff composition and organization

This is a key factor if a complete or partial task analysis is to be carried out for the definition of the control room layout. Also the division of responsibility between the staff, normal for the utility practice, affects requirements. The design should identify as exactly as possible the responsibilities of the different operating staff members and their supervision before attempting any redesign of the control room layout, to avoid possible incorrect or unsafe location of controls and indication groups.

The possible refit of a back-up or auxiliary control room for use if the main control room is not operable, or of a technical support centre, will require an exact determination of the role of the new room, the circumstances in which it is manned, and the type of staff who will operate it. This influences the requirements for the equipment and services in the room strongly.

The utility may require modifications to the detailed plant operating and emergency procedures to be limited.

4.6.2. Degree of automation intended

The degree and the structure of the process automation have a great influence on the structure and the functionality of the I&C refit as well as on the resulting control room layout. Analysis work will be needed to confirm or identify the requirements (see Appendix II).

The feasibility study should consider and basic requirements specification should define targets when appropriate for:

- automation of operational sequences,
- station power control automation,
- automatic power limitation,
- automatic protection.

The detailed design specifications should include requirements for validation of the automatic control and protection functions by computer modelling, as described in Sections 6.2.1 and 6.4.3, and for validation tests to demonstrate all functions during FAT and SAT.

4.6.3. Available operator competence and skill

The operator formal qualification level, experience, competence and skill influences the choice of the HMI, both in the general philosophy (e.g. use of VDUs for control) and in the detailed implementation (e.g. use of special symbols, windowing, etc.). In cases of upgrading of one unit alone of a plant with several units, the utility policy with respect to operators interchangeability could lead to limits in the modifications allowed in this area.

The feasibility study should identify the operator skills available and their attitudes to refits and upgrades. The BRS should take account of these skills and attitudes. Operators should be kept informed of the project progress and intentions throughout the project. It is essential to retain utility site staff co-operation throughout the project.

Operator competence and skill influences the training requirements and the operation and maintenance requirements (see Section 4.7). Site software expertise may allow some part of the modification and retest process to be done on site.

4.6.4. Utility philosophy for centralised or local control

The utility may require facilities for local switchgear control of plant or control at the plant itself. This may be needed for all safety plant systems, or all systems needed to attain hot shutdown, or for all plant. Their normal practice clearly imposes basic constraints on the I&C structure and on control rooms. The utility requirements should highlight this topic. This may affect the provision of computerised multiplexed or touch screen control very greatly, since a standby control point may be needed for multiplex system failure. The requirements for the addition of an auxiliary or back-up control room will also be affected by this.

4.6.5. Tools available for V&V of the upgrade designs

The tools available for V&V of the upgrade will influence the requirements. If a plant simulator is available, it will be of great use in the evaluation of the HMI and in task analysis. Such simulators are recommended. Suppliers may have existing tools which allow verification of the functional requirements.

The feasibility study should identify the need for such tools and the possible supply and installation of simulators. The BRS and system specifications should define requirements for the use of tools for the verification tests of requirements or of new equipment and for the evaluation of the integrated human-machine performance. They may be valuable as support for a safety case.

If simulators are needed, their design and provision should be considered for inclusion in the project. The training characteristics and support tools should be selected to be suitable to the technical culture of the plant personnel.

4.7. FACTORS LINKED TO I&C SYSTEM OPERATION AND MAINTENANCE

4.7.1. Maintenance, repair and maintenance strategy

The utility may decide to rely either mainly on the supplier's after sale service or mainly on his own resources. This will affect the requirements for the number of spare parts to be available at the plant and the training program to be planned for maintenance staff. Software changes after handover for operation will be needed, and the utility should plan for this. The strategy should be agreed and defined early in the project.

The requirements arising from the strategy should be integrated in the BRS (see Sections 3 and 12).

Provision to cope with obsolescence of I&C systems equipment and to preserve their initial qualification should be stated according to the decision taken above.

Hardware and software configuration management for all equipment and programs of the systems should be planned, along with suitable long-term archive means and procedures.

4.7.2. I&C system periodic testing

Facilities needed for periodic testing of the systems will influence the detailed design. These facilities depend on utility practice and on safety category, which should be agreed in the BRS development. The BRS should define the requirements and reference any relevant standards. The impact on operation of the systems, coverage of the tests and associated periodicity should be specified (see Section 2).

At the detailed design stage, according to the auto tests and diagnostic capabilities embedded in the systems to be implemented, a more precise specification of the tests should be produced and included in the operation and maintenance manuals.

4.7.3. Hardware and software change control

The safety category and regulatory requirements will influence the QA planning and the design of procedures for hardware and software modification. Some changes may be possible (for example, selection of turbine control mode) from the operator's desk, some changes will require supervisory authorisation on site (such as alarm level changes), and some changes will require detailed analysis (a change to a software function), and suitable detailed testing after inclusion, with the facility to undo the change if not satisfactory.

Detailed design and planning should pay close attention to the processes of hardware and software change and change control.

5. ELEMENTS OF REQUIREMENTS

The requirements are grouped against four main headings:

- project requirements, covering scope division and responsibilities, costs, time-scale and planning, and system support and services,
- system requirements, for the functionality, performance, dependability, operability and safety characteristics of the system,
- implementation requirements, for the technology required, software approach, the engineering interfaces and the plant services,
- qualification requirements and testing.

5.1. PROJECT REQUIREMENTS

5.1.1. Scope division and responsibilities

The requirements for the feasibility study should define the intended scope of systems involved in the refit or upgrade work, and the relative responsibilities foreseen for:

- the utility or their agent,
- the site organization and site staff,
- the architect-engineer,
- any project co-ordinating body,
- the suppliers of equipment, software or services,
- any consultancy or source of specialist advice.

These scope and responsibility statements should be enlarged in detail in the invitation for tenders, and confirmed in contract negotiations. The utility or his sponsor will normally be expected to take responsibility for payment of main contractors and suppliers of services.

Responsibilities would normally be taken by the utility and his agent acting for him for such aspects as:

- definition and agreement of the detailed scope of the project,
- acceptance of the detailed design of the supplier,
- provision of site services and supplies,
- site assistance, cranes, lifts, location for on-site accommodation for supplier's staff,
- project management.

The utility may wish to take responsibility for some aspects of the design, for example the task analysis of the effects and changes made in the control rooms, the panel layouts in the control rooms, the assignment of alarms, the design of VDU display layouts and other matters where his direct experience and expected use of the system facilities have a strong influence. When this is done, the interfaces with the supplier must be clearly defined.

5.1.2. Costs

Cost is a most important project factor, and the statements of requirements and project plans must always take account of actual or potential costs. Contract matters and contract arrangements are not within the scope of this report, so no discussion is given of cost control or limitation methods. Cost plans will be needed for major projects, to show the time-scale of expenditure and the payment progress stages. These should be agreed at the order placement stage.

5.1.3. Time-scale and planning

Time-scale and planning are essential parts of the management of the project. The requirements at the feasibility study stage should call for outline plans of the design, manufacture and installation process, and for time-scales of the refit or upgrade which allow for planned outages of the plant.

The invitations for bids should require the tenders to show basic plans for the major activities, with firm time-scales for design, manufacture, software production, integration, testing and installation.

The detailed design phase should involve the development of plans for:

- system verification and validation,
- qualification of hardware,
- qualification of software,
- system integration,
- factory acceptance test (FAT),
- site installation and setting to work,
- site acceptance test (SAT),
- commissioning with plant,
- training,
- operation and maintenance.

These plans should show the intended activities and the expected time-scales or time of undertaking the activities. Preliminary plans to show the strategy of qualification, integration, testing and installation are valuable for large projects. The detailed FAT and SAT plans should define the exact process and anticipated results of each test. The requirements for and types of testing, V&V and qualification are discussed further in Section 5.4.

5.1.4. System support and services

System support does not relate directly to the primary system functions, but is of great importance for the project success. This includes requirements for:

- supporting services provided by the supplier covering:
  - training,
  - software maintenance,
  - spares,
  - hardware maintenance and module repair,
- quality assurance,
- special testing facilities, other than covered by qualification testing, FAT and SAT.

5.1.5. Documentation

Documentation requirements should be stated in the invitation for bids, and agreed during contract negotiations. Allowances should be made for more detailed agreements on final documentation later in the project. Allowances should also be made for revisions to documents and technical specifications to reflect the as-built state, in particular in the context of the safety case. Agreements on documentation should include definition of the requirements for:

- design information provided for information or approval by the utility,
- design drawings, equipment layouts,
- lists of power supplies and services required by the supplier,
- support documents and analysis reports needed for licensing and the safety case,
- software specification, design, and code listings,
- system databases and system configuration details,
- qualification reports for hardware and for software,
- procedures and reports of FAT and SAT,
- commissioning tests and procedures,
- spares recommended for site use,
- training course notes and documents,
- operation and maintenance manuals and handbooks.

5.2. SYSTEM REQUIREMENTS

The system requirements are described using basic elements that should be included at different stages of the work. These are derived from IEC-1069 [17], as elements needed in assessment of any I&C system. Any element may contain a number of more detailed items. All elements that are significant during the system life cycle should be evaluated and included in the specifications suitably. Note that the majority of the elements are important to the testing phases of a project.

5.2.1. Functionality

Functionality describes the extent to which one or more functions are performed, and the nature of those functions. The functionality of a system depends on the range of functions provided, the capability to execute the functions in real time (or at the required time), and the flexibility to select and implement the necessary functions if and when they are required. The functionality of

predeveloped products should be evaluated in relation to the intended application. Alternatively the products may be evaluated to identify extensions or modifications to the product to meet the intended application requirements.

The following functions can be expected to be important, and to require careful definition:

- process interface functions to receive data from sensing devices and send data to actuating devices,
- logic processing to make decisions on actions required,
- calculation algorithms and formulas,
- data processing functions which may be dedicated to individual tasks or may support a combination of tasks required to achieve the system mission,
- communications functions to provide communication between modules or to other systems,
- human interface functions to provide process operators, technical professionals, maintenance personnel and management with access to the system and process information on the process,
- interface functions to external equipment to operate plant or alarms or to provide display information.

Characteristics, or sub elements, of functionality that may be relevant to system requirements specifications include the following:

- flexibility, including:
  - configurability,
  - programmability,
  - expandability,
  - segmentation,
  - standardization,
- functional coverage,
- functional capacity.

Examples and detailed discussion of the main requirement items above can be found in Section 7.3.4 of [2].

5.2.2. Performance

Performance describes the extent to which the functions provided can be executed under defined operational and environmental conditions. This element should also include characteristics required if a system or its components fail. The required operational conditions should be determined and compared to those designed for, or experienced in use of the product. The consideration of operational history may be important to performance evaluation and specification. The performance requirements should include:

- accuracy (zero and full scale, linearity),
- stability (drift and repeatability),
- response time in normal and loaded conditions,
- consistency of behaviour,
- any requirement for equipment qualification, to show suitable performance of all functions in the worst expected environment.

Qualification is discussed in Section 5.4.2 and in Section 7.3.5 of [2]. The performance of some designs may depend on system loading. Requirements should consider the performance needed at major plant trips, when the rapid and continued initiation of many hundreds of alarms can occur.

5.2.3. Dependability

Dependability describes the extent to which the system can be relied upon to perform its intended functions under defined operational and environmental conditions. This includes requirements for:

- availability (reliability and maintainability),
- probability of failure on demand,
- frequency of spurious actuation,
- assessment work needed in association with PSA studies,
- robustness, changeover and standby features,
- safety integrity level (hardware and software),
- features needed to withstand common cause failures,
- security against accidental or malicious actions.

The safety integrity level of potential system products should be compared with the software and hardware requirements for dependability. Proven operational history may be relevant to dependability and if so should be addressed in the requirements.

5.2.4. Operability

Operability describes the features of a system which allow it to be used simply and effectively and kept in use easily and without degradation. Operability depends on several factors, including procedures for access to and entry of information and data into the system, the extent of information obtained by a single user request, the information formats used and the interface devices used. Operability has a strong influence from human engineering.

Other characteristics of operability include:

- actions required on failure of modules, such as:
  - system hot or warm changeover,
  - adoption of a predefined state at failure,
- facilities for modification,
- facilities for operation and maintenance,
- system safe operation during maintenance and testing,
- on-line testing.

The consideration of operability should include all aspects of the HMI.

Consideration of system operational history may be relevant to evaluation and specification of operability.

5.2.5. Safety characteristics

Safety characteristics are those describing the extent to which the system will not by itself impose potentially hazardous conditions on the reactor plant, on personnel or on the environment. Safety characteristics of the system or sub-elements include:

- personnel safety,
- process safety,

- defence in depth features,
- the safety of the system itself.

The safety characteristics of an I&C system depend on the inherent safety of the system, for example the use of fail-safe engineering principles, and the use of suitable EMI suppression to prevent external effects. Note that if a system is required for a role important to safety on a reactor plant, the system requirements will be mainly defined by its functionality, dependability and operability, which define its capability to provide its safety function.

5.3. IMPLEMENTATION REQUIREMENTS

5.3.1. Technology

The technology element of requirements concerns the basic nature and operating principles of the equipment system. Examples of technology are the use of:

- fail-safe,
- field programmable arrays (ASIC, EPLD devices),
- digital computer or microprocessor technology.

These basic requirements should be defined. Requirements for specific instruments or specific operating principles may include:

- thermocouples or resistance temperature detectors (RTDs),
- pressure, level and flow measurement instrument type (0 - 20 mA, 4 - 20 mA, ...),
- in-core and ex-core flux measurement instrument type.

Previous qualification of hardware and of software is also relevant. Specific subjects include:

- compatibility of hardware and software,
- computer communications methods,
- availability of standard modules for standard functions,
- special development needed.

5.3.2. Software

The software element of requirements concerns the software approach, standards to be followed and the degree of integrity required in the software. Requirements should include:

- software languages and methods,
- software life-cycle, documentation, verification and validation,
- automatic software generation features,
- software production approach and internal code standards,
- use of proprietary software not in the direct control of the system supplier,
- evaluation and assessment of proprietary software,
- software standards and specific software QA,
- software safety integrity level.

The requirements should identify the safety role of the software, any special V&V of software, and the licensing support needed. The requirements of IEC880 will be applicable for safety system software. The IEEE software standards give a comprehensive basis of requirements for software design, production and support through the life-cycle.

5.3.3. Engineering

The engineering element of requirements concerns the interfaces on the plant and detailed requirements for construction methods. Clearly, all potentially relevant engineering subjects cannot be listed here. Some important aspects are given only. Interface requirements on the plant are concerned with:

- cable access and cable routes available,
- supplier's cable requirements for the new system,
- power sources available and their characteristics,
- power required by the supplier,
- rooms, areas and buildings available for equipment,
- supplier's layout requirements for the new equipment,
- mounting and holding down for equipment,
- heating, ventilation and air conditioning (HVAC) services available,
- physical properties such as heat dissipation and weight limitations.

Construction methods requirements are concerned with:

- module and component types, identification and interchangeability,
- mounting of components and printed circuits,
- plugs, sockets, internal cables and wire routes in cabinets,
- cable terminals and cable entry to cabinets from below or above,
- cabinet shape and size, construction, sealing, door locks, markings and labels,
- cable termination and individual wire marking methods.

It can be an advantage to produce a single specification covering requirements for all construction topics, for all suppliers. If this is not provided, the supplier should define to the utility the methods he will adopt.

5.4. QUALIFICATION AND TESTING REQUIREMENTS

5.4.1. Verification and validation (V&V) and testing

Verification and validation (V&V) and testing are costly and should be defined early. The requirements should be stated in the invitations to tender and agreed in principle at the time of contract negotiation. Section 5.1.3 discusses the development of plans for these activities. The test requirements should be agreed for:

- type tests, in which a representative unit or module is tested to show the full range of its capabilities,
- prototype tests, to show correct operation of a newly developed module or unit,
- manufacturing test, in which each module, component or device is tested in a summary way to show correct manufacture,
- integration tests, where the modules and units of a complete subsystem or system are shown to operate together,

- FAT, in which the complete set of equipment and software of a major subsystem or system are shown by formal tests to operate as required,
- SAT, in which the installed system on site is shown to operate for its full range of capability, for formal acceptance by the utility,
- commissioning tests, in which the system is shown to interface and to operate correctly and safely with the existing plant.

Some of these tests may not be required to be reported, but may be required to be done with records available for QA audit in the supplier's works. Some may not be usual practice and would be omitted. It is usual for the FAT and SAT to be reported formally, with retention of the detailed test records in an auditable form. These would normally be a reference from the safety case.

Software V&V methods and tests are discussed in Ref. [10]. Verification should be done of all software design and code documents, or their equivalent. Validation of the software should be done by integration tests, FAT and SAT, against the original requirements. Validation of the requirements and the implementation may be done or assisted by the method described in Section 6, using simulations of the plant already validated by other means. Software V&V may require analytical methods of software code decomposition and complexity assessment, and may require special testing using test systems (test harnesses) which compare a proven model of the required functions against the new system. These are normally only relevant for the highest safety and reliability requirements.

5.4.2. Qualification

Qualification is required for safety system instruments which are subject to harsh conditions. The testing requires detailed definition of tests and recording of results, for several representative instruments, and is defined in IEC980 [33] and IEC780 [8], together with IEEE323 [21] and IEEE344 [22]. The detailed requirements for the acceptance of previously qualified instruments should be agreed carefully.

Qualification testing of equipment will be needed, to show suitability for the intended environment. This may be accepted as covered by the normal performance specification of standard modules, where safety is not concerned, but normally requires audit of module or unit type tests to support this claim. Often, an elevated temperature test of a cabinet during FAT is needed for confidence. For safety system cabinets, formal testing is necessary, and may require seismic tests if applicable to the plant site. These require special attention to the site conditions, the building seismic spectra and response at the intended building locations. Seismic tests are normally undertaken by specialist organizations.

Qualification testing of software is normally part of the software V&V process, but may require detailed reporting of the results and audit for the records of the design and development. Qualification of previously used software is discussed in detail in Ref. [10]. These records of qualification will normally be required as references for the system safety case.

The design phase should define the qualification plan for both hardware and software (see Section 6.4.4). This will need full development into the detailed tests needed for qualification of the equipment and software. Normally,

- hardware qualification is based on environmental testing, analysis and feed-back of experience,
- software qualification is based on a qualitative evaluation of the confidence in the software quality; it is based on the analysis of the design, development, verification and validation and QA of the software,

- operating experience may be a compensating factor for lack of some detailed documentary information on a proprietary product, such as a software operating system.

The qualification plan should distinguish between:

- The qualification of the general (non plant specific) properties of the I&C product system. To a large extent these general properties may be covered by the pre-existing qualification of the individual modules and of the system software.

- The qualification of the plant specific features and notably of the application software of the I&C system.

The required input information includes:

- documentation on pre-existing qualification of the product system,

- the status of the documentation needed for any additional system qualification, in particular concerning:
  - the existing accessible, existing proprietary, and configurable,
  - the amount of the documented operational history.

Hardware qualification should show that the equipment operates correctly in the extreme environmental conditions to which it may be exposed in operation. This may require environmental chambers or temporary tents able to be heated and brought to high humidity. Seismic testing may be needed, using a specialist contractor. Guidance on methods for software V&V is given in an IAEA report [10]. For safety system software, the requirements of IEC880 and its supplement will apply. Independent software V&V may be needed.

TABLE I. LIFE-CYCLE PHASE: PROJECT PREPARATION AND FEASIBILITY STUDY (SECTIONS 3.1.1, 6.1)

Initial activities: Development of scope of feasibility study **Main activities: Feasibility study**				
Objectives of the phase activities	**Inputs & constraints**	**Main influence factors**	**Requirements, outputs & constraints**	**Deliverables**
- Identify modernisation goals. - Identify modernisation scope & constraints. - Identify I&C affected and constraints. - Identify target time-scale.	- Utility requirements. - Importance to safety. - Plant documentation. - Plant context: lay-out, power supplies, cables, interfaces.	- Status of as-built documents. - Scope split, interfaces. - Safety category. - Layout, space, cables and services. - Utility attitude to digital technology. - Utility practices.	- Modernisation goals. - Functionality. - Performance. - Dependability. - Operability and HMI; - Preferred technology. - Services and space needed.	**- Feasibility study requirements.**
- Develop conceptual design alternatives for new systems with comparisons. - Identify probable risks, costs, time-scales.	- Utility staff knowledge. - Information from similar plants. - Information on equipment size and service requirements. - Products and software from potential suppliers.	- HMI & automation targets. - Preferred implementation of engineering. - Preferred technology. - National & international codes and standards. - National licensing practices.	- Conceptual design & engineering approach. - Lay-out, service requirements, - Technical uncertainties. - Probable costs. - Time-scales. - Advantages and disadvantages.	**- Feasibility study report.**

Note: If the feasibility study is done to meet a simple request, rather than a formal specification, the feasibility study report should itself define the goals, functionality, performance and other requirements indicated.

TABLE II. LIFE-CYCLE PHASE: I&C ARCHITECTURE AND BASIC REQUIREMENTS SPECIFICATION (SECTIONS 3.1.2, 6.2)

Initial activities:	**Review of suitable products and suppliers;** **Review of I&C, sensors and actuators;** **Human factors review of control room (where applicable);** **Consideration of safety improvements, fire and other hazards.**
Main activities:	**Development of design concepts;** **Development of basic requirements specification.**

Objectives of the phase activities	**Inputs & constraints**	**Main influence factors**	**Requirements, outputs & constraints**	**Deliverables**
- Provide and justify a conceptual architecture of the I&C systems for the refit or upgrade project.	- Feasibility study report. - Goals of modernisation. - Utility requirements. - Plant diagrams, drawings and documentation. - Suppliers' information on products, tools and facilities.	- Codes and standards. - Utility preferences. - Safety and operational improvements required.	- Safety classification of I&C functions & systems. - Requirements for I&C safety, automation, control and display functions.	**- Product review.** **- I&C review.** **- Human factors review.** **- Safety review.** **- Conceptual I&C architecture.**
- Define the main interfaces between the equipment. -Define interfaces between the engineering activities. - Provide the Basic Requirements specification for procurement of the I&C systems concerned. - Qualification strategy for equipment and software.	- Product, I&C, Human factors and safety reviews. - Conceptual I&C architecture. - Equipment and software available. - Consistency of plant information database. - Established QA requirements and programs.	- Utility preferences and practice. - Scope split, interfaces. - Safety category. - Layout and services. - Utility O&M approach. - Utility attitude to digital technology. - Regulatory requirements. - Budget costs.	- Project. - System. - Implementation. - Qualification. - Testing. - Overall I&C/HMI architecture. - Boundaries & Interfaces of systems & of modernisation process. - Requirements for implementation and installation. - Time-scales.	**- Basic requirements specification.** *Note: This stage of specification for bids is supplier independent*

TABLE III. LIFE-CYCLE PHASE: TENDER SPECIFICATION AND PURCHASING OF THE INDIVIDUAL SYSTEMS (SECTIONS 3.2.1, 6.3.)

Initial activities: **Specification of requirements for quotations.** **Main activities:** **Suppliers' initial development of designs, costs and time-scales; Suppliers' quotations, place order**				
Objectives of the phase activities	**Inputs & constraints**	**Main influence factors**	**Requirements, outputs & constraints**	**Deliverables**
- Provide the requirements specification for bids. - Preparation of bid evaluation criteria. - Issue invitations to tender.	- basic requirements specification. - Detailed information on suppliers' products. - Detailed information on engineering tools environment from the suppliers. - Suitability report on each supplier asked to quote.	- Regulatory position. - Scope split. - Interfaces. - Utility practice. - Safety category. - Layout and services. - Utility O&M approach. - Qualification strategy for hardware & system/application software.	- Project. - System. - Implementation. - Qualification. - Testing. - Overall architecture. - HMI. - Requirements on interfaces. - Codes and standards. - Engineering software tools.	**- Requirement specification for each individual system .** **- Invitations to tender.**
- Suppliers' tender preparation. - Selection of product and supplier. - Evaluate bids and place order.	- Requirements specification for the system. - Identification of time-scales.	- Compliance to codes & standards. - Costs of products, specific interfaces, qualification & engineering.	- Hardware and software extent of supply. - Time-scales for implementation and installation. - Cost plans and quality plans. - Details of design and architecture. - Equipment and software details. - New/novel designs needed. - Risks, contingencies.	**- Suppliers' tenders for each system.** *Note: The use of existing software will need clarification and justification, depending on the safety category.* **- Order placed on selected supplier.**

Note: After product/supplier selection and before placing the order the above specification is to be amended in order to reflect decisions taken during bid-discussions and to serve as contractual base for the project.

TABLE IV. LIFE-CYCLE PHASE: SPECIFICATION OF INDIVIDUAL SYSTEMS (SECTIONS 3.2.2, 6.4)

Initial activities: **Interchange of design and interface information.** **Main activities:** **Development of system requirements information;** **Functional requirements specification;** **Production and agreement of detailed integration and testing plans.**				
Objectives of the phase activities	**Inputs & constraints**	**Main influence factors**	**Requirements, outputs & constraints**	**Deliverables**
- Generate the system requirements. - Define the software requirements.	- Specification and contract documents of the previous phase. - Functional requirements diagrams.	- Regulatory positions and guides. - Equipment qualification strategy. - Software qualification strategy.	- Functional assignments. - Dependability. - Operability. - Testing. - HMI.	
- Generate and validate the application software functions. - Generate plans for integration & validation. - Generate qualification plan.	- Independence between designers and development of validation plan for Category A. - Utility requirements. - Quoted design. - Contractor extent of supply and of work. - Work to be done by the utility or customer.	- Available simulation facilities. - Project time scale. - Utility organization. - Availability of qualification reports.	- Detailed software and engineering requirements. - Details of components, cards, cubicles, etc., must be defined as requirements for manufacture. - Requirements for product qualification and plant specific features.	**- System requirements documents.** **- Software requirements specification.** **- Agreed planning proposals.** - Integration plan, software QA plan, validation plan. Qualification plan - hardware. Qualification plan - software.

Note: The planning activities for site installation, test, commissioning and O&M are shown in Tables VIII to X, and will depend on this phase. The design and planning documents may be for information or for approval by the utility.

TABLE V. LIFE-CYCLE PHASE: SYSTEM REALISATION (SECTIONS 3.2.3, 6.5)

Initial activities: Definition of detailed design and interface information. **Main activities: Equipment manufacture and subsystem test;** **Software production and verification.**				
Objectives of the phase activities	**Inputs & constraints**	**Main influence factors**	**Requirements, outputs & constraints**	**Deliverables**
- Development of detailed system design. - Development of detailed software design.	Design and planning documents of the previous phase: - System requirements, - The hardware & software architecture, - The agreed detailed plans .	- Utility practices. - Scope split and extent of utility direct design activities. - Documentation of previous design. - Regulatory approach. - Safety category. - Independence of V&V.	- Lists of all sensors and actuators and characteristics. - All control room controls. - All control room indications, alarms and VDU designs. - Equipment layouts. - Finalisation of all plans (see Table IV).	**- Detailed hardware and software designs.** **- Agreed detailed design documents.** - Equipment layouts. - Service, power requirements. - Signal & output allocations, - VDU designs
- Manufacturing and test of standard components. - Development of specific equipment. - Software production. - Integration of hardware & software for FAT.	- Specifications of individual hardware & software modules. - Contractor scope of supply and work. - Work to be done by the utility or customer.	- Software code standards. - Extent of re-used code. - Safety category. - Delivery of bought-out equipment or software. - Loading on supplier's works.	- Finalisation of all VDU designs. - Finalisation of all sensor, actuator characteristics. - Finalisation of system software configuration. - Finalisation of application software.	**- Production of equipment and of software.** **- Supplier's assembly of subsystems.** **- System integration.**

Note: In many contract arrangements, the supplier may have authority to develop the detailed design and proceed to manufacture and software implementation, without formal agreement by the utility or purchaser. The supplier will then normally review and agree the designs and plans internally.

TABLE VI. LIFE-CYCLE PHASE: FACTORY ACCEPTANCE TESTS (SECTIONS 3.2.4, 6.6)

Initial activities: Detailed qualification tests **Main activities: Testing to detailed test plans; FAT**				
Objectives of the phase activities	**Inputs & constraints**	**Main influence factors**	**Requirements, outputs & constraints**	**Deliverables**
- Factory testing to show the requirements are met. - Qualification of hardware. - Qualification of system software. - Qualification of application software.	- Agreed qualification plans. - Extent of any independent V&V. - Compliance to codes and standards. - Established QA and records system. - Software document status. - Previous qualification reports.	- Supplier's practice for manufacture and type testing of modules. - Safety category. - Regulatory requirements. - Generic or plant-specific qualification. - Use of operating experience in qualification. - Relationship to FAT, SAT.	- Functionality. - Performance. - Operability. - Environments. - Criteria for software defects. - Reports of equipment behaviour. - Detailed analysis of software code, where necessary. - Detailed software findings on defects.	**- Final specification of FAT.** **- Qualification reports:** **- Hardware** **- Software** *Note - Normally required for the system safety case*
- Plant specific software tests for the system. - Validation of the integrated system. - Full functionality must be known and tested.	- Integration of the equipment subsystems and system. - Agreed validation plan (from phase IV). - Test platform availability. - Testing phased in time. - Manufacture testing of modules and components completed.	- Utility attitude and involvement in tests. - Extent of independent V&V. - Deferred FAT work may be done on site. - Development of test documents independent from designers is desirable. - Tests for category A systems should be traced to the requirements.	- Utility test requirements. - Detailed design. - Functional and performance requirements. - Compliance to codes and standards. - HMI aspects must be defined carefully for testing. - Detailed records of all tests done.	**- FAT report** *Note: Normally required as references of the safety case*

TABLE VII. LIFE-CYCLE PHASE: INSTALLATION & SETTING TO WORK OF THE INDIVIDUAL SYSTEM (SECTION 3.2.5, 6.7)

Initial activities: Development of installation plan and installation tests; **Main activities: Installation; Installation testing.**				
Objectives of the phase activities	**Inputs & constraints**	**Main influence factors**	**Requirements, outputs & constraints**	**Deliverables**
- Definition of site activities. - Generate plans for installation. - Avoidance of site problems. - Clarification of interfaces and interface activities.	- Defined design and scope. - Defined interfaces.	- Utility involvement. - Extent of interfaces with existing plant and I&C. - Effect on plant operation.	- Interfaces to other plant. - Functionality. - Performance. - Dependability. - Operability.	- **Detailed installation procedures.** - **Installation test listings and specifications.**
- Installation and integration with plant. - Satisfactory initial operation.	- Installation & commissioning plans, (from phase IV). - Development of site test documents with independence from designers is desirable. - Completion of manufacture and relevant FAT activities.	- Integration of the system with the plant; - Testing phased in time; - Utility attitude, approach and possible involvement in tests.	- Performance of digital communications should be carefully tested. - Operation on site power supplies should be tested.	- **Installed and operating equipment.** - **Installation tests.**

Note: Installation tests are not always a formal part of the contract, but a supplier will normally test to give himself confidence to start SAT and commissioning

TABLE VIII. LIFE-CYCLE PHASE: TRAINING AND CONTRACT DOCUMENTATION (SECTIONS 3.2.6, 6.8)

Initial activities: Training proposals and agreement of a training programme. **Main activities: Supplier's training courses;** **Provision of all contract drawings, and documents;** **Provision of all application software and documents;** **Production of all system manuals and handbooks.**				
Objectives of the phase activities	**Inputs & constraints**	**Main influence factors**	**Requirements, outputs & constraints**	**Deliverables**
- Production of a training specification and agreement of a training programme.	- Utility requirements; - Utility familiarity with digital or other technology used. - Plant documentation;	- Staffing policy. - Numbers of staff. - Staff qualification level. - Specialist courses may be needed for software maintenance.	- Operability. - Testing. - Storage and installation. - Maintenance.	**- Training programme.**
- Implementation of a training programme. - Production or availability of handbooks and manuals. - Provision of all information needed for O&M. - Provision of all information needed for licensing.	- Agreed training programme. - Existing documentation of the system. - Plant documentation.	- Staffing policy. - Numbers of staff. - Staff qualification level. - O&M policy.	- Functionality. - Performance. - Operability. - Testing.	**- Handbooks, manuals and O&M documentation.** **- Trained staff.** **- Contract drawings and documents.**

TABLE IX. LIFE-CYCLE PHASE: SITE ACCEPTANCE TEST & COMMISSIONING WITH PLANT (SECTIONS 3.3.1, 6.9)

Initial activities: Production of test plans and commissioning documents **Main activities: Site Acceptance Tests; Commissioning of systems with plant.**				
Objectives of the phase activities	**Inputs & Constraints**	**Main Influence factors**	**Requirements, Outputs & Constraints**	**Deliverables**
- Generate plans for SAT & commissioning. - Validate periodic test procedures.	- Integration plan. - Final validation plan. - Qualification plans. - Tests for category A systems should be traced to the requirements.	- Utility requirements. - Utility involvement in testing and commissioning. - Documentation of existing plant. - Endurance tests may be needed to demonstrate dependability.	- Functionality. - Performance. - Dependability. - Operability. - HMI. - Criteria for software defects. - Detailed plan and lists of tests for the SAT. - Detailed plan and lists of commissioning tests.	- **SAT plan.** - **Commissioning plans and procedures.** - Validated periodic test procedures.
- Completion of satisfactory tests. - Acceptance of the system for contract completion and operation. - Commissioning tests of the interconnected system in the plant itself.	- Agreed SAT plan and detailed tests. - Agreed commissioning plan and tests. - Completion of installation.	- Special operations in parallel with the old systems may be required.	- HMI aspects must be defined carefully for site testing. - Endurance tests may be done to demonstrate dependability. - Detailed records of tests and results. - Documents for the safety case.	- **Site Acceptance Test Report.** - **Commissioning test records.** *Normally a reference of the safety case.*

TABLE X. LIFE-CYCLE PHASE: SYSTEM OPERATION & MAINTENANCE (SECTIONS 3.3.2, 6.10)

Initial activities: Development of Operation and Maintenance procedures. **Main activities: Operation and maintenance of the operational systems**				
Objectives of the phase activities	**Inputs & constraints**	**Main influence factors**	**Requirements, outputs & constraints**	**Deliverables**
- Generate plans and procedures for operation & maintenance. - Develop disciplines for modifications.	- Handbooks. - Detailed designs. - System interfaces. - On-site QA procedures.	- Staffing policy. - Numbers of staff. - Staff qualification level. - O&M policy.	- Modification procedures: - hardware - software	**- Operation and maintenance procedures.**
- Operate and maintain the interconnected system so that the safety and operational goals are not violated. - Implementation of suitable on-site QA processes. - Ensure reporting of system experience.	- Agreed operation & maintenance plans. - Completion of SAT and commissioning tests. - Regulatory acceptance. - Trained staff.	- Staffing policy. - Numbers of staff. - Staff qualification level. - Use of supplier's staff in O&M.	- Operability. - Testing. - Details of defective modules - hardware - software.	**- Maintenance reports.** **- Software incident reports.**

6. APPLICATION OF METHODOLOGY

The requirements specifications must be seen in relation to the life cycle phases of I&C systems presented in Section 3. Table XI below clarifies their sequence in time.

6.1. PROJECT PREPARATION AND FEASIBILITY STUDY

If a utility wants to renew, refit or upgrade part or all of the existing I&C systems, they should first initiate a feasibility study. The refit or upgrade may be envisaged to cover replacement of a single simple system, or may be a comprehensive renewal of several systems with added functionality. Extensive safety improvements may be envisaged, with replacement of protection equipment. For the simplest type of renewal, a feasibility study may be done against a simple request, but for more extensive work, a specification of the nature and scope of the study is recommended. The project preparation or the feasibility study itself should include the following actions:

- determination of modernisation goals,
- determination of scope of refit or upgrade,
- clarification of constraints,
- recommendations on the feasibility of the project.

TABLE XI. REQUIREMENTS SPECIFICATIONS SEQUENCE IN TIME

LIFE CYCLE PHASES	RESULTS, PLANS	SAFETY CASE
Overall project phase 1. Project preparation and feasibility study.	Feasibility study • Technical feasibility. • Budget estimates.	**Preliminary safety case** • Basic requirements specification. • QA-programme. • List of documents. • Technical standard.
2. I&C architecture and basic requirements specification.	Basic requirements specification • Overall I&C architecture. • Categorisation of functions.	
Individual system phase 3. Tender specification and. Purchasing of the individual systems.	Suppliers' tenders. Order to the supplier.	
4. Specification of individual I&C systems.	Validated specification and plans on: • System validation (FAT&SAT). • System operation and maintenance. • Staff training.	**Safety case** Safety justification. Requirements specifications. Verification and validation plans.
5. System realisation. Detail design of individual I&C systems. Manufacturing and system integration.	Detailed manufacturing and installation documentation and operating and maintenance manuals. System ready for tests.	
6. Factory acceptance test (FAT).	System is ready for shipment to site • FAT test report.	
Plant related phases 7. Installation and setting to work of the individual systems.	Start of system failure reporting. System installed, operating.	
8. Training and contract documents.	All contract documents provided.	
9. Site acceptance test and commissioning with plant.	System ready for operation • SAT test report.	
10. System operation and maintenance.	Continued system failure reporting. Reporting of the result of routine tests.	**Final safety case** System description. V&V test results.

6.1.1. Determination of goals

The main objective of this activity is to identify the overall goals for the renewal or upgrade of the I&C system. Normally, the utility is in the best position to identify these. They may be:

- to maintain or increase safety,
- to maintain or increase plant operability and availability,
- to simplify plant maintenance,
- to simplify and optimise the I&C maintenance and maintainability,
- to ensure the continued availability of spares and spares support,
- to reduce the cost of the maintenance of the I&C system.

6.1.2. Determination of scope of refit or upgrade

Based on the goals of 6.1.1., the scope of the I&C systems to be renewed must be estimated. This depends on the logistics of the implementation and the time allowed for the necessary installation and commissioning work. This estimate must take into account which parts of the I&C renewal can be performed during operation and which parts have to be performed during shut down conditions. These estimates form a preliminary time schedule and establish conditions for expected planned refuelling outages, including links to the plant budget planning.

The determination of the renewal scope should address:

- identification of the I&C systems concerned,
- identification of the constraints,
- the target time-scale for achieving the project goals,
- the extent of the renewal or upgrade.

The utility is generally best placed to identify this information. The utility may have a preferred technology or computerisation approach, and this should be identified. The scope and goals identified should be defined as a specification of the scope for the feasibility study required.

6.1.3. Feasibility of the project

The full feasibility of the modernisation project should be investigated. The utility itself may wish to do this work, but often a consultancy or major supplier of nuclear services will be in a better position to undertake this work. A sponsor for the work may be involved, who may wish to agree to the extent and nature of the study.

Based on the documentation of the existing I&C systems to be replaced or upgraded, as a first step, the existing functions must be identified and categorised according to safety. This work should also identify the required performance, dependability, HMI and operability characteristics required.

Difficulties arise, if no design documentation is available or if the existing documentation is incomplete. Suggestions related to the specific documentation needed for the existing design are given in Section 4.3 of [2]. In such a case the only possibility is to generate as-built documentation by means of plant inspections and discussions with the plant personnel. It is important to identify documents and make sure that all involved persons in the project understand the existing documentation of the I&C systems. Guidance on this is given in Appendix II.

For the analysis of the technical feasibility of the intended upgrade, the influence factors (Section 4) and the key requirements (Section 5), must be taken into account.

With the focus on the part of the I&C system to be renewed first, the technical feasibility of the intended upgrades with respect to the following should be analysed:

- key properties and physical size available and needed for possible products,
- the capacity needed from electrical supply systems and other services,
- the availability of adequate measurements and actuators in the case of intended functional upgrades.

The analysis should identify:

- conceptual design alternatives,
- probable risks and costs,
- the scope of hardware and engineering, to a level of detail sufficient to be used later for development of a full specification for the work.

Based on the feasibility study, a full report of the work with recommendations should be made. This will be required by the utility and any sponsor, and possibly by the safety authority. A management decision must be taken whether to proceed with the project or not.

If the decision is to continue the project, the next step will be to produce a basic requirements specification. This specification should include all necessary information needed for the quotation and purchasing phase. The basic requirements specification also forms part of the documentation needed for concept licensing.

6.2. I&C ARCHITECTURE AND BASIC REQUIREMENT SPECIFICATION

6.2.1. Production of the BRS

When the feasibility study has been discussed, agreed and accepted, the overall categorisation and architecture for all I&C systems should be developed. The utility has the primary responsibility for this work at this stage. The utility or sponsor will normally require an experienced supplier of nuclear services to undertake this work, although the utility itself may be in the best position to specify the details for some types of upgrade. The BRS (see Section 4.1.) is the deliverable document which provides the general basis for the renewal project. It should give an overview of all potential systems for refit or upgrade, whether the refit of a specific system is urgent or not. The output from this phase is generic and should be applicable independent of any future supplier or detailed technical solution.

The preliminary work needed to generate this specification includes:

- product reviews, to identify suitable specific products and suppliers,
- detailed review of the existing I&C installation, its problems, strengths and weaknesses,
- potentially, a human factors review, to identify improvements in control room design, specifically where extensive VDU information may be being added to the design,
- a detailed safety review, if the work is intended to improve safety following recommendations such as those provided by IAEA reviews,
- identification of the preferred architecture, based on the feasibility study recommendations.

The main steps in writing the BRS are:

- full identification of the functions, to be renewed or upgraded, and their allocation to the safety or other goals identified in the feasibility study,
- formal safety categorisation of the intended functions (see Section 2.1.) and the identification of their relation to the safety or other objectives, the single failure criterion, the use of defence in depth and functional diversity,
- identification of deterministic features for fault tolerance and changeover, and for design values of probability of failure and spurious trips or actuations,
- identification of functional assignments between the operators and the I&C system (IEC 964 and see Appendix II).

During the functional allocation the link between the identified functions and the equipment intended to implement them is evaluated with respect to the requirements of categorisation. The mapping of functional category onto the I&C equipment and systems should be determined. The QA level needed and qualification requirements depend on this.

Figure 3 below gives an overview on the data flow between the design steps needed to develop the basic requirements of the I&C system specification (forward flow). Potential feedback influences from later design steps are marked with dotted lines. The information flow from the influences and constraints (Section 4) and from the requirement elements (Section 5) are shown in summary form. The potential for validation of the functional requirements, using a validated plant model, is also shown.

The BRS generally should not depend on a specific I&C product range or system. The BRS defines the overall architecture and the essential features required for the I&C systems, and their co-ordinated functions. It also forms the basis for any future upgrades. The BRS is central to the work of the project, and should be formally provided to the utility and sponsor organizations as a major deliverable.

6.2.2. Basic functional requirements

A re-engineering of the existing functional requirements may be necessary. Experience is that for I&C systems which have been in operation for several years the documentation shows how the I&C systems are built, but the documentation does not provide basic functional requirements nor the system properties. The safety importance may not be shown or known, except for the safety system itself. Appendix II gives guidance on the analysis needed to identify or confirm the requirements.

Continued further use of existing sensors and transducers or the installation of new measuring equipment should be analysed. The functional requirements developed for the identified I&C functions should contain:

- the identification of the use of existing measurements,
- the identification of the need of the installation of new sensors,
- the need for on-line validation of the input signals,
- the extent of functional processing of the signals,
- the identification of command signals to trigger the actuators,
- the identification of operator interaction with the system,
- the processing to initiate alarms,
- the identification of deterministic requirements on failure tolerance and CCF management and the probabilistic target values for availability and reliability design.

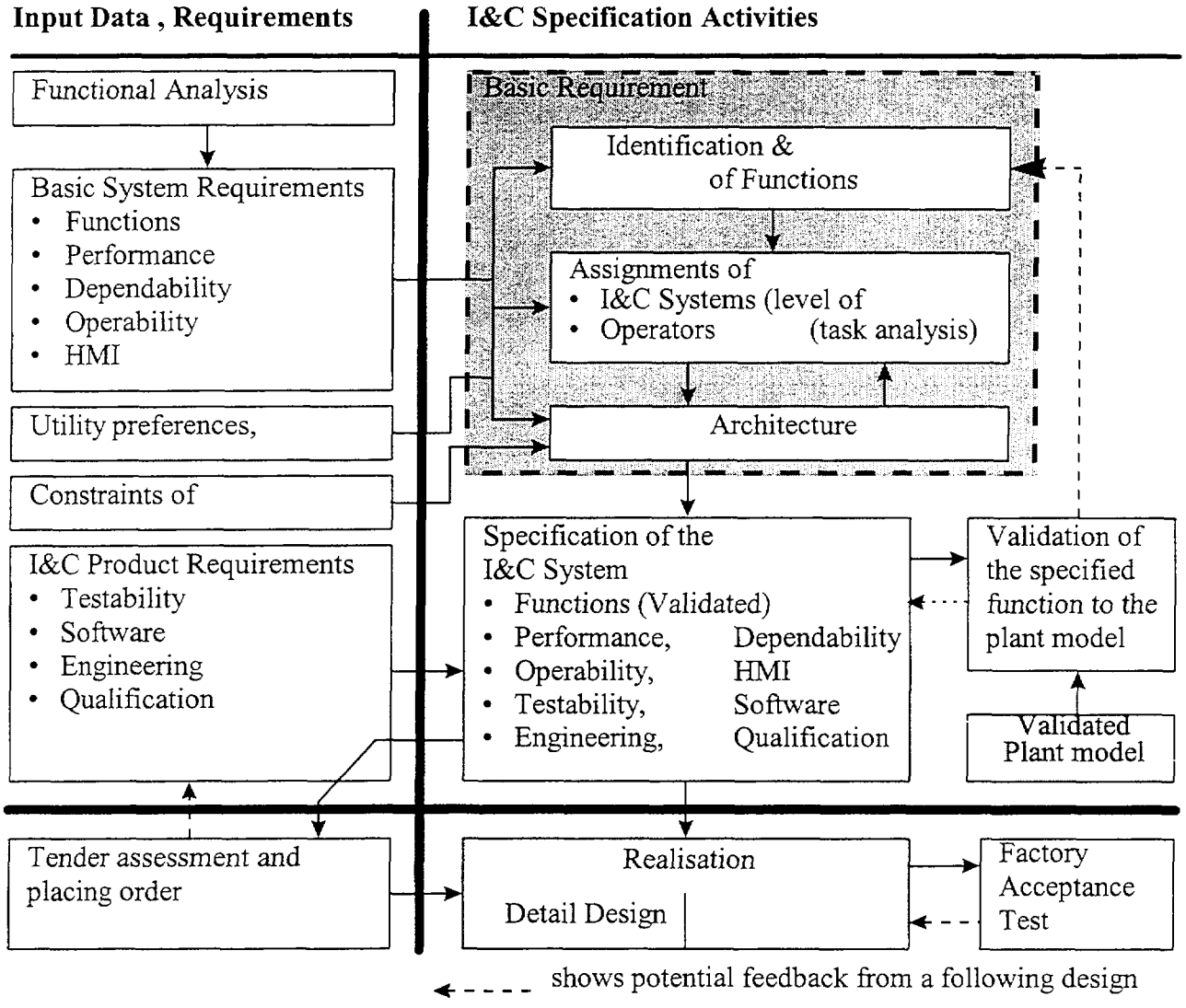


FIG. 3. Validation of the basic requirements specification.

6.2.3. Review of possible products

At the time of generation of the BRS, the utility or his agent should review products believed to be able to implement the systems concerned. This will involve discussions and visits to the various vendors, and consideration of the hardware, software and design tools which the vendor may be able to offer. The records of the vendors in implementing similar project will be of concern. Any regulatory acceptance of the product in the country of origin will be of importance in justification of safety. The review should be recorded by suitable internal reports, able to be provided to the regulator if necessary as justification of the product and vendor chosen.

6.2.4. Analysis and categorisation of the I&C functions

The I&C functions which are to be renewed or upgraded should be identified and their relation to the global safety objectives should be analysed. The method of categorisation of functions, including the consequential main requirements, is described in Section 2.1. When there are other I&C functions which are outside the renewal scope but are also important to safety, these functions have to be taken in account.

The availability of an existing safety analysis or of one performed specifically for the work forms the basis for the categorisation of the I&C functions. Key criteria are the consequences of an assumed failure of a function on demand. The existence of independent functions, either within or outside the system to be renewed or upgraded, can reduce the qualification requirements if they ensure the same safety objective.

The result of these analyses is the relative importance of the functions to be renewed, and their importance in ensuring that the plant safety objectives are met. This gives the basis for the potential application of functional diversity and defence in depth. The analyses also provide the basis for the safety categorisation.

6.2.5. Architecture of I&C systems

An important system requirement is that the I&C system architecture should fulfil requirements on fault tolerance. To meet the single failure criterion, redundancy is required. To withstand possible common cause failure of an individual I&C system, independent subsystems and diverse functions may be needed. In addition, the design of the I&C system redundancy in combination with the intended voting method used in the protection system must reflect the required target values for availability and reliability. To a great extent, the requirements on failure tolerance depend on the safety categorisation for the functions to be realised.

The required I&C system architecture forms the basis for additional consideration of constraints from the existing plant design, such as the availability of separate rooms for cabinet installation and the air conditioning and power supply situation.

If parts of the HMI or even the complete control room are in the scope to be renewed, then in addition to the functional architecture, the spatial arrangement of displays for information and actuation, and the arrangement of conventional controls and indications, as well as all other ergonomic aspects of the project must be analysed and specified.

The architecture specification should produce:

- the hardware architecture specification,
- the software architecture specification,
- the integration specification.

As necessary inputs, the following information should be available, as shown on Fig. 3:

- influences and constraints from the utility,
- influences and constraints from the plant,
- functional and performance requirements,
- implementation requirements.

6.2.6. Functional allocation

Based on the results of the previous design steps the identified functions are allocated to I&C systems and their subfunctions are allocated to subsystems within the total I&C architecture. The main activities of this design step are:

- to ensure the functional scope of each subsystem is met by an adequate equipment performance;
- to ensure the assignment of functions to independent I&C systems is sufficient to meet the requirements of "defence in depth" or are graded as diverse functions with respect to a common plant safety objective;
- the assignments of operators tasks.

6.2.7. Function and task analysis and HMI

When functions have been assigned either to the operators or to the I&C system, task analyses should be performed for functions or tasks which are to be performed by the operator and functions which support the operator. The result of the task analyses is an important input for the design of the HMI and other related parts of the I&C system, e.g. the alarm function. Task analysis may be done in parallel with the development of the BRS. The task analysis should result in the specification of:

- operator information requirements,
- human action requirements,
- general ergonomic requirements.

In cases when the control room or parts of the human machine interface are in the scope to be renewed, task analysis is also used in order to specify or confirm the following:

- the arrangement of displays in the control room both for the final design and for intermediate steps,
- the adequate adaptation of operating procedures for the operators tasks and the function of the I&C system,
- the design of the arrangement of visualisation objects in the displays and the processing of the conditions to provide the status of plant systems and actuators,
- that the burden on the operators during important procedures is not excessive, due to possible media interchanges.

This functional specification should be reviewed by safety and process engineers, and verified, to avoid costly reworking.

For the above HMI topics, reference to IEC964 [18] and IEC1771 [26] is recommended. This is expanded on in Appendix II.

6.2.8. Data collection and design tools

To ensure consistency and availability of all design data for the complete life cycle of an I&C system it is essential, soon after the start of the project, to prepare for the introduction and installation of a powerful data base system, to hold all project information on sensors, actuators and other devices, equipment cubicles etc. As far as possible, facilities for later automated links to the design tools should be provided. Provisions should be made to ensure the consistency of common data of different I&C systems. Therefore the application of a commercial standard database management system is recommended.

The database system should have facilities for automatic checks of information format as it is entered. It should be noted that for a complete installation of information displays and controls in a control room, several million items of data must be identified accurately, entered into the database and verified. It is often found that the design documentation available as drawings and instrument lists is out of date or otherwise unsatisfactory. On-site validation of this data will require a flexible yet secure method of correction of errors found in the data, by comparison with the plant, and with suitable supporting QA.

If a set of VDU displays is being designed for the HMI, it should be noted that typical plants may need several hundred or more different displays. Each will require careful and exact layout, using a set of reference project standards on character sizes, colour, names of plant items, types of measurements and symbols for plant devices such as pumps and valves. Care should be taken to

include only such a number of measurements on any typical display as can be rapidly understood and is clear to the operators. Presentations should include the state of the plant at the current time, and also the ability to show historical traces. The design of these displays will also require good tools, preferably with CAD facilities and if possible automatic links to the database management system for signal characteristics. A human factors review of all display layouts should be undertaken. Some guidance on display design is given by IEC1772 [25]. Therefore the methodology for producing the design documentation for the intended I&C-system refit or upgrade should meet the following requirements:

- the specification should be understandable by I&C engineers, safety engineers and evaluators as well as by process engineers;
- the formats of the specification should be standardised;
- the design data should be kept in a data management system which contains each data item only once and supports all phases of the I&C life-cycle.

6.3. TENDER SPECIFICATION AND PURCHASING OF THE INDIVIDUAL SYSTEMS

In the project basic requirements specification phase the relevant requirements for an intended I&C system realisation are documented. These requirements then need to be broken down to the requirements for each individual system of the total refit and upgrade project. These are described here as the specifications of the I&C systems, and will normally be generated by a project co-ordination group from the basic requirements specification. These specifications form the input reference for quotations by suppliers and the subsequent contact placement, detail design, manufacture, software production and installation work.

6.3.1. Specification of I&C system properties for candidate products

This section describes the basic requirements which are necessary for the successful production of the I&C system specification. The properties listed are recommended with the aim of easing the licensing procedure for the realisation of category A functions (IEC1226). For the realisation of lower category functions, category A requirements may be omitted or reduced consistent with the safety or operational importance. The following points should be covered in the requirements:

- the hardware of the I&C system should be qualified or qualifyable to assure sufficient environmental robustness (IEC987, IEC1000, IEC801, IEEE 323, IEEE 344),
- the software should have a clear modular structure with a co-ordinated development according to IEC880 and its supplement, or other relevant software requirements,
- the I&C system should have sufficient flexibility and performance capability to ensure the required functionality, with a satisfactory response time,
- the required I&C system behaviour should be specified and reflect the functional categorisation.

For reasons of effort in design and software maintenance during the total life cycle, the state of the art is to have engineering tools with the capability of automatic code generation. The licensing of I&C systems may be eased by the use of:

- a proven procedure for code generation based on proven software modules,
- a graphic representation of the application functions for ease of understanding,
- integration of formal checks to ease the verification of design results,
- a standard language code for functional validation, used to enable the direct use of the generated code in the target system,

- validation of the tool, documented and accessible,
- configuration management support.

6.3.2. Specification of requirements for quotations

The documentation of the detailed requirements for each system should take the form of a specification for the equipment, software and services required. Where several systems are involved, possibly originating from different suppliers, it is recommended that common specifications are produced for such aspects as environmental qualification testing, equipment construction standards, software general requirements and standards, and to define the site services and interfaces.

An important precondition for issue of the specifications and invitations to bid is that the project co-ordination group and the utility or sponsor agree a short list of suitable suppliers. They should be experienced in the class of equipment required, in the class of refit or upgrade work involved and the work involved on site, which may be in a difficult location.

The method of assessment and criteria for acceptance of quotations should be agreed before issue of the specification to potential suppliers. It is important that the suppliers are aware that the assessment will be full and fair, and that they will be informed about the evaluation of their bid in the assessment, since considerable work is involved in the production of quotations for nuclear plants.

6.3.3. Suppliers' tenders for each system

The potential suppliers will need to undertake preliminary design, based on the tender specifications issued to them, sufficient to provide suitable quotations and technical tenders for the systems concerned. An important part of refit and upgrade work may be the use of existing software, previously supplied for similar uses. It is important that the operational experience and details of such software is well described by the supplier, and that he is prepared to make available full details, with suitable agreements on confidentiality, to allow assessment for re-use in the application.

6.3.4. Order placement

When tenders have been submitted and assessed, and the utility and any sponsoring organization have agreed on the choice, a formal order will be placed on the supplier. Part of this work should be the detailed negotiation of options and any additional aspects, the agreement on non-compliant aspects of the offer, and full clarification of any work areas (such as cable design, task analysis or VDU display design) which the utility itself may wish to undertake.

It is good practice to provide a new document issue, revised in detail to reflect the agreements made during the contact negotiations, for subsequent contract use. This document may be based on the tender specification or tender document. The agreed document will then serve as a reference for proceeding with detail design, implementation and installation of the system.

6.4. SPECIFICATION OF THE INDIVIDUAL I&C SYSTEMS

After order placement with the selected supplier, the required behaviour of each of the individual I&C systems, based on the results of all the previous steps, should be documented by its supplier in detail. Some joint working with the utility or architect engineer will be needed to finalise the behaviour needed, and to identify other necessary characteristics of the system. Site surveys by the supplier of the old equipment and the investigation of site conditions will generally be needed, to identify in detail the actual constraints, and to establish relations with the site staff.

6.4.1. Specification of the I&C systems functions

The main input for the full specification or confirmation of the I&C systems functions are the basic functional requirements including:

- definition of the safety parameters,
- definition of processing logic,
- required response time values,
- actuators of the plant safety systems,
- requirements on reliability and failure tolerance,
- HMI requirements.

These should be identified from the results of plant analysis (Appendix II) and the basic requirement specification (Figure 3).

This should include definition, typically by means of functional diagrams, of the following:

- the allocation of input signals to functions and the specific processor units,
- the design of the principle for online validation during plant operation of redundant input signals,
- the functional processing of the validated input signals (algorithms, setpoints, logic gating, etc.),
- the time response,
- the design of process information necessary for the human machine interface and process alarms to alert the operators in the control rooms,
- the design of alarms on disturbances and failures in the I&C system to alert the maintenance personnel,
- the design of the voting process, to achieve as far as possible that commands to the actuators are not adversely affected by single failures within the I&C system,
- the design of the priority of commands of the safety system when the safety and operational I&C systems use the same actuators,
- the design to link the actuator commands to the switch gear with provisions for periodic testing.

6.4.2. Specification of software requirements

The software functionality should be specified in a software requirements specification. This may use functional diagrams and should identify the assignment of functions to individual processors. Some methods of implementation will require the development of detailed software designs for each function, and the code and test activities to implement those software designs, as described in IEC880. Some methods of implementation may be able to use off-the-shelf software, for example for VDU display.

Each stage of development of the software requirements specification should include appropriate verification to ensure the initial requirements are represented in the final product. Ideally each requirement should be traced through to the final code and the defined validation tests, when safety is involved.

After completion of the software requirements specification and the assignment of the individual functions to processors or processing clusters, the design of the application via an automated code generation process or by other means can be started. Recent developments allow code generators to operate from a graphical representation of the functional requirements. Some engineering tools offer a library with standard function modules able to provide the basic elements of the software requirements specification. Engineering tools for automatic code generation should have integrated formal checks to ensure that only correct data inputs are used and that the logic is complete and consistent. The generated code should be in a suitable standard language to permit its direct application to functional validation.

The system will normally depend on system software (software to organise the operation of the processors and their intercommunications) and application software (the project-specific software for the application). The system software may be a proprietary system or the supplier's own system for organising and operating tasks. The place of system software may be taken by specific general purpose software modules written by the supplier to the high standards needed for category A. These modules may be configured by a suitable software tool, or be manually configured with tool assistance, or be configured by special code, code in a configuration language, or tables of data items specifying the links and interfaces. Configuration information will be needed to arrange for the operation of the system software in the specific architecture of the project, and also for the definition of the characteristics of all signals and actuators and all VDU displays. The extent and scope of this software should be identified.

6.4.3. Functional validation

It is preferable to include functional validation within the specification or system design stage. Functional validation then terminates the basic requirements specification for the I&C system to be renewed or upgraded. Functional validation should give assurance that all of the basic requirements have been addressed. Functional validation at this time assures requirements are correct, complete and consistent, assures quality in the project and prevents possible costly rework later during the detailed design.

The functional validation of the application software should include checks to give assurance for the following:

- there are no possible uncertainties from the re-engineering of the functional requirements to the detailed design,
- for any intended functional upgrades, the basic safety objectives are achieved adequately,
- the correct dynamic behaviour of the designed functions is achieved.

The objective should be that the validation of the complete I&C system within the factory acceptance test (FAT) can be reduced to demonstration via stimulated input signals to show that the correct output signals are initiated as response to predefined input data trajectories.

The process of validation is shown in Figure 4.

The activities of the above diagram should be suitably interpreted and adapted to the specific situation of the upgrade project to cover:

- off-the-shelf tools used by the utility or architect engineer,
- supplier's tools used by the utility of architect engineer,
- supplier's tools used by the supplier himself.

An adequate procedure for performing functional validation depends to a great extent on the complexity of the functions to be renewed:

- For a reactor trip function, where the reactor trip is initiated during a transient when a given setpoint is exceeded by a safety parameter without further required interaction from the I&C function, a review by a person responsible for the safety analysis may be sufficient.
- For complex functions e.g. to open and to close valves depending on different safety parameters and logic depending on the plant condition, a validation of the specified functions by means of a simulator is recommended.
- The application of disturbance analysis simulator code linked to the application software code allows functional validation in away which permits the relation between plant process time and simulator processing time to be flexible.
- If a training simulator is available, there are additional advantages, especially if parts of the human machine interface are in the scope to be renewed, by an early involvement of shift personnel in the validation process.

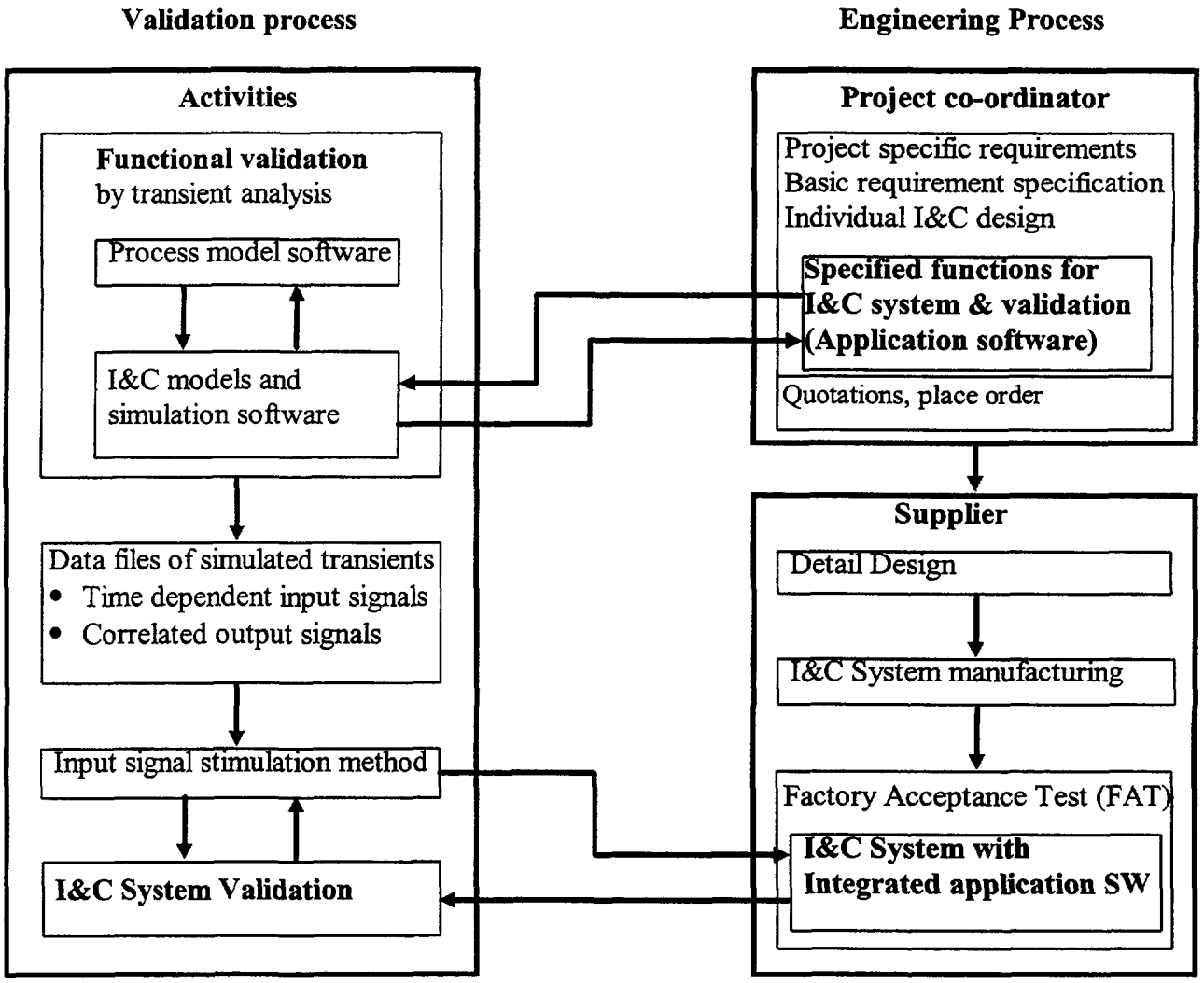


FIG. 4. Validation of I&C functions and systems.

The architecture specification expands the functional allocation process at the level of the individual processing units and other components on the basis of the selected product system. The main purpose of this step is:

- to verify that the anticipated performance of the individual functions after segmentation and allocation to the individual processing units is consistent with the specifications,
- to ensure the allocation of functions to different redundant subsystems and equipment according to the requirements for response time and reliability is suitable.

In particular the step should ensure that the I&C hardware configuration for each function, correlated to the redundancy of plant equipment and the distribution and separation of the I&C equipment, will meet:

- the single failure criteria when this is applicable,
- the specified reliability requirements,
- the required isolation between functions of different categories.

If the control room or parts of the HMI are to be upgraded, a specific V&V process should be followed. IEC964 and IEC1771 give guidance in this area. If a VDU based plant process operation has to be introduced, the operability of essential procedures should be validated by means of a real-time simulator. (see Section 6.7 on training)

The functional validation terminates the specification process for an individual I&C system. It gives assurance that during the following phases of detailed design, software implementation, system manufacturing, system integration and FAT reworking can be avoided.

6.4.4. Planning for future life-cycle phases

To ensure that the requirements from future phases of the system life-cycle are met, plans for the activities and undertaking of those phases should be specified. The plans needed include:

- the system integration plan, for integration of hardware and system software,
- integration planning for integration of system and application software,
- the strategy and detailed plans for environmental testing of equipment and for hardware qualification (see Section 5.4.2),
- the strategy and detailed plans for software qualification (see Section 5.4.2),
- the detailed plans for validation of the system in the factory tests and site tests (see Sections 5.4.1., 6.6.2, 6.9).

Other detailed planning should be initiated at this phase, as described in sections referenced, for site installation, site testing, commissioning (6.9), operations and maintenance (6.10), and possibly for training (6.7).

The detailed activities of the phase define the plans for system installation, testing and qualification. The integration plans may need agreement with the utility, or may only require agreement with the internal testing organization of the supplier. The planning of the site installation will need to be agreed with the utility site organization. The plans for qualification of hardware and of software will generally need to be agreed as suitable, and may need agreement with the safety authority.

6.5. SYSTEM REALISATION

6.5.1. Detail design of individual I&C systems

During detail design, all necessary documents for software implementation, hardware manufacturing, erection and installation of the upgraded system in the existing plant are developed. The development of hardware and software for specific functions which do not affect the overall I&C system functions are elaborated, such as details of testing facilities. Any special design unique to the project is undertaken. This work is based on the I&C system specification (Section 6.4).

This design work defines the organization in cabinets and modules, the layout, the methods of separation and isolation between sub-systems components and signals, the interconnections with the power sources and the detailed ergonomics of the HMI.

A main section of design work covers the specification of full details of the manufacture, erection and installation as well as procurement and follow up of the components, modules and equipment of the system. This will include:

- details of all special to project modules and cards to be developed and made,
- assignments of each card to each cabinet and cabinet position,
- earthing and power supply distribution within cabinets.

The specifications include hardware descriptions and manufacturing information, database listings, manufacturing drawings and equipment layouts. The functionality and other software requirements must be defined, together with the software design.

Documents are needed for the installation in the plant defining:

- cable routes to all other systems,
- interconnecting cables and cables to other systems,
- connections to MCR, switchgear, sensors and transducers,
- power supply distribution.

The erection and installation procedure in the plant requires detailed procedures to be developed in close correlation with the scheduled outage (see Section 6.8).

6.5.2. Development of interfaces to other systems

The new system will normally interface to both new and existing systems and equipment (see Ref. [2]). Required input information includes:

- I&C systems architecture requirements specification,
- the properties of the other interfacing systems,
- the interface requirements of voltage, current, datalink protocol etc.

The detail design should specify:

- the adaptations and development necessary to interface with the systems & equipment of the I&C architecture,
- the procedures or tools for the validation of data exchanged between the I&C systems.

This phase as a whole should include development of specifications, drawings, build lists, database schedules and descriptions. Design requirements should cover main interfaces and utility requirements of detailed practice such as:

- the equipment physical layout, dimensions and services needed,
- cable entry, termination and support details, earthing methods,
- earthing arrangements to avoid earth loops for instruments etc.,
- seismic equipment hold-down methods requirements.

6.5.3. Agreement on detailed design

The detailed design specifications developed as described above define the architecture of the individual I&C systems and sub-systems and components, define the equipment to be manufactured or ordered from suppliers and provide the inputs requirements for the following phases of the life-cycle of the system (installation, factory acceptance tests, site acceptance tests, etc.).

In many contract arrangements, the supplier has authority to proceed directly to manufacture and software implementation after the detailed design process. In his own interests, the supplier will normally review his specifications and plans, and revise them suitably for any comments within his organization. In some cases, the utility or sponsor may require the project to be held before the major cost of manufacture is involved, until funds are released. This will allow review of the design documents and approval of the interfaces, the design and the plans for the site and other work. When the reviews have been completed, manufacture and software implementation can begin with minimum risk of error.

Where a major refit of the control room is involved, it is advisable to obtain full agreement on the control room design between the utility and supplier. Where joint work is involved, for example for the design of new VDU displays by the utility and their implementation in the supplier's organization, a process of agreement on the constraints is often needed. For VDU design, agreement on layout and content constraints, and agreement that the designs can be implemented in detail with resolution of all queries (such as the exact identities of each signal shown) will be needed.

The integration plans may need agreement with the utility, or may only require agreement with the internal testing organization of the supplier. The planning of the site installation will need to be agreed with the utility site organization. The plans for qualification of hardware and of software will generally need to be agreed as suitable, and may need agreement with the safety authority.

6.5.4. Hardware manufacture

Following detailed agreement of the designs, the system specifications will be passed to the manufacturing part of the supplier's organization, and internal authorisation for manufacture will normally be needed. Items to be bought from external suppliers will be ordered, unless advance ordering of key components has been authorised beforehand.

Special design and development may be needed for some equipment. Examples could be interfaces to existing plant items, power actuator drives and communication channels to other supplier's equipment. These items will normally require prototype testing and may require qualification tests.

6.5.5. System software configuration

The system software modules must be arranged to operate the actual equipment of the application, and in the manner required. This will require them to be configured by suitable information. The software may be configured by a suitable software tool, or be manually configured with tool assistance, or be configured by special code, code in a configuration language, or by tables of data items specifying the links and interfaces. An important task is therefore to define carefully this

configuration information, load it to the relevant system software and confirm its validity. The validation of this configuration forms an important part of system integration.

6.5.6. Application software implementation and configuration data

Detailed work to write or automatically produce the application software can begin. Detailed work to compile information on sensor characteristics, ranges, alarm levels, calibration etc., is needed, with the production of databases. Detailed VDU designs can be produced. Test information will be needed for use during system software configuration and application software development. This gives confidence that the system software and application software will process information correctly when the detailed information on sensor characteristics or VDU designs is included in the system.

6.5.7. System integration

Integration starts as the equipment arrives in the supplier's test areas for assembly of the test arrangements of equipment. Depending on the nature of the system, this may be as a completed system, or as a test platform in which major modules can be exercised appropriately and representative equipment configurations can be assembled and tested. The system equipment will now normally be integrated with the system software and then the application software, often with sample data rather than the full system configuration data.

The integration work should be carefully planned within the supplier's own organization. It is often undertaken by specialist staff who then take the system forward for the factory tests. At the time of integration, the supplier normally will test to give himself confidence in the integrated operation and the correct integration of any new module types or specially developed units. The phase will reach completion when this work is complete, and factory acceptance tests can begin.

6.6. FACTORY ACCEPTANCE TEST

6.6.1. Requirements for FAT

The detail design process must develop the requirements for the FAT as part of the validation plan (see Section 6.4.4). The plan specifies the activities to be performed during the factory acceptance tests to assure that the integrated I&C system correctly implements the I&C specification. For this part of the validation see Section 4.1.7. of [10].

This phase includes the manufacturing and workshop tests of the hardware modules and of the wiring and interconnection. It is good practice to produce a document which gives the principles of the FAT, before the detailed test listings and detailed test procedures are produced. This document of principle should be reviewed by the utility site staff, to ensure that their requirements are included in the detailed test listings. These principles will also provide support to the licensing process and should form part of the system safety case. The validation of the application software to ensure that the original basic functional requirements are met by the I&C system specification can be performed according to the procedure described in Section 6.4.3. For this part of the validation see also 1.4.1. of [10].

Specific interfaces may require new hardware and software development (according to 3.1 of [10]), with or without integration of existing software (according to 3.2 and 3.3 of [10]). These specific interfaces sometimes cannot be tested during FAT and therefore additional effort is needed during SAT.

Inputs from the previous phase include:

- the hardware and software architectures,
- specifications of system software configuration,
- the specifications of the individual hardware and software modules.

6.6.2. Conduct and reporting of FAT

The FAT itself is normally conducted by specialist staff on the factory test platform area, after completion of integration of the equipment as it comes from the factory. Special test wiring may be needed, and normal test areas have special equipment set up for injection of test voltages, power sources, facilities for testing subsets of the equipment at raised temperature and temporary mountings for VDUs, printers etc. It is normal practice for the supplier to give advance notice to the utility that testing is planned to start. This will allow participation or test witnessing by the utility. It is good practice for the supplier to appoint a test supervisor and the utility to appoint a test witness to agree each day which tests are to be done, and with authority to accept the day's log of test work done. They should have authority to retest if needed, to restart testing after a test interruption if problems are found, and to sign test certificates for satisfactory completion of testing.

The FAT should be logged carefully, with signing of each group of tests done on the list of test. Any accepted defects or deferred tests should be recorded. A suitable report should be written as a record, in a form able to be sent to the safety authority and for reference during the SAT.

6.7. INSTALLATION AND SETTING TO WORK OF THE INDIVIDUAL SYSTEMS

6.7.1. Documents for site installations

Based on the design of detailed I&C system architecture, the documentation for the installation will be developed. This documentation is described in Section 5.1.5.

6.7.2. Delivery and installation

Following the FAT, the equipment is delivered to site. In some cases, phased delivery is needed, with equipment groups (such as the redundant sections of a safety system) being tested in the factory one after another and then installed in sequence. Installation will require care in room preparation, use of cranes, access to lifts, corridors and stairways, moving into position, fixing, connection of power and temporary protection. Generally formal authority covering personnel safety considerations will be needed before high voltage power is allowed to be connected. Site installation will normally be with simulated input signals and dummy output loads until completion of the initial parts of the SAT.

It is good practice for the supplier to complete his installation with his own tests to give confidence in the acceptability of the equipment and the success of the following SAT and commissioning phases.

6.8. TRAINING AND CONTRACTUAL DOCUMENTS

6.8.1. Requirements and training courses

The requirements for training staff must be defined by the utility in conjunction with the supplier of the equipment and where relevant, the software supplier. The management of a digital system requires software skills on site, and this must be planned for by the plant management.

The specification for training of utility personnel should include requirements for instruction concerning each individual I&C system. Training should include:

- storage and installation of equipment,
- operation,
- calibration, set-up, maintenance of components and modules,
- periodic tests and tests needed after repair and maintenance,
- operation of procedures for modification of software and hardware,
- methods of changing existing and inclusion of new displays and logs,
- defect and other reporting procedures,
- site quality assurance and record keeping.

The number and object of the training sessions should be defined, taking into account the number of trainees, their technical knowledge and general technical culture, the language to be used and the availability of special training tools (special computer programs, simulators, etc.).

The training, including the on-the-job training of plant personnel, should be performed early, if possible involving trainees during system integration and FAT. The training programme should be completed before the installation and commissioning on site of the system, in such a way that plant personnel are available for these activities, under suitable supervision, when required.

In cases when the control room or parts of the HMI are renewed, specific training should be provided for control room operators, when necessary with the use of a real-time simulator. This training should show that the operators are ready to act safely and efficiently in the new control room layout and, possibly, with modified procedures. Special tests should be defined, according to the level of the upgrading performed.

6.8.2. Documents and handbooks

Suitable handbooks, manuals, operation and maintenance procedures, as-built drawings and documents should be provided in the normal course of a well-managed project. It has been found by experience that these may not be able to be fully specified in the initial requirements of the contract. The planning for the training phase of the project may be a suitable time for the exact definition of these requirements, if they have not been defined earlier.

Wherever possible, the supplier should have standard documents for the products concerned, but the application will have specific documents, as-built drawings, installation wiring diagrams, its own specific layout and arrangement of cabinets and cards, and its own specific cable lists, VDU layouts, drawings and database information. These should be provided to the utility and the site staff.

The utility may require specific instructions written in the form of the normal plant operating instructions, and forming part of the plant index of operating instructions. These may need development with reference to plant simulators.

6.9. SITE ACCEPTANCE TEST AND COMMISSIONING WITH PLANT

The objectives of the SAT and of system commissioning with plant include:

- verification of the state of the system,
- checking that the system state is comparable with the state at the end of the FAT,
- validation of any aspects of functionality which were not possible in the FAT and
- undertaking tests to show full compatibility with the plant.

To achieve these objectives, the commissioning of the on-site installed system should be performed in two phases:

- tests of the I&C system with deactivated links to the actuators but with the input signals active as far as possible,
- commissioning and tests of the new system with the plant itself, integrating system tests with the tests using the plant and its interfaces, to overlap the testing of the system alone.

Special conditions may be applicable if the new system is to be operated in parallel with the existing system until it is accepted by the plant and the safety authority.

6.9.1. SAT planning and testing

The SAT must be planned carefully, and operation of the tests should follow the detailed requirements of the SAT plan. The SAT is normally based on the FAT, but with modifications to allow for site conditions. A test on site supplies is needed. Any excessive rate of module failure should be a reservation on the success of the test. It is good practice for large systems to have an endurance trial for a period of weeks, with the system operating in different modes from stimulated or real plant inputs, but with plant actuators not connected. The trial should include a complete test of each individual function of safety systems, which may not be possible in the shorter time of a FAT. The normal routine cycle of calibration, maintenance and self-testing can be started at this time. The supplier may undertake all the SAT process or be assisted by the utility staff under the supplier's supervision.

The SAT should be conducted under the supervision of a test controller appointed by the supplier and a test supervisor appointed by the utility, who jointly control all activity. The supplier and the utility representatives should agree the day-to-day testing to be done, and agree the log of each days work. They should have authority to order suspension of the test, retesting and system acceptance. The SAT may be completed with minor reservations, provided a clear plan and time-scale to resolve them is agreed.

The SAT normally forms the completion point of the utility contract with the supplier, and the start of a warranty period.

6.9.2. Commissioning planning and testing

After the SAT, commissioning tests show that the system fulfils the requirements for operation with the plant and for interfaces with other operating systems. The specification for the complete commissioning of the new system or the upgraded system should include a step by step and progressive activation of the links to other systems, to the inputs and to the switchgear. The complete process should be controlled by a formal, written document with a list of detailed tests. This commissioning plan should be developed by the utility with input from the supplier, or by the supplier with the co-operation of the utility staff.

Commissioning of the system with live plant can only follow careful preparation, and must be done in a way which gives full confidence of the system operation and its interfaces to the plant. An example is the connection of the plant signals into a normal display and logging computer system, where a procedure might include:

- simulated input injection at system input terminals of the selected input,
- check of correct VDU display and associated alarm title,
- with the sensor disconnected locally, checks of cable continuity to the sensor,

- check of zero and full scale from each sensor location by signal injection,
- confirmation of alarm settings and alarm titles of alarms generated by each sensor,
- check of sensor signal polarity and safety to prevent sensor damage,
- confirmation of correct VDU display of the sensor measurement,
- connection of the sensor.

The successfully connected sensor will then be marked onto a master listing of sensors, and a signature recorded of its correct connection. A corresponding careful process should be followed for connection of plant actuators and switchgear for control by the new system, with allowance for the importance of personnel and plant safety.

A similar process to that described for sensors is clearly of special importance for safety system signals and actuators.

The objectives of periodic tests should be stated and the procedures for performing these tests must be written. In this context it is important to take into account the self-tests and other tests that the system performs automatically. Commissioning tests should also include validation of periodic testing procedures.

In some systems, the computer system will provide closed loop control. Nuclear plant design should involve suitable simulation modelling of the plant to show stability and suitable interaction with other controls. Well developed procedures exist for such commissioning, which should only be done after transfer and check of the values of the appropriate proportional, integral, derivative, hysteresis and other settings to the controller.

The commissioning tests with plant require a formal, signed record to be made, to be held with the station records. A commissioning report may be needed, recording the significant features of the tests done, for the safety case.

6.10. OPERATION AND MAINTENANCE

The detailed design must develop a specification of the routine actions needed to maintain the system, the constraints on maintenance during operation, the records which need to be maintained and the operation and maintenance procedures for hardware and software. The recommended spares to be held on site should be listed, and the utility may need to order these specifically.

The procedures for hardware and software modification should be agreed with the site utility staff. These and their importance are discussed elsewhere.

It is good practice for the operation staff to record suitably all equipment failures and the action taken to repair the system. It is good practice for software anomalies and incidents to be recorded and reported by a formal reporting system, preferably forming a database of events. This is essential for a safety system.

7. KEY RECOMMENDATIONS

This report provides guidance on a methodical approach to preparing and establishing the requirements and plans for the different phases of the life-cycle, for digital I&C systems hardware and software refits and upgrades in nuclear power plants.

A basic recommendation is that a reference life-cycle should be established for the refit or upgrade project. It is very important that projects define from the beginning which documents and what work is expected at different phases, and this can only be done from the base of an agreed life-cycle. The life-cycle should be produced with reference to the information in the draft standards IEC1508 [11] and IEC1513 [12], taking IEC880 [23] into account.

For systems refit or upgrading, the report emphasises the importance of the initial feasibility study, which is essential for a successful project. The following recommendations are made:

- the initial feasibility studies are of great importance in establishing the utility expectations, safety role of the equipment and extent of use of digital systems,
- a clear scope and division of work should be defined,
- the expectations of the utility should be clearly understood and agreed in this stage,
- the safety authority approach to licensing digital systems important to safety should be clearly appreciated and agreed by the project at an early stage in the project.

The requirements documents and plans to be developed at each stage of the project life-cycle should take into account:

- the appropriate document within the life-cycle (discussed in Section 3),
- the consideration of specific influencing factors (discussed in Section 4),
- the appropriate key elements of requirements to be determined (discussed in Section 5).

The methodology recommended is therefore to consider the influences and constraints, and the elements of requirements in a systematic manner, at the time of production of each planned document at each phase of the life-cycle.

This guide recommends that a basic requirements specification should be developed for the total scope of safety important I&C systems in order to avoid, during a stepwise upgrading procedure, a reengineering of earlier upgraded parts. This should not be necessary as a consequence of upgrades that are scheduled in a later stage, if an integrated consideration of the total expected requirements is undertaken.

An important recommendation is that plans for system integration into the plant as well as qualification and testing requirements and requirements for operational and maintenance are emphasised during the specification phase. The methodology emphasises the importance of planning and of revision of the documents produced to reflect agreements and changes made to each system. In comparison to the life-cycle of analog I&C systems, plans are required earlier for digital systems.

Appendix I and Tables I to X, which summarise the information flow and the main topics, provide concise guidance and bring together the descriptions in the text to indicate the different life-cycle phase, the influence and constraint factors, and the requirement elements identified in Section 3, 4 and 5 of the report, to allow for this. The tables and Appendix I show, for each phase of the life-cycle:

- the objective of the phase activities,
- inputs and constraints,
- main influence factors,
- requirements and plans to be specified and defined,
- outputs and constraints,
- typical deliverables.

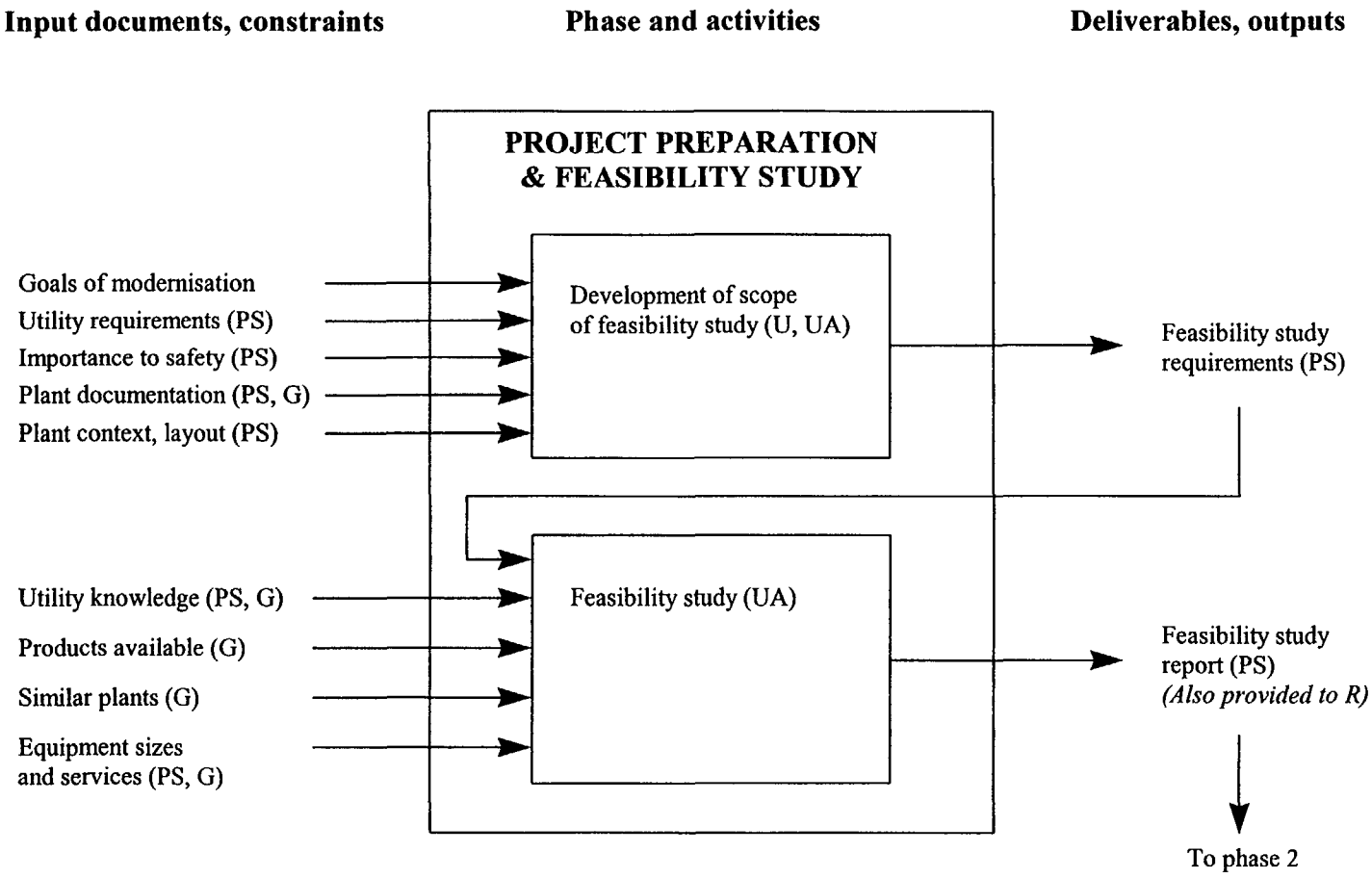
Each table covers one phase of the life-cycle, as comprehensively as necessary for that phase of implementation of the project.

The provision of complete and clear specification documents and plans will encourage good communication and will reduce the chance of misunderstandings between utility, design authority and supplier. It applies to the personnel involved in manufacture, software design and production, and testing and installation processes. It will finally contribute to a successful achievement of the upgrading goal, whether this is relevant to plant safety or operability.

Appendix I

MAIN ACTIVITIES, INPUTS, OUTPUTS AND DOCUMENTS

The following pages give the main activities, inputs, outputs and documents referred to in the main text of the report, and in the tables. The arrows indicate the information flow. The boxes indicate the activities. The expected organizations responsible for the activities are indicated, and explained in the legend.



LEGEND: U = Utility, UA = Utility or Agent, V = Vendor or Supplier, G = Generic, PS = Project
R = Regulator

Fig. 5. Phase 1.

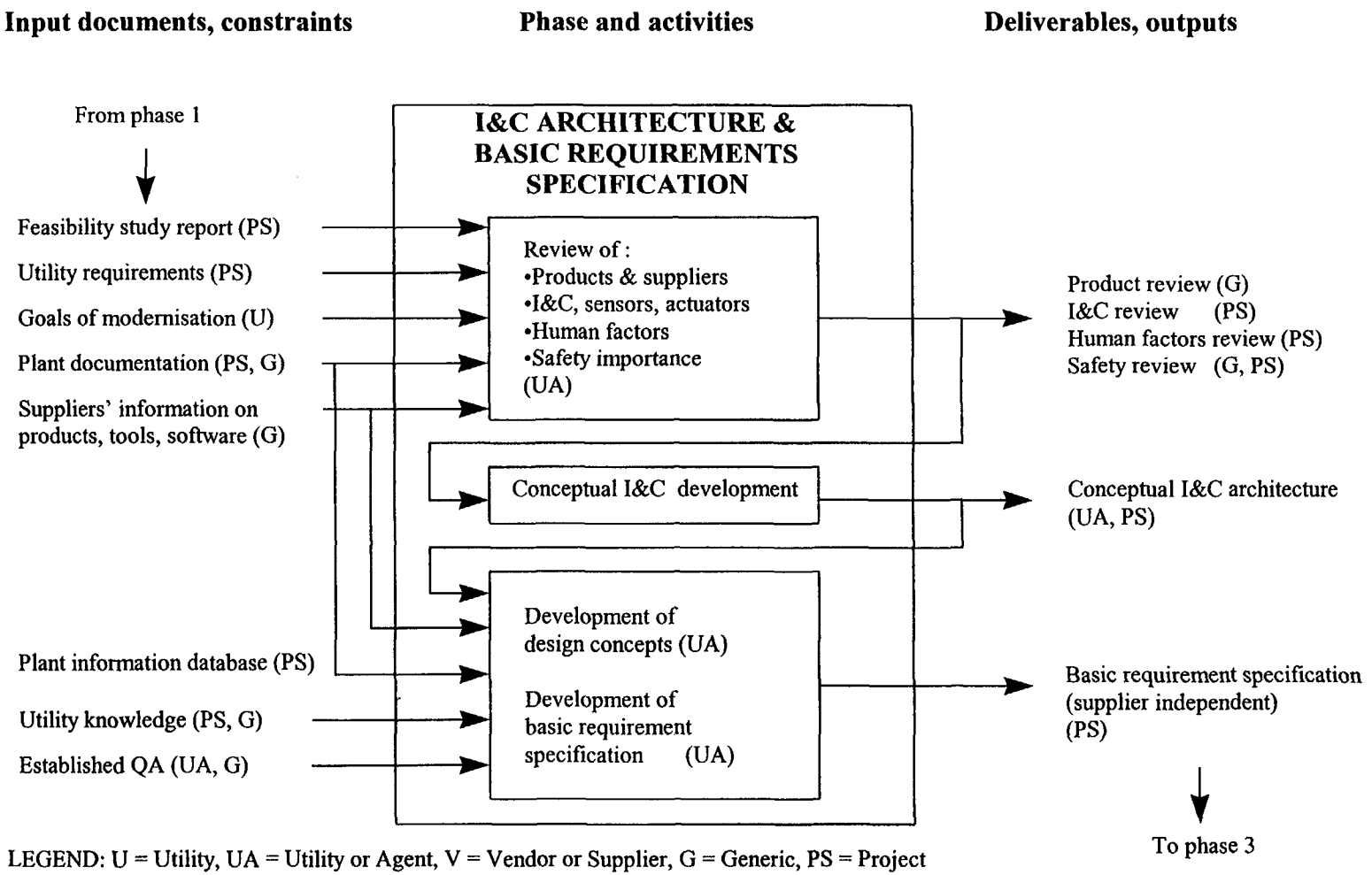
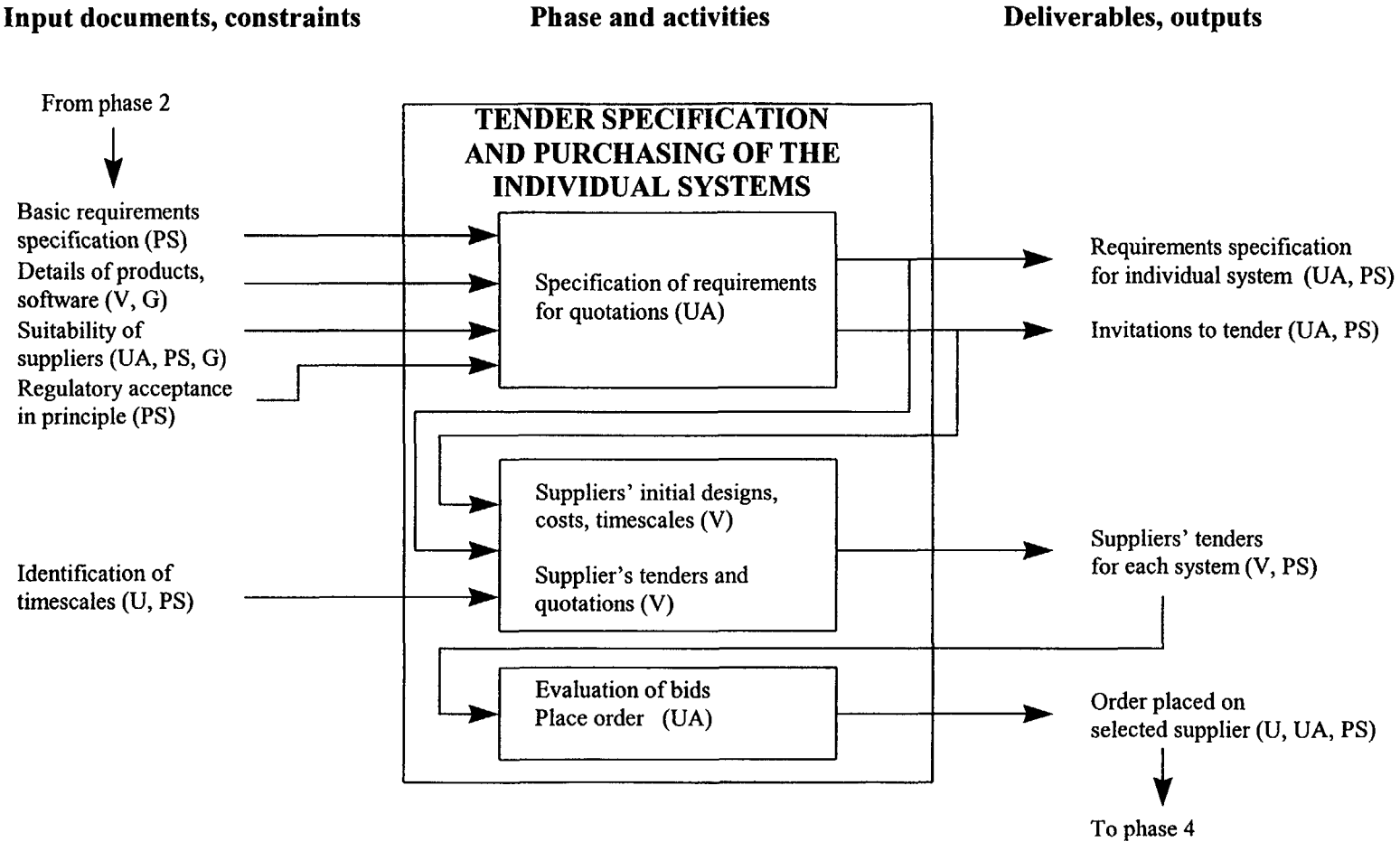
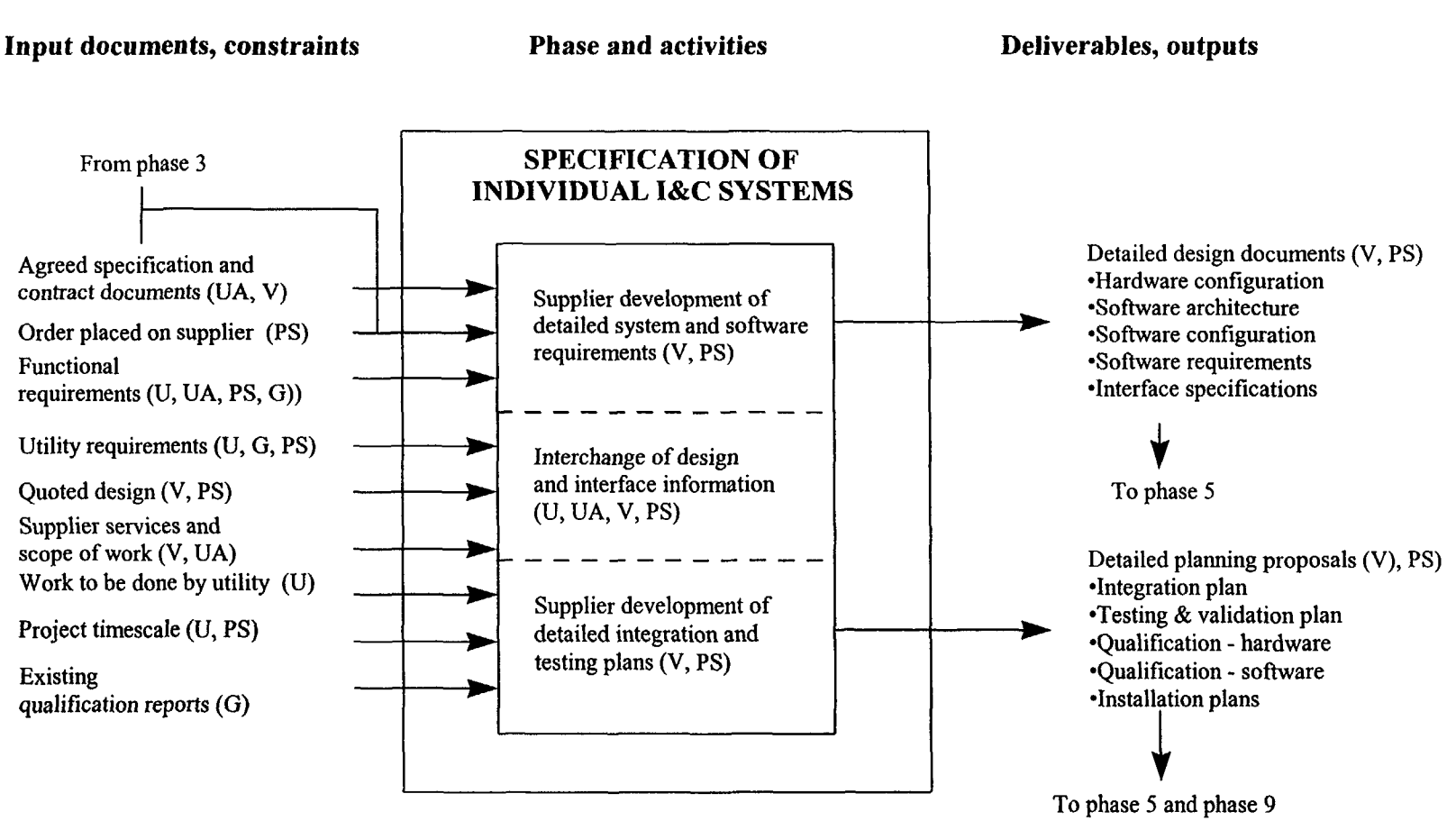

Input documents, constraints
Phase and activities
Deliverables, outputs
From phase 1
I&C ARCHITECTURE & BASIC REQUIREMENTS SPECIFICATION
Feasibility study report (PS)
Utility requirements (PS)
Goals of modernisation (U)
Plant documentation (PS, G)
Suppliers' information on products, tools, software (G)
Review of :
•Products & suppliers
•I&C, sensors, actuators
•Human factors
•Safety importance
(UA)
Product review (G)
I&C review (PS)
Human factors review (PS)
Safety review (G, PS)
Conceptual I&C development
Conceptual I&C architecture (UA, PS)
Plant information database (PS)
Utility knowledge (PS, G)
Established QA (UA, G)
Development of design concepts (UA)
Development of basic requirement specification (UA)
Basic requirement specification (supplier independent) (PS)
To phase 3
LEGEND: U = Utility, UA = Utility or Agent, V = Vendor or Supplier, G = Generic, PS = Project

Fig. 6. Phase 2.



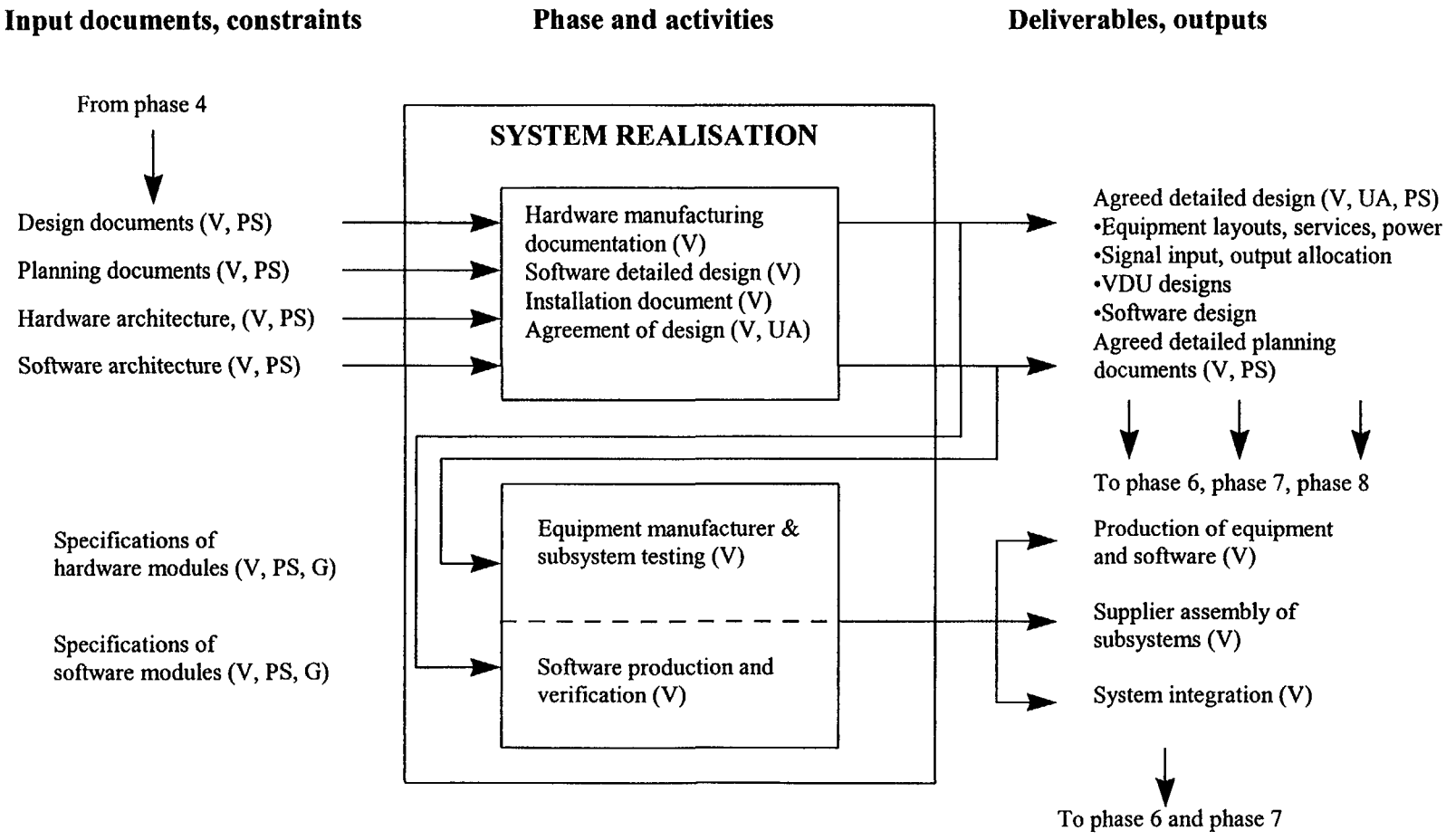
LEGEND: U = Utility, UA = Utility or Agent, V = Vendor or Supplier, G = Generic, PS = Project
R = Regulator

Fig. 7. Phase 3.



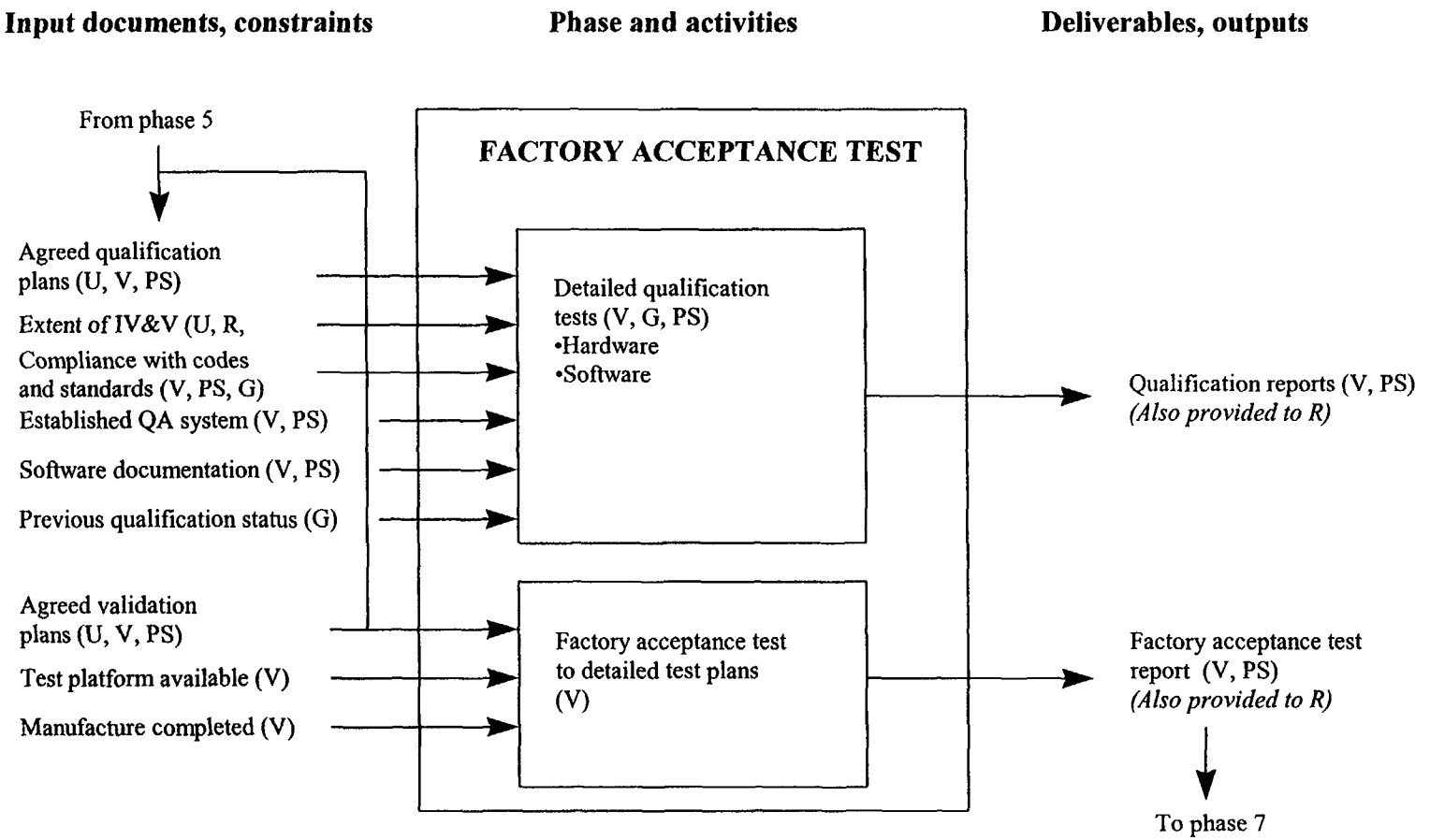
LEGEND: U = Utility, UA = Utility or Agent, V = Vendor or Supplier, G = Generic, PS = Project

Fig. 8. Phase 4.



LEGEND: U = Utility, UA = Utility or Agent, V = Vendor or Supplier, G = Generic, PS = Project

Fig. 9. Phase 5.



LEGEND: U = Utility, UA = Utility or Agent, V = Vendor or Supplier, G = Generic, PS = Project
R = Regulator

Fig. 10. Phase 6.

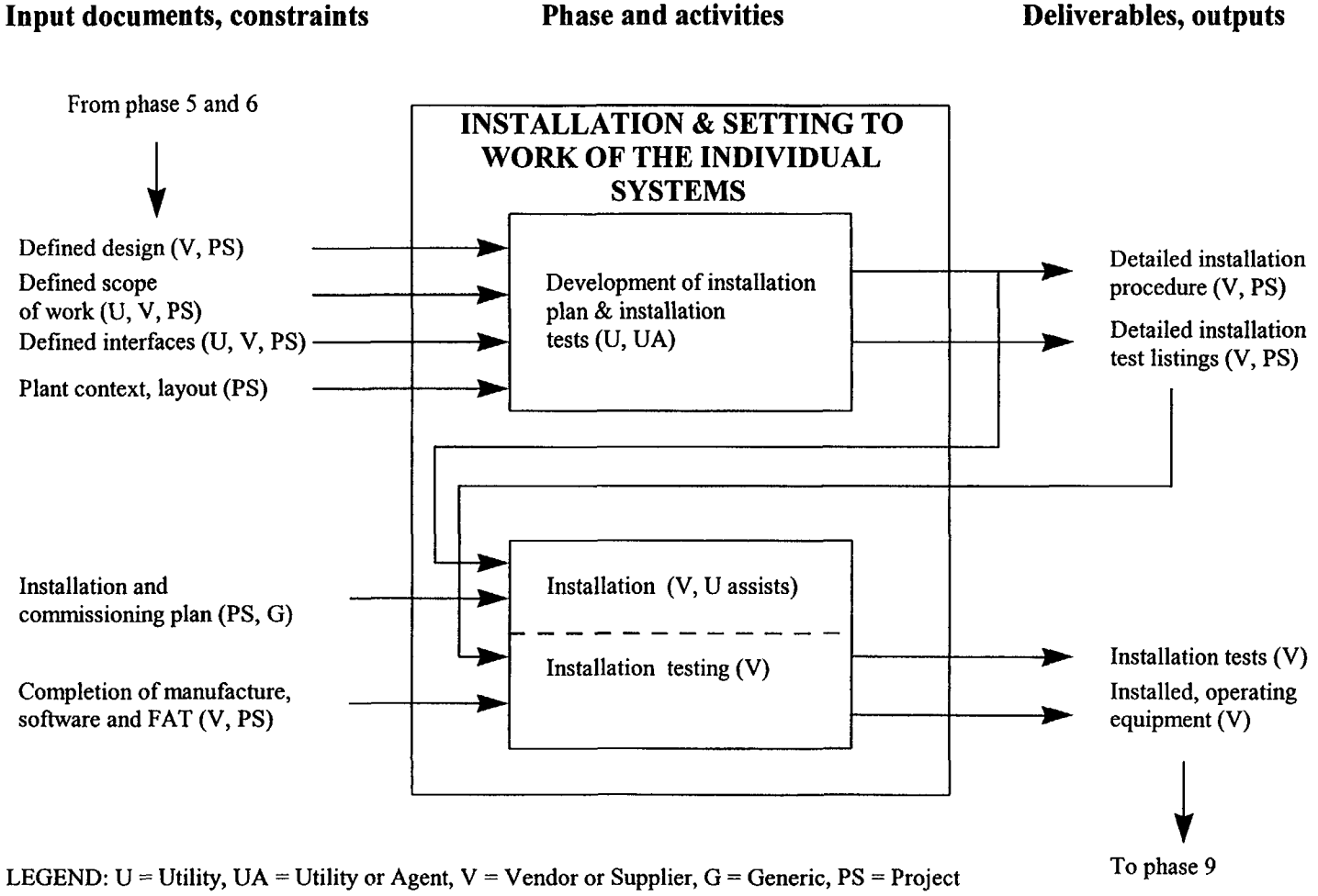
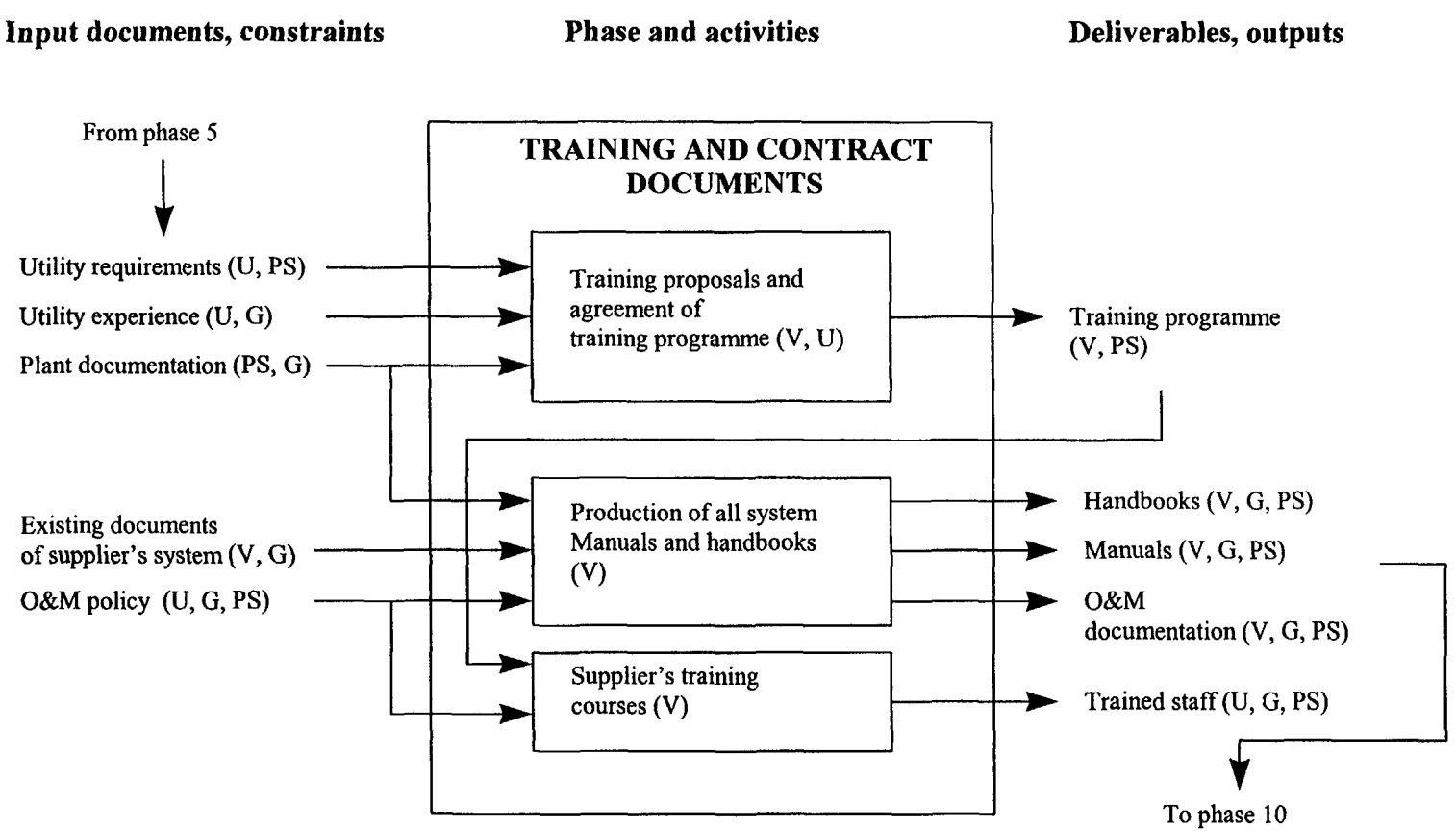
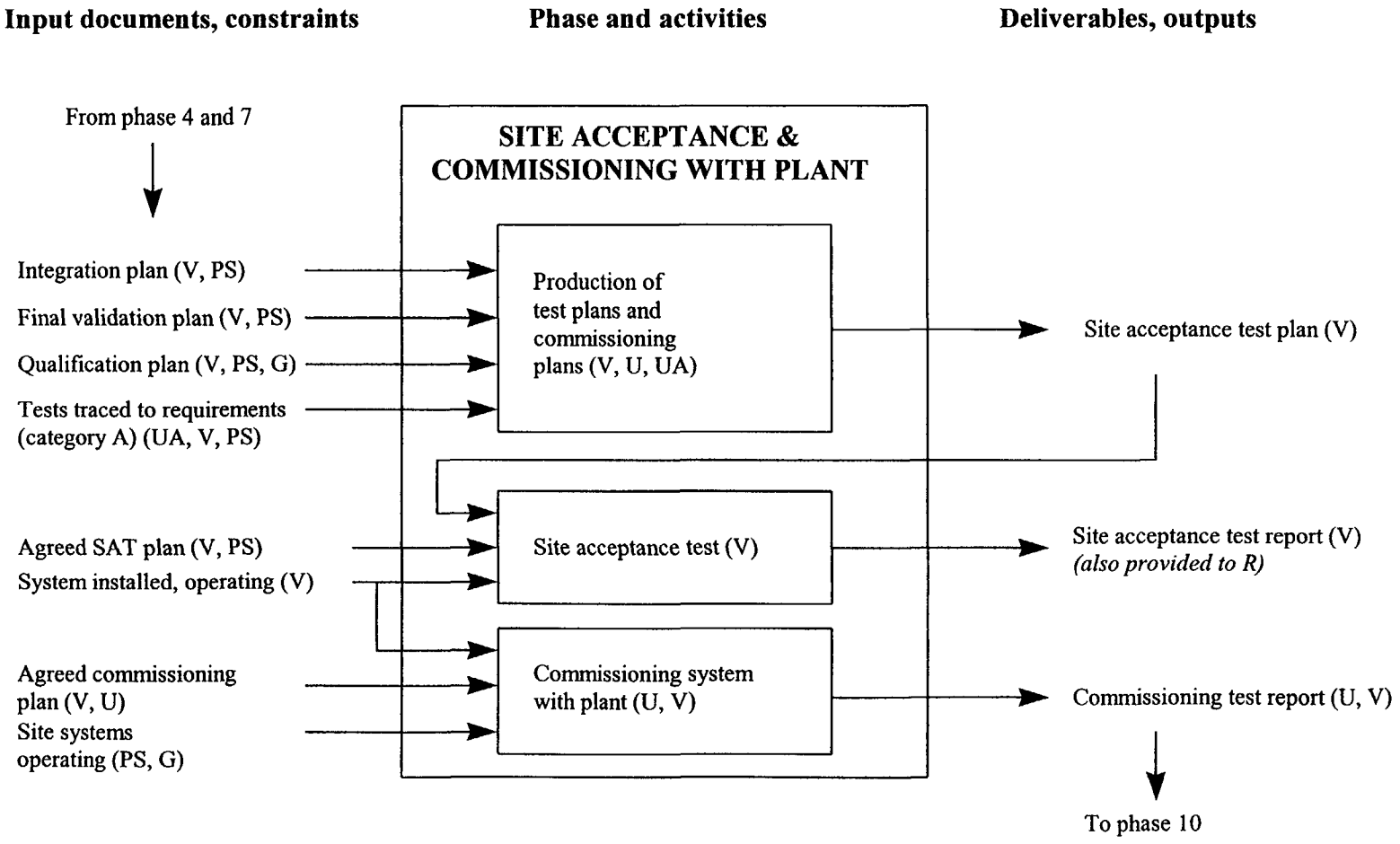


Fig. 11. Phase 7.



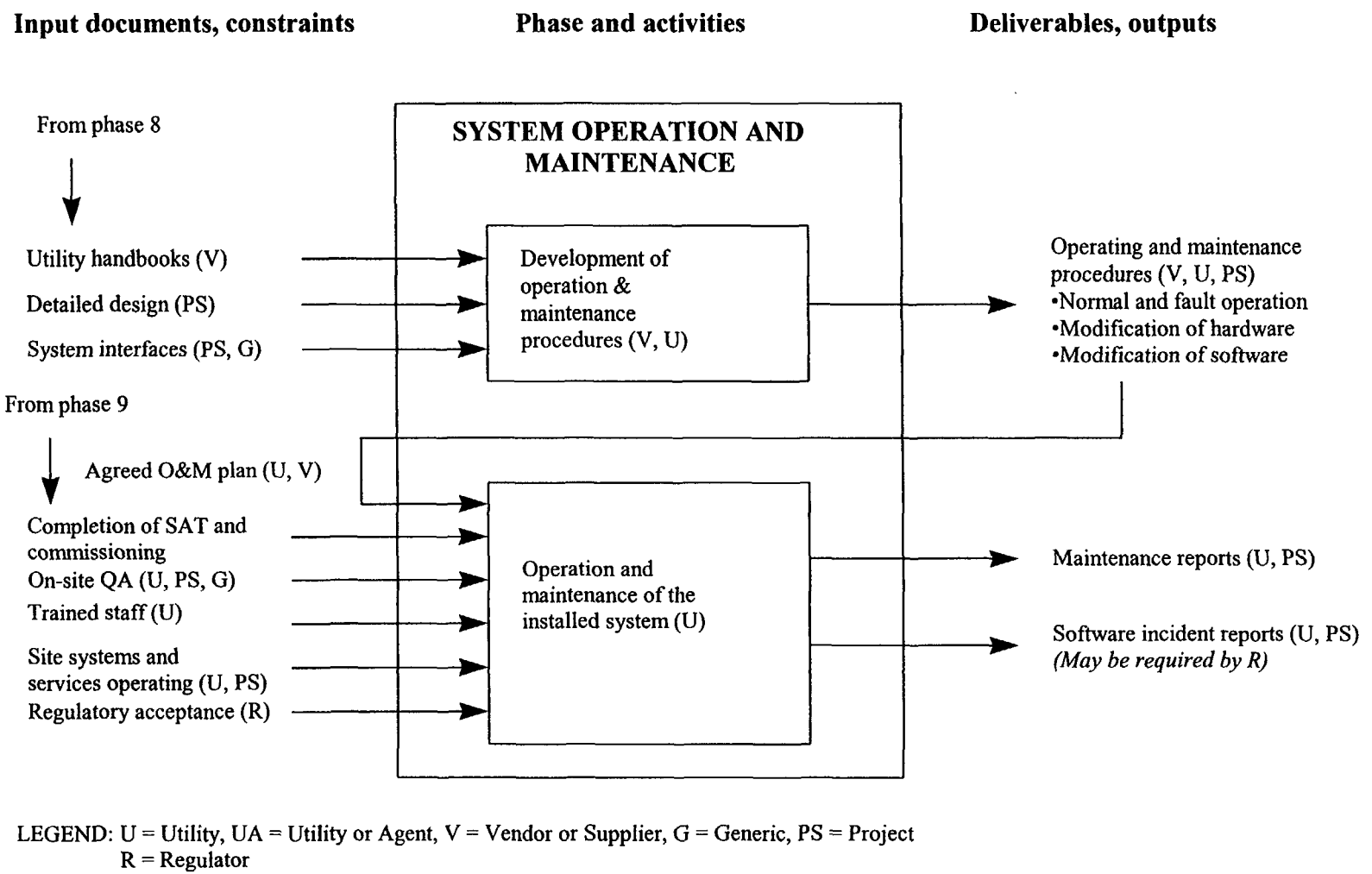
LEGEND: U = Utility, UA = Utility or Agent, V = Vendor or Supplier, G = Generic, PS = Project
R = Regulator, O&M = Operation and

Fig. 12. Phase 8.



LEGEND: U = Utility, UA = Utility or Agent, V = Vendor or Supplier, G = Generic, PS = Project
R = Regulator

Fig. 13. Phase 9.



LEGEND: U = Utility, UA = Utility or Agent, V = Vendor or Supplier, G = Generic, PS = Project
R = Regulator

Fig. 14. Phase 10.

Appendix II

PERFORMANCE OF ANALYSIS IN I&C DESIGN

II.1. INTRODUCTION

Analysis is a necessary part of the process of refit or upgrade. Some of the analysis which needs to be performed are not within the scope of I&C design and implementation, but need to be understood by the I&C engineers. Two main parts of analysis are relevant here - functional analysis of the reactor protection and control functions and theoretical analysis of the reactor performance. Functional analysis is necessary when control rooms are to be upgraded or changed, in particular for the design of alterations and extensions of the human–machine interface. This analysis shall, if applicable, cover all modes of operation including postulated initiating events (PIEs) such as faults and accidents as well as events beyond design basis emergencies (DBEs). Reactor performance analysis is needed for determining the requirements for control systems. Analysis is particularly relevant for the determination of the requirements for protection when these are being increased, or where they are not known fully by the plant. This will apply when the reactor protection system is being upgraded or refitted.

The performance of functional analyses for a nuclear power plant will normally also include or require task analysis processes of the main part of the I&C and the control room. This may involve experts in human factors, as well as I&C engineers. The purpose of the functional analysis is to identify the functional goals for a system with respect to available manpower, technology and other resources and to provide the basis for determining how functions may be assigned and executed. The performance of these types of analyses are equally important in retrofit projects although basic overall plant analyses do normally not have to be redone. The performance of functional and task analysis for I&C and the control room is discussed in IEC 964 "Design for control rooms of nuclear power plants"

Task analysis for the operators is one of the more important types of analysis performed during the design process. Task analysis shall be performed in the earlier phases of the design process in order to address all human factor issues in a cost-effective way.

The functional and performance requirements for the reactor protection and control systems may be not fully available to the utility staff responsible for the refit or upgrade. They must then be determined systematically and confirmed as suitable by analysis using validated reactor models. The analysis work is generally the concern of safety or performance engineers, although I&C engineers will be involved. The utility staff may wish to improve the protection by adding or altering the functions provided, for example by including a computerised calculation function, such as assessment of shut-down margin from the total worth of control rod insertions. Analytical work is then needed to establish the functional algorithms and logic on a sound footing, and to prove it is safe and sufficient.

II.2. CONTROL ROOM ANALYSIS PROCESSES

II.2.1.System based approach to the functional design of control room and I&C

As stated in IEC 964 different types of analysis are used as tools in the design of the I&C and of the control room. Different types of analysis may be used in a top down approach which can be divided in four basic steps, performed in an iterative manner:

(1) Functional analysis of the plant concept and identification of functions where I&C systems and the control room can be involved.

Step one encompass functional analysis of the main objectives of the I&C systems and the main control room, functional design objectives of the I&C systems and the main control room as well as the relationship with other control and management centres.

(2) Analysis to identify the distribution of functional assignments between man (M), technology (T) and the organisation (O). Such assignments are based on regulatory requirements, an operational policy and the concept of the plant design. The organisation should be understood to include e.g. administrative support, procedures etc.

Step two encompass more detailed analysis in order to identify the distribution of functional assignments for the control room staff and the I&C. Task analysis is one of the most important tools during this step. Task analyses are also performed in order to identify the distribution of tasks between the members of the shift crew, centralised versus local manoeuvre etc.

(3) After the two first steps a verification and validation process is carried out to demonstrate that the acceptance criteria are met.

(4) When a more developed plant and control room design is available more detailed analysis are performed which, for example, shall be the basis for development of training of the operating staff and the writing of procedures. The analysis performed during this step are also used to verify the capability of the organisation, technology and operators to perform their assigned tasks.

II.2.2.Input data for the performance of control room analysis

Important inputs during the performance of the functional analysis and task analysis are the safety requirements and the operational principles.

Some examples of operating criteria and principles are:

- the number of personnel in the control room staff,
- the automation level for safety but also for operational reasons,
- the philosophy of the distribution between conventional and computer based displays,
- the philosophy of centralised or local control,
- the split up of responsibility between operation, maintenance and technical support organisations,
- the assignment of functionality between O&M systems for normal plant operation and O&M systems for tasks important to safety,
- the responsibility for security and access control as well as the responsibility for the fire protection of the plant,

An important part of the analysis is to identify the advantages and weak points in the existing control room design.

More general design principles and guidance can be found in IEC 964, chapter 2.

II.2.3.The concept of task analysis

The concept of task analysis covers a wide range of methods used in order to describe and evaluate the interactions between man, technology and organisation.

Task analysis can be defined as a study of what operators are required to do in order to achieve system goals and the associated performance demands put on operators. Task analysis often includes: descriptions of information requirements, evaluations and decisions, task times, human actions, environmental conditions etc.

Task analysis is a methodology which is supported by a number of specific techniques to help the analyst collect information, organise it and then use it to make various judgements or design decisions. The application of task analysis methods will provide the user with a knowledge of human involvement in the system and with detailed information of the system from the human perspective. Such structured information can then be used to ensure that there is compatibility between system goals and human and organisational capabilities, so that the system goals will be reached.

II.2.4.Task analysis in control room system design

In the past, classic ergonomics and human factors have been somewhat preoccupied with details at the expense of the over all system characteristics. Traditional ergonomic design focus on postures, human–machine interfaces, lighting conditions etc. but often fails to consider the system as a whole. This does not in any way imply that traditional ergonomic design should not be performed or considered.

On the contrary, traditional 'micro-ergonomics' must be performed, but a 'macro-ergonomic' thinking must also be implemented in order to ensure that the over all system goals are reached. Task analysis is an important tool in this process.

Task analysis are also needed in order to put focus on the integration of other functions, such as maintenance, management, QA etc. Weak spots may often be found in the interaction of tasks performed by different groups of people.

There exists several formal methods for the performance of task analysis. A good oversight of such methods is given in IEC 964.

Some of the more common used methods are:

- hierarchical task analysis (a description of main tasks and sub-tasks),
- activity sampling and work study,
- task decomposition and decision/action diagram,
- walk-through and talk-through,
- simulations in simulators or in a mock-up.

II.2.5.The process of task analysis

Even if there are many task analysis methods, most of them start with a description of what people actually shall do (in terms of cognitive processes and actions) in the system and how the tasks relates to each other. In short, task analysis shall be used in order to:

- provide a list of all the tasks that shall be performed and by whom,
- assess what support will be needed for the performance of each task,
- determine how this support will be provided by the design.

The information obtained in this process will be the basis for more detailed analysis, for example: job analysis, analysis of procedural need etc.

II.3. REACTOR PROTECTION SYSTEM

II.3.1. Outline methodology

When requirements for functionality and performance of the reactor protection system or power control systems are not fully known, or they may be being extended, the following main steps are necessary:

- Identification and recording of the functions of the installed system.
- Initiation of analysis using suitable theoretical models of the plant.
- Consistency analysis.
- Development of a revised requirements specification.
- Development of safety justification.

The following gives more detail.

II.3.1.1. Identification and Recording of the installed system

The installed system will normally be well understood by the site staff, and by the engineering support organisation of the utility. The manuals, handbooks, drawings and specifications of the installed system will normally be available. However, the documents may not identify the functions and performance of the system with respect to the design basis faults of the plant, and they may not be in a form suitable for a plant safety case. It is in such cases necessary to record the installed system in a form which allows for its functional verification as suitable for the safety of the plant. For this purpose, analysis should be undertaken to identify and record:

- each parameter measured and its sensor characteristics,
- trip settings and accuracy,
- time responses,
- trip and safety feature actuation logic and algorithms,
- so far as possible, the apparent intended fault protected by each function,
- maintenance, test, operability and HMI functions.

This should be recorded in natural language, with lists and tables suitable for understanding during the consistency analysis to follow.

II.3.1.2. Analysis

The first step needed is the identification of a suitable validated reactor and plant model, able to cover the operational range of interest, and including all plant needed for protection and control. It is not suitable to use an operator training simulator for this, due to the simplifications needed to provide a training simulator able to run in real time. If the use of a training simulator is proposed, the validity, range and accuracy of the model should be carefully checked. Normally, a model specifically developed for safety and performance analysis of the reactor concerned is necessary. The second step needed is the identification of the PIEs of concern. These may be, for example,

- reactor trip,
- loss of main feedwater,
- small break LOCA, with extension to medium and large LOCA.
- loss of off-site power,
- spurious actuation of a safety function or isolation valve closure without a demand.

Each of the relevant PIEs for which no functional and performance information is available will need to be modelled. Normally at least two different parameters need to be identified for the

detection of each PIE, both of the parameters can then be used to initiate reactor protection actions independently. From the transients taken from the model, the following types of information will need to be derived:

- identification of the preferred measurement sensor for each trip parameter,
- definitions of the trip thresholds and accuracies needed to detect incipient faults,
- the time responses for each trip or safety actuation from detection of an incipient fault,
- natural language definitions of the trip or safety features actuation logic,
- definition of calculation algorithms,
- logic diagrams or other formal representation of the logic and algorithms.

It will be necessary to reference PSA studies to determine fully the dependability requirements. These will be likely to be demanding, and probabilities of failure on demand may be needed at a very low level.

In addition, systems in category A or B will normally need to meet the single failure criterion and the consequences of spurious initiation of the I&C safety functions should not lead to unacceptable conditions of the plant.

The recorded system and the model analysis results should be analysed for consistency, to determine the final requirements. A process for this could be:

- compare each recorded safety parameter with the modelled parameter,
- identify all thresholds, accuracy and time response factors in both,
- identify and resolve discrepancies,
- compare each recorded logic or algorithmic function with the modelled function,
- identify and resolve discrepancies,
- model specifically all changes arising from discrepancies and verify the requirements.

From this process, a specification of requirements can then be developed, to show each measurement needed, and each logic function or algorithm needed. This should give the functions, performance, dependability and operability requirements, as outlined in the main report.

II.3.2.Initial safety justification

The specification of the system, as developed above, will not be in a form which justifies the safety of the system systematically. It will be necessary to develop these detailed requirements in a form which allows confidence in the safety of the reactor if the intended refit or upgrade is undertaken. Various methods of providing this confidence have developed in different nations. The information needed should include:

- a description of the conceptual system,
- identification of the faults of the design base of the plant,
- description of the work done to model the plant ,
- description of the work done to define the safety functions and performance needed,
- identification of the key functions of the system, and reference to detailed descriptions of them,
- a justification that each function of the system will be achieved when it is needed,
- a justification that the integrity and dependability of the system is sufficient for the safety required.

Some valuable guidance on the practices of Canada, France, USA and UK is given in [34].

Appendix III

STRUCTURE FOR THE BASIC REQUIREMENTS SPECIFICATION DOCUMENT

III.1. TABLE OF CONTENTS

Remark: This document is intended to provide a specification contents for the technical requirements of a typical refit digital I&C system. For tendering or ordering purpose it should be used jointly with an administrative requirements document that should provide needed commercial, planning, QA and methodolgy information.

(The contract management material is provided for information on a typical method of working, but is outside the scope of the present report.)

III.2. SUMMARY OF CHAPTER CONTENTS

III.2.1. Introduction and objective

This chapter introduces general information about the I&C systems that are involved, the plant or plants that are concerned, the purpose of the refitting or upgrade.

III.2.2. Functions and performance of the delivery and warranties

Functions to be performed and associated performance required are described and detailed under the various operating conditions to be taken into account (normal, incidental, accident). Are indicated also the safety classification of the functions.

The performance requirements constitute also an input to contractual part of the contract as far as penalties are concerned.

III.2.3. Description, scope and limits of the delivery

In this section should be described as precisely as practicable:

- what is included/excluded from delivery,
- services to be provided as related to the delivery and its associated interfaces,
- included ancillary equipment that is needed for operation, tests and maintenance of equipment,
- part of the delivery,

- training to be foreseen for both operational and maintenance people,
- included spare parts and special tools.

III.2.4. Rules, norms, standards and QA

Rules, norms and standards that are to be taken into consideration are listed here, applicable revision of those documents are indicated. Provisions are taken relative to applicability of new revisions that could be issued during I&C project.

The safety or regulatory authorities or their representatives are identified.

Imposition relative to QA /QC are also listed.

III.2.5. Working conditions

Exhaustive list of working *(operating, environmental)* conditions are stipulated relative to the following aspects:

- type and characteristics of power supplies,
- signal isolation/separation characteristics,
- EMI classification,
- equipment/component life expectancy,
- ambient conditions for normal, exceptional, incidental, accident situations as far as temperature, pressure, dust, humidity, radiation, etc. are concerned,
- vibration required response spectra induced from mechanical origin, by earthquake, by aeroplane crash.

III.2.6. Design requirements

The design requirements to be elaborated and explained here are mainly originating from the methodology related analysis eventually amended by impacts of influencing factors.

This section may be used to give references to more detailed equipment and software specifications for each subsystem of the total project. General specifications may be referenced for generic technical aspects, such as seismic testing, environmental qualification, fire protection and cable or other interface requirements. A general specification of this type for software requirements and V&V can be an advantage. A general specification for equipment construction aspects can be an advantage. The section may separate into subsections for requirements for functional, performance, dependability, operability, and technology.

III.2.7. Design studies

As far as the studies to be performed by the I&C Contractor are concerned, following aspects should be outlined:

- methods involved,
- division or splitting of the studies into well identified steps,
- choice of tools, of software, etc.

III.2.8. Manufacturing, construction

Requirements associated with material selection, working procedures, electronic cabinet construction and wiring, electrical equipment safety, termination and cable requirements ...

Tests following manufacture are generally defined in principle. A requirement for detailed test documents produced during the contract for FAT and SAT is given.

III.2.9. Packing, transport, storage and handling

The specific precautions to be taken to maintain the quality of the delivered goods during transport up to the site, handling on site and storage on site

III.2.10. Erection and commissioning

What is expected from the contractor in relation with personnel number and qualification for on site activities.

Interactions with operation/maintenance procedures of the plant are identified.

Supplier site requirements for accommodation, parking, canteen services, temporary power supplies, heating etc., may be called for.

III.2.11. Controls and tests

The controls and tests that are to be performed in factory during design and construction and on the site during commissioning of the systems. Authorised Control organisms are also identified here. Support of I&C system suppliers during overall functional validation tests when restarting the plant should also be defined.

III.2.12. Documentation and training

All the documents should be listed that are required to be produced by the supplier throughout the life cycle of the I&C systems. Requirements about format, verification, legal approval (if required), etc. are given together with the planning for associated delivery. The training programs to be foreseen are detailed as far as content, number of attendees, time span, are concerned.

Appendix IV

RELATED STANDARDS

Listed below are standards related to the specification of requirements for upgrade of digital I&C systems. To limit the number, standards from the following institutions are included:

IAEA	International Atomic Energy Agency Codes on Safety and Safety Guides
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
ISO	International Organisation for Standardisation
US NRC	United States Nuclear Regulatory Commission Code of Federal Regulation (10CFR50) Appendix A of 10CFR50, General Design Criteria (GDC) Nuclear Regulations (NUREG) Regulatory Guides (RG).

The standards are grouped by the following areas:

- Safety,
- Life cycle and design,
- Qualification,
- Verification and validation,
- Quality assurance,
- Documentation,
- Detailed technical I&C-standards,
- Analysis methodologies,
- Miscellaneous.

IV.1. SAFETY

IV.1.1. IAEA

IAEA Safety Series No. 50-C-D	Code on the safety of nuclear power plants: Design.

IV.1.2. IEC

IEC 639 Ed.1	Nuclear reactors. Use of the protection system for non-safety purposes.
IEC 709 Ed.1	Separation within the reactor protection system.
IEC 1226 Ed.1	Nuclear power plants — Instrumentation and control systems important for safety - Classification.
IEC 61513 (in preparation)	Nuclear power plants — Instrumentation and control systems important to safety — General requirements for computer based systems.

IV.1.3. IEEE

IEEE-279-1971	Criteria for protection systems for nuclear power generating stations (This standard is withdrawn and is substituted by IEEE Std 603).
IEEE 384-1981	Criteria for independence of class 1E equipment and circuits (An updated 1992 edition is available).
IEEE 379-1988	Application of the single-failure criterion to nuclear power generating station safety systems (An updated 1994 edition is available).
IEEE 603-1980	Criteria for safety systems for nuclear power generating stations (An updated 1991 edition is available).
IEEE 7-4.3.2 - 1993	Criteria for digital computers in safety systems of nuclear power generating stations.

IV.1.4. US NRC

US 10CFR50a(h)	Protection systems.
US 10CFR50 Appendix A	General Design Criteria (GDC) GDC 10 Reactor design GDC 13 Instrument and control GDC 19 Control room GDC 20 Protection system function GDC 21 Protection system reliability and testability GDC 23 Protection system failure modes GDC 25 Protection system requirements for reactivity control malfunctions
US NRC NUREG-0800	Standard review plan, Section 7.0. Instrument and controls.
US NRC RG 1.152	Criteria for digital computers in safety systems of nuclear power plants.
US NRC RG 1.153	Criteria for power, instrumentation, and control portions of safety systems. *Note*: This Regulatory Guide endorses the IEEE Std 603 which is a system-level standard that contains some requirements related to performance and timing.

IV.2. LIFE CYCLE AND DESIGN

IV.2.1. IAEA

IAEA Safety Series No.50-SG-D3	Protection system and related features in nuclear power plants. A Safety Guide (currently under revision).

IAEA Safety Series No.50-SG-D8	Safety-related instrumentation and control systems for nuclear power plants. A Safety Guide (currently under revision).

IV.2.2. IEC

Note: In order to comply with the EU low voltage directive 73/23/EEC several different IEC-standards are applicable which are not included in this listing.

IEC 801 (part 1-4) (EN 60801)	Electromagnetic compatibility for industrial-process measurement and control equipment. Testing.
IEC 1000 (five sections) (EN 61000)	Electromagnetic compatibility for industrial process measurement and control equipment. Requirements.
	Note: IEC 801 and IEC 1000 are the most important standards to verify compliance to the EU (European Union) EMC directive. EMC-directive 89/336/EEC, 92/31/EEC.

The two set of standards are partly overlapping each other. But in general terms is IEC 801 dealing with testing and the requirements are given in IEC 1000.

IEC 643 Ed.1	Application of digital computers to nuclear reactor instrumentation and control.
IEC 880 Ed.1	Software for computers in the safety systems of nuclear power stations.
IEC 880-1 (In preparation)	Software for computers in the safety systems of nuclear power stations, as a first supplement to IEC 880.
IEC 960 Ed.1	Functional design criteria for a safety parameter display system for nuclear power stations.
IEC 964 Ed.1	Design for control rooms of nuclear power plants.
IEC 965 Ed.1	Supplementary control points for reactor shutdown without access to the main control room.
IEC 987 Ed.1	Programmed digital computers important to safety for nuclear power stations.
IEC 1225 Ed.1	Nuclear power plants — Instrumentation and control systems important for safety — Requirements for electrical supplies.
IEC 1227 Ed.1	Nuclear power plants — Control rooms — Operator controls.
IEC 1131 Ed. 1 (4 sections)	Programmable controllers.
IEC 1508 (In preparation)	Functional safety: safety-related systems. Part 1: General requirements.

IEC 1772 Ed.1	Nuclear power plants — Main control room — Application of visual display units (VDU).

IV.2.3. IEEE

IEEE 830-1993	Recommended practice for software requirements specifications.
IEEE 934-1987 (R1992)	Requirements for replacement parts for class 1E equipment in nuclear power generating stations.
IEEE 1023-1988	Guide for the application of human factors engineering to systems, equipment, and facilities of nuclear power generating stations.
IEEE 1042-1987	Guide to software configuration management
IEEE 1074-1991	Standard for developing software life cycle processes.

IV.2.4. US NRC

US NRC RG 1.172	Software requirements specification for digital computer software used in safety systems of nuclear power plants.
US NRC RG 1.173	Developing software life cycle processes for digital computer software used in safety systems of nuclear power plants. (This Regulatory guide endorses the use of IEEE Std 1074).

IV.3. QUALIFICATION

IV.3.1. IEC

IEC 780 Ed.1 and Amendment 1	Qualification of electrical items of the safety system for nuclear power generating stations.
IEC 980 Ed.1	Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations.
IEC 68 several parts (EN 60068)	Basic environmental testing procedures.
IEC 721 several parts (EN 60721)	Classification of environmental conditions.
	Note: The standards IEC 68 and IEC 721 are used during environmental qualification of I&C hardware. These two standards define the environmental conditions and the methods for qualification. Part 3 of IEC 68 deals with seismic test methods for equipment. (IEC 68-3-3).

IV.3.2. IEEE

IEEE 323-1983 (R1996)	Standard for qualifying class 1E equipment for nuclear power generating stations.
IEEE 344-1987 (R1993)	Recommended practice for seismic qualification of class 1E equipment for nuclear power generating stations.
IEEE 627-1980 (R1996)	Standard for design qualification of safety system equipment used in nuclear power generating stations.

IV.4. VERIFICATION AND VALIDATION

IV.4.1. IEC

IEC 671 Ed.1	Periodic tests and monitoring of the protection system of nuclear reactors.
IEC 1771 Ed.1	Nuclear power plants - Main control-room - Verification and validation of design.

IV.4.2. IEEE

IEEE 1008-1987	Standard for software unit testing.
IEEE 1012-1987	Standard for software verification and validation.
IEEE 1028-1988	Standard for software reviews and audits.

IV.4.3. US NRC

US NRC RG 1.168	Verification, validation, reviews and audits for digital computer software used in safety systems of nuclear power plants.
US NRC RG 1.170	Software test documentation for digital computer systems used in safety systems of nuclear power plants.
US NRC RG 1.171	Software unit testing for digital computer software used in safety systems of nuclear power plants.

IV.5. QUALITY ASSURANCE

IV.5.1. IEEE

IEEE 730.1-1989	Standard for software quality assurance plans.

IV.5.2. ISO

ISO 9000-3 Ed 1 (EN 29000-3)	Quality management and quality assurance standards-Part 3: Guidelines for the application of ISO 9001 to the development, supply and maintenance of software.

Note: This part of ISO 9000 sets out guidelines to facilitate the application of ISO 9001 to organisations developing, supplying and maintaining software.

The nature of software development is such that some activities are related to particular phases of the development process, while others may apply throughout the whole process (the life time of the software). ISO 9000-3 has therefore been structured to reflect these differences. Because of this does ISO 9000-3 not correspond directly in format with ISO 9001. To facilitate references between the two standards there are two cross-reference indexes provided as annex A and annex B in the standard ISO 9000-3.

IV.5.3. US NRC

US NRC RG 1.169	Configuration management plans for digital computer software used in safety systems of nuclear power plants.

IV.6. DOCUMENTATION

IV. 6.1. IEEE

IEEE 829-1983	Standard for software test documentation.

IV.7. DETAILED TECHNICAL I&C STANDARDS

IV.7.1. IEC

IEC 568 Ed.1	In-core instrumentation for neutron flux rate (flux) measurements in power reactors.
IEC 737 Ed.1	In-core temperature or primary envelope temperature measurements in nuclear power reactors. Characteristics and test methods.
IEC 772 Ed.1	Electrical penetration assemblies in containment structures for nuclear power generating stations.
IEC 910 Ed.1	Containment monitoring instrumentation for early detection of developing deviations from normal operation in light water reactors.
IEC 911 Ed.1	Measurements for monitoring adequate cooling within the core of pressurised light water reactors.
IEC 988 Ed.1	Acoustic monitoring systems for loose parts detection - Characteristics, design criteria and operational procedures.
IEC 1031 Ed.1	Design, location and application criteria for installed area gamma radiation dose rate monitoring equipment for use in nuclear power plants during normal operation and anticipated operational occurrences.

IEC 1224 Ed.1	Nuclear reactors — Response time in resistance temperature detectors (RTD) — In situ measurements.
IEC 1250 Ed.1	Nuclear reactors — Instrumentation and control systems important for safety — Detection of leakage in coolant systems.
IEC 1343 Ed.1	Nuclear reactor instrumentation — Boiling light water reactors (BWR) — Measurements in the reactor vessel for monitoring adequate cooling within the core.
IEC 1500 Ed.1	Nuclear power plants — Instrumentation and control systems important to safety — Functional requirements for multiplexed data transmission.
IEC 1559 Ed.1	Radiation in nuclear facilities — Centralised system for continuous monitoring of radiation and/or levels of radioactivity.

IV.8. ANALYSIS METHODOLOGIES

IV. 8.1. IEC

IEC 300-3-9 Ed 1 (EN 60300-3-9)	Risk analysis of technological systems.
IEC 300-1 Ed 1 (EN 60300-1)	Dependability management.
IEC 1069 (EN 61069) five parts	Industrial process measurement and control — Evaluation of system properties for the purpose of system assessment.
IEC 1078 Ed 1 (EN 61078)	Analysis techniques for dependability — Reliability block diagram method.
	Note: The standards IEC 300, IEC 1069 and IEC 1078 cover methods to verify the reliability of equipment. All four standards are applicable for I&C equipment in order to verify reliability requirements.
IEC 812 Ed 1	Analysis techniques for system reliability — Procedure for Failure Mode and Effects Analysis (FMEA).
IEC 1025 ED 1	Fault tree analysis (FTA).
IEC 1069 five parts	Industrial process measurement and control — Evaluation of system properties for the purpose of system assessment.
IEC 1078 Ed 1	Analysis techniques for dependability- Reliability block diagram method.

IV.8.2. IEEE

IEEE 352-1987 (R1993)	Guide for general principles of reliability analysis of nuclear power generating station safety systems.
IEEE 577-1976 (R1992)	Requirements for reliability analysis in the design and operation of safety systems for nuclear power generating stations.
IEEE 845-1988	Guide to evaluation of human–machine performance in nuclear power generating station control rooms and other peripheries.

IV.9. MISCELLANEOUS

IV.9.1. IEC

IEC 557 Ed.1	IEC terminology in the nuclear reactor field.

IV.9.2. IEEE

IEEE 610.12	Glossary of software engineering technology.
IEEE 982.1	Standard dictionary of measures to produce reliable software.
IEEE 982.2	Guide for the use of IEEE standard dictionary to produce reliable software.
IEEE 1061	Standard for a software, metric methodology.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook, Technical Reports Series No. 387, IAEA, Vienna (in press).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Modernization of Instrumentation and Control in Nuclear Power Plants, IAEA-TECDOC-1016, Vienna (1998).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Advanced Control Systems to Improve Nuclear Power Plant Reliability and Efficiency, IAEA-TECDOC-952, Vienna (1997).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Code on the Safety of Nuclear Power Plants: Design, Safety Series No. 50-C-D (Rev.1), IAEA, Vienna (1988).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection System and Related Features in Nuclear Power Plants: A Safety Guide, Safety Series No. 50-SG-D3, IAEA, Vienna (1984).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Instrumentation and Control Systems for Nuclear Power Plants: A Safety Guide, Safety Series No. 50-SG-D8, IAEA, Vienna (1984).

[7] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Classification, IEC -1226, IEC, Geneva (1993).

[8] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Qualification of Electrical Items of the Safety Systems for Nuclear Power Generating Stations, IEC Standard 780, IEC, Geneva (1984).

[9] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Environmental Testing. Part 3: Guidance. Seismic Test Methods for Equipment, IEC 68-3-3, IEC, Geneva (1991).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Verification and Validation of Software Related to Nuclear Power Plant Control and Instrumentation, Technical Reports Series No. 384, IAEA, Vienna (in press).

[11] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Functional safety: Safety-Related Systems. Part 1: General Requirements, IEC 1508, IEC, Geneva (in preparation).

[12] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — General requirements for Computer Based Systems, IEC 61503, IEC, Geneva (in preparation).

[13] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Electromagnetic compatibility (EMC), IEC, Geneva (1990–1995).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Quality Assurance for Safety in Nuclear Power Plants and other Nuclear Installations: Code and Safety Guides Q1–Q14, Safety Series No. 50-C/SG-Q, IAEA, Vienna (1996).

[15] INTERNATIONAL ORGANIZATION FOR STANDARDISATION, ISO-9000 Standard Series: Quality Management and Quality Assurance Standards, ISO, Geneva (1990).

[16] INTERNATIONAL ORGANIZATION FOR STANDARDISATION, ISO-9000 Standard Series: Quality Management and Quality Assurance Standards, Part 3: Guidelines for the Application of ISO 9001 to the Development, Supply and maintenance of Software, ISO, Geneva (1990).

[17] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Industrial-Process Measurement and Control — Evaluation of System Properties for the Purpose of System Assessment. Part 1 - General Considerations and Methodology, IEC 1069-1, IEC, Geneva (1991).

[18] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Design for Control Rooms of Nuclear Power Plants, IEC 964, IEC, Geneva (1989).

[19] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Programmed Digital Computers Important to Safety for Nuclear Power stations, IEC 987, IEC, Geneva (1989).

[20] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Electromagnetic Compatibility for Industrial-Process Measurement and Control Equipment, IEC 801, in two parts: IEC 801-1, Part 1: General Introduction (1984) and IEC 801-2, Part 2: Electrostatic discharge requirements, IEC, Geneva (1991).
[21] INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, IEEE Std 323, IEEE, Piscataway (1983).
[22] INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS, IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, IEEE Std 344, IEEE, Piscataway (1987).
[23] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Software for Computers in the Safety Systems of Nuclear Power Stations, IEC 880, IEC, Geneva (1986).
[24] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Software for Computers Important to Safety for Nuclear Power Plants (first supplement to IEC 880), IEC 880-1, IEC, Geneva (in preparation).
[25] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Main Control Room - Application of Visual Display Units (VDU), IEC 1772, IEC, Geneva (1995).
[26] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Verification and Validation of Control Room Design, IEC 1771, IEC, Geneva (1995).
[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Issues for Advanced Protection, Control and Human–Machine Interface Systems in Operating Nuclear Power Plants, Safety Reports Series No. 6, IAEA, Vienna (1998).
[28] INTERNATIONAL ATOMIC ENERGY AGENCY, Computeriztion of Operation and Maintenance for Nuclear Power Plants, IAEA-TECDOC-808, Vienna (1995).
[29] INTERNATIONAL ATOMIC ENERGY AGENCY, Control Room Systems Design for Nuclear Power Plants, IAEA-TECDOC-812, Vienna (1996).
[30] INTERNATIONAL ATOMIC ENERGY AGENCY, Computerizd Support Systems in Nuclear Power Plants, IAEA-TECDOC-912, Vienna (1994).
[31] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment of Computerized Control and Protection Systems, IAEA-TECDOC-780, Vienna (1994).
[32] INTERNATIONAL ATOMIC ENERGY AGENCY, Software Important to Safety in Nuclear Power Plants, Technical Reports Series No. 367, IAEA, Vienna (1994).
[33] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Recommended Practices for Seismic Qualification of Electrical Equipment of the Safety Systems for Nuclear Generating Stations, IEC980, Geneva (1989).
[34] Four party regulatory consensus report on the safety case for computer-based systems in nuclear power plants. UK Health and Safety Executive Publication — HM Stationary Office, Norwich.

GLOSSARY

Backfit	See retrofit, refit.
CCF	Common cause failure. The failure of a number of devices or components to perform their functions as a result of a single specific event or cause (IEC 61513). The event or cause which triggers the I&C system failure may be internal or external to the safety system, a specific process dependent loading, a human induced operation or a maintenance error, a natural phenomena or a change in ambient conditions.
EMC	Electromagnetic compatibility. The capacity of I&C equipment to withstand an electromagnetic field of a certain field strength (V/m) and the properties of the equipment such that it does not cause an electromagnetic field higher than a certain level. A certain level of electromagnetic field strength must not cause any electromagnetic interference. The requirements for Electromagnetic Compatibility are given in IEC 1000 and the requirements for testing the electromagnetic compatibility are given in IEC 801.
EMI	Electromagnetic interference. See EMC.
EQ	Equipment qualification. Systematic testing or analysis undertaken to demonstrate that a system or an item of equipment will perform all its safety functions correctly in any environmental condition for which it is required to operate. The requirements for environmental EQ are given in IEC 780, IEC 68 and IEC 721 as well as IEEE 323 and IEEE 627. The requirements for seismic EQ are given in IEC 980 and in IEEE 344.
FAT	Factory acceptance. Systematic written tests, defined beforehand, and undertaken in the factory to demonstrate that the functionality and performance of equipment meets the requirements. (See also SAT).
HELB	High energy line break. (Referring to the release of high energy steam or water following breach of pipelines or vessels).
HMI	Human–machine interface. Human–machine Interface formerly called Man–machine Interface and sometimes called Human-Computer Interface. The means of communication between human and a computer or control panel for plant or equipment. This is frequently a VDU, dependent on computers and a design which should allow for human factors interests.
HVAC	Heating, ventilation and air conditioning equipment.
IV&V	Independent verification and validation. A process of verification and validation of the software of a computer-based system by a group or organisation independent from the software developer. IV&V may involve human examination of documents and code, automated analysis, additional testing and other work described in [10].
Migration	The progressive or phased installation of new equipment in a manner which allows for continuity of service, when applied to refits and upgrades and similar improvements.
MMI	Man–machine interface. See HMI.
PSA	Probabilistic safety analysis. PSA is a systematic assessment and estimation of the probability of reactor system faults and their consequences.

Refit	To design, provide and install equipment to replace obsolete equipment, usually with identical functionality. An example might be to refit a plant with new pressure transducers, replacing obsolete devices. See also retrofit, backfit.
Retrofit	Also backfit, refit. To design, provide and install equipment in order to replace or improve existing equipment performance or dependability, with little or no change of equipment functions. Examples would be to refit or backfit a plant with new qualified pressure instruments, replacing unqualified instruments, or to add redundant power supplies to improve reliability, or to replace an analogue electronic card with one that incorporates an integrated circuit to perform the same card functions.
Refurbish	To identify weaknesses in existing equipment and to replace parts, modules or components which are obsolete, damaged, broken or otherwise unsuitable. For example, replacing all the power packs and damaged terminals in an electronic cabinet with switched mode power packs and fitting new terminals. Another example would be to replace aged capacitors in power supplies.
Safety authority	The government organisation responsible for granting a licence to operate the power, and any agent acting for it which considers the design and the safety of the plant. The safety authority is often known as a regulator or a safety inspector, or a similar term.
Safety case or safety analysis report	A systematic statement of justification of the properties of a system, which has a major role in or supports the safety of the plant concerned. The statement gives the justification in relation to the design, implementation, testing, installation and operation of the system. The safety case is prepared for the Safety Authority concerned with licensing acceptance of the plant. Normally a safety case will also reference other documents and give their conclusions, where they report activities such as EQ, IV&V and the system acceptance test.
SAT	Site acceptance test. Systematic written tests, defined beforehand, and undertaken on site after installation to demonstrate that the functionality and performance of equipment meets the requirements. (See also FAT).
Test	A set-up of equipment, often of computer equipment, in a test environment platform usually in the factory, arranged to allow systematic tests of configurations of hardware and software relevant to some application.
Upgrade	To design, provide and install equipment to replace equipment, hardware and software of one or more systems, with added functionality, performance or reliability features. An example would be to provide a new information, display and logging computer system, with VDU displays and logs, replacing analogue control room instruments and a reactor monitoring computer. Another example would be to replace a control room array of alarm annunciators with a computer-based system with automatic logic to assign safety or operational importance to each alarm.

CONTRIBUTORS TO DRAFTING AND REVIEW

Andersson, O.	Forsmarks Kraftgrupp AB, S-742 03 Östhammar, Sweden
Bock, H.-W.	Siemens AG-KWU, Abt. NLL, Frauenauracher Strasse 85, D-91056 Erlangen, Germany
Naisse, J.-C.	TRACTEBEL, Technical Department, Avenue Ariane 7, B-1200 Brussels, Belgium
Neboyan, V.	International Atomic Energy Agency, Division of Nuclear Power, Wagramer Strasse 5, P.O. Box 100, A-1400 Vienna, Austria
Park, Ik-Soo	System and Comm. Laboratory, Korea Electric Power Research Institute, 103-16 Munji-dong Yusong-gu, Taejon 305-380, Republic of Korea
Santinelli, A.	ANSALDO Divisione Nucleare, Corso Perrone 25, I-16161 Genova, Italy
Skull, G.	Siemens AG-KWU, Abt. NLL5, Fraunauracher Strasse 85, D-91056 Erlangen, Germany
Welbourne, D.	Manor Farm Barn, Little Humby, Grantham, Lincolnshire NG33-4HW, United Kingdom
Wilkinson, D.	SAIC, 14015 Oak Valley Road, Morgan Hill, California 95037, United States of America

Advisory Group Meeting

Vienna, Austria: 29 September – 3 October 1997

Consultants Meetings

Vienna, Austria: 17–21 March 1997, 9–13 March 1998