COMMISSARIAT A L'ENERGIE ATOMIQUE

INSTITUT DE PROTECTION ET DE SURETE NUCLEAIRE

DEPARTEMENT D'ANALYSE DE SURETE

RAPPORT DAS/729e

BALANCE BETWEEN AUTOMATION AND HUMAN ACTIONS IN NUCLEAR POWER PLANT OPERATION.
RESULTS OF INTERNATIONAL COOPERATION.

BASTL W. *, JENKINSON J. **,
KOSSILOV A. ***, OLMSTEAD R. ****,
OUDIZ A. *****, SUN B. ******

INTERNATIONAL ATOMIC ENERGY AGENCY SYMPOSIUM ON BALANCING AUTOMATION AND HUMAN ACTION ON NUCLEAR POWER PLANTS.
Munich, 9-13 july, 1990.

RAPPORT DAS/729e

BALANCE BETWEEN AUTOMATION AND HUMAN ACTIONS IN NUCLEAR POWER PLANT OPERATION. RESULTS OF INTERNATIONAL COOPERATION.

BASTL W. *, JENKINSON J. **,
KOSSILOV A. ***, OLMSTEAD R. ****,
OUDIZ A. *****, SUN B. ******

INTERNATIONAL ATOMIC ENERGY AGENCY SYMPOSIUM ON BALANCING AUTOMATION AND HUMAN ACTION ON NUCLEAR POWER PLANTS.
Munich, 9-13 july, 1990.

1990

* GRS, Garching, RFA
** Nuclear Electric PLC, Gloucester, U.K.
*** AIEA
**** AECL, Mississauga, CANADA
***** EPRI
****** DAS/LEFH

INTERNATIONAL ATOMIC ENERGY AGENCY
OECD NUCLEAR ENERGY AGENCY

INTERNATIONAL SYMPOSIUM ON BALANCING AUTOMATION AND HUMAN ACTION IN NUCLEAR POWER PLANTS

Munich, Federal Republic of Germany, 9–13 July 1990

IAEA-SM-315/ 1

BALANCE BETWEEN AUTOMATION AND HUMAN ACTIONS IN NUCLEAR POWER PLANT OPERATION - RESULTS OF INTERNATIONAL CO-OPERATION

W. BASTL, J. JENKINSON, A. KOSSILOV, R. OLMSTEAD, A. OUDIZ, B. SUN

International Atomic Energy Agency
Wagramerstrasse 5, P.O. Box 100
A-1400 Vienna, Austria

BALANCE BETWEEN AUTOMATION AND HUMAN ACTIONS IN NUCLEAR POWER PLANT OPERATION - RESULTS OF INTERNATIONAL CO-OPERATION

Abstract

Automation has long been an established feature of power plants. In some applications, the use of automation has been the significant factor which has enabled plant technology to progress to its current state. Societal demands for increased levels of safety have led to greater use of redundancy and diversity and this, in turn, has increased levels of automation. However, possibly the greatest contributory factor in increased automation has resulted from improvements in information technology. Much recent attention has been focused on the concept of "inherently safe reactors", which may simplify safety system requirements and information and control system complexity.

The allocation of tasks between man and machine may be one of the most critical activity in the design of new nuclear plants and major retro-fits and it therefore warrants a design approach which is commensurate in quality with the high levels of safety and production performance sought from nuclear plants.

Facing this climate, in 1989 the International Atomic Energy Agency (IAEA) formed an advisory group from member countries with extensive experience in nuclear power plant automation. The task of this group was to advise on the appropriate balance between manual and automatic actions in plant operation.

Based on earlier research and their own experience, the group determined that a single, fully deterministic solution to the task allocation problem is not possible. However, since the role of the operator is expected to change over time to that of system manager, it is imperative that a systematic process for allocating tasks must be used by the design team. The group proposed a methodology which builds upon earlier published work but adopts a pragmatic approach, suited to real-project needs. The methodology identifies a number of factors which are relevant to the decision making process, discusses viable approaches to decision making, provides guidance on such decision making and identifies areas which it is considered that further research is required.

INTRODUCTION

Automation has long been an established feature of power plants. In some applications, the use of automation has been the significant factor which has enabled plant technology to progress to its current state. Societal demands for increased levels of safety have led to increased use of redundancy and diverse systems. This, in turn, has led to increases in the use of automation. However, possibly the greatest contributory factor in increased automation has resulted from improvements in information technology.

Much recent attention has been focused on the concept of "inherently safe reactors", which may simplify safety system requirements and information and control system complexity. If such concepts eventually lead to commercial power reactor designs there may well be simplifications in plant systems but is difficult to see how the total protection, control and monitoring requirements will remove the need for systematic allocation of functions between men and machines.

Data from accident and significant event reports, together with a review of past and current design processes reveals that plant designers often do not demonstrate the use of a systematic method for making the necessary series of critical decisions which allocate functions to men or machines, that is to establish the extent and role of automation. Similar sources indicate that design teams have not always adequately considered the capabilities and limitations of humans when making these ad hoc decisions. Post Three-Mile-Island studies in Europe, such as that carried out by CEC JRC Ispra in 1980 [1] have examined a comprehensive range of factors material to safe operation including m.m.i. design, training, simulation and management factors but there has been little formal examination by such groups of the actual role assigned to operators.

Although nuclear power plants are designed to exacting standards, using thorough quality assurance systems, they are designed and operated by humans and as such, they can never be perfect or free from the consequences of error. This situation effectively ensures that there is a continuing role for the operator for the foreseeable future. As automation takes over the more prescriptive tasks, the role of the operator becomes that of a situation manager - an innovator to manage the unexpected.

The allocation of tasks to a combination of man and machine may be one of the most critical activity in the design of new nuclear plants and major retro-fits and it therefore warrants a design approach which is commensurate in quality with the high levels of safety and production performance sought from nuclear plants.

Facing this climate, in 1989 the International Atomic Energy Agency (IAEA) formed an advisory group from member countries with extensive experience in nuclear power plant automation. The task of this group was to advise on the appropriate balance between manual and automatic actions in plant operation. Even the most recent control room design standards (e.g. IEC Standard 964), [2], make no attempt to define a methodology for the allocation of functions between men and machines. Consequently, the advisory group undertook to develop tha base for such a design process.

Based on earlier research and their own experience, the group determined that a single, fully deterministic solution to the task allocation problem is not possible. However, since the role of the operator is expected to change with time to that of a system manager, it is imperative that a systematic process for allocating tasks must be used by the design team. This paper describes a proposed methodology which has been developed by the group. The proposed methodology builds upon earlier published work but adopts a pragmatic approach, suited to real-project needs. The document uses the term 'design team' to encompass all those whose responsibilities include design of the control room and other man-machine interfaces, together with the allocation of functions to men and machines.

It is summarised in a simplified diagram (Figure 1) illustrating the main features of the process.

RESEARCH INTO ALLOCATION OF FUNCTIONS

To achieve a balance between automation and human actions the designer must assign operational function to either machines, human operatives or, more commonly in nuclear plants, a combination of man and machine. The process is usually known in the ergonomics literature as "allocation of functions". The general principles of allocation of functions have been well established by research which dates back some 40 years.

The concepts of systems engineering, components within those systems and the relative performance of the parts and the whole are accepted tenets, which are supported by practical experience in their application to a variety of industrial and other situations. Design methodologies have been proposed, developed and proven which allow non-specialists to apply known principles and hence achieve acceptable system designs. However, as plant designs have become more complex the required level of sophistication has also risen and system performance targets have had to be raised. A consequence has been that the process of allocating functions must be carried out to a greater degree of surety to ensure that overall system performance can be reliably achieved.

This search for improved design quality requires a greater understanding of the way in which the components of a man-machine system behave. In high-risk industries, where system performance is critical to safe operation, human behaviour under extreme circumstances becomes of dominant interest. In all these areas, the extent of available knowledge is incomplete and many workers are researching these topics. There is scope for more work specifically directed to the needs of the nuclear power industry.

The Attribute List Approach

Research into what has commonly become known as allocation of functions in complex industrial systems can be traced to the work of Paul Fitts in 1951 [3]. His fundamental axiom was to assign tasks to man or machine according to what each is best as. For example, rapid and reliable processing of mathematical data is best achieved using a computing machine of some sort.

Conversely, pattern recognition within a noisy signal or handling of infrequent information overloads are areas where humans can excel over machines. Similarly, tasks which require intuition or inventive solutions cannot be readily assigned to a machine and again, man can achieve higher performance.

Fitts' concept was to identify various attributes of both humans and technological systems which reflected their differing abilities and capabilities and to express these in the form of standard lists. These lists were then used to assist in classifying tasks to be performed either by man or machine. Numerous examples of such tables can be found throughout the ergonomics literature.

It must be noted that the theory reflected the prevailing state of technology at the time the theory was propounded. Advances in computer-based devices and in software have modified the previously clear cut boundary which Fitts perceived.

Practical Problems

Human capabilities remain substantially the same over time, whereas advances in technology result in rapid changes to what can be reasonably expected from the machine. A bigger problem is that this approach suggests a separation of tasks between the two components, man or machine whereas in a modern man-machine system the need is to ensure complimentary working of man and machine. Experience shows that simple tabulations are relatively crude in the advice they give and they may be regarded only as introductory material for the novice worker. Experienced designers will find the lack of subtlety in the data and the lack of guidance on how it is affected by practical situations a severe limitation.

Attempts to Quality Behaviour

Jordan, (1963) see Edwards & Lees 1972, [4] clarified the basic problem with the simple comparison list approach by asserting that such comparison tables will commonly favour the machine, particularly if they use quantitative data. Attempts to quantify human behaviour have not been totally satisfactory and although it is possible to measure human performance to an extent, databases of such information are not easily and satisfactorily combined with the more factual and actuarial data obtained from studying machines. This is particularly true when human reliability is studied in the context of overall system reliability which is often done when evaluating nuclear power plants.

Relative Strengths of Humans and Automation

Jordan expressed this problem in the following terms: "Man is not a machine, at least not a machine like the machines made by men". The conclusion must be that men and machines both have properties which can contribute to overall system operation. Machines are consistent but inflexible; men are inconsistent but flexible. Many such opposing attribute-pairs can be identified. The challenge to the system designer is to utilise both sets of attributes in an optimum manner in creating his design. Man and machine work best in a complementary manner where the design of their individual roles is in harmony. In many cases this will involve a sharing of tasks between man and machine and the allocation process becomes one of controlled sharing.

Chapanis, (1965) [5] continued this theme when he argued that the systems engineer, when taking the fundamental decisions about the functions to be performed by the various parts of a system, must throughout keep in mind that the separate parts of the system must cooperate effectively. Decisions about the machine component are based partly on what the machine can and can't do. This is relatively well known but varies with time, as machine capabilities increase.

System Design Goals

Earlier research took as its goal the optimisation of the human and machine components in a system in order to achieve overall system objectives, specified in terms of the overall performance required. As performance requirements have increased, increased attention has had to be paid to factors which can lead to degradations in the performance of the human component in a system. Situations which challenge the performance of humans can increasingly be seen to relate to the social and socio-environmental aspects of working situations, particularly where increased automation has led to a change in role of the human to one of system manager. Kantowitz and Sorkin, (1987) [6] support this need for any system design to be based on sound definition of goals. They also point out that allocation of functions determines not only how well the overall man-machine system will operate, but also the quality of the working life for the persons involved with the system. It can be argued that such goals should, inter-alia, include the well-being and job-satisfaction of the operator. This view is often seen to be in conflict with the traditional 19th Century-based concept of humans as an expendable part of a system and its later 20th Century derivatives of humans as 'flexible' components of a system, which can be relied on to meet extremes of demand using extremes of behaviour.

DESIGN METHODOLOGY STATUS

Initial attempts to provide a design methodology to support the allocation of functions were based upon a simple view of the relative attributes of men and machines. Although later workers showed the limitations of this approach, it has the merit of simplicity. An even more simple approach which has been proposed is to automate everything which can be automated. Although lacking in elegance, this approach is increasingly popular given that the capabilities of machines can be increased for relatively little cost nowadays. A consequence of this approach is that the human being is given the leftovers from the process, rather having a set of tasks deliberately assigned to him.

Major problems can arise from either overloading or under-loading the human being. In many cases, such problems may remain un-revealed during normal operation, but it is common for the results of such a coarse approach to be revealed in an unacceptable manner during fault operation or transient management, where operators fail to cope successfully due to performance overload or insufficient skills due to lack of involvement or practice. Again, inappropriate allocation of functions can result in increased stress for the operators, with consequent degradations in performance during operational situations where maximum performance is sought from the human components in the system.

Improved approaches which overcome some of these problems rely on a more sophisticated classification of functions. In many practical situations, there will be constraints on the designer which effectively dictate a particular allocation. Custom and practice, or indeed statutory requirements may dictate that a particular function be carried out in a certain way. Furthermore, a priori decisions by management may reduce the designer's freedom. Where the designer is concerned with a modification to or a partial extension of an existing system he may not have the freedom to examine previous allocation decisions and hence may not be able to achieve optimised allocations.

In many instances, it will be necessary to provide a quality-assured design in which all decisions regarding allocation of functions are documented and supported by adequate data. Approaches have been developed which seek to provide quantification of the factors involved by establishing decision criteria based on safety, availability, reliability, maintainability, cost, etc. and then assigning quantitative values to each factor, [6]. Paired comparison techniques are then used to establish relative importances and weighting the results. It is difficult to see this approach yielding unequivocal results or becoming widely used but it may have merit in causing the designer to consider all relevant factors in more systematic manner.

The most comprehensive approach to the problem of allocating functions in Nuclear Power Plants was produced by Pulliam, Price, et al., in 1983 as NUREG CR-3331, [7]. The method consists of many stages of analysis which if performed for each and every function of a new plant design would represent a significant engineering resource. This report was preceeded by a comprehensive review of the subject, including a useful set of references to which the interested reader is directed, [8]. The value of this work to the present proposals is acknowledged. However, whilst the earlier work is comprehensive, it is questionable whether the method proposed is realistic in a true design situation. Also, the method does not fully account for the practical 'sharing' of tasks which occurs when the operator is provided with means of intervening in automatic processes and when automation is used to support operator decision-making.

The proposed methodology addresses these points by presenting a pragmatic, and it is hoped, cost-effective method for allocating functions in a large-project context.

PROPOSED ALLOCATION METHODOLOGY TO ACHIEVE A BALANCE

Principles

Underlying the proposed methodology are a number of principles. These may be stated as follows:-

(1) Human cognitive strengths should be fully exploited by the designer - there are some things that man does better than machines. The three disciplines of engineering, ergonomics and psychology must work in harmony to exploit these strengths.

(2) Automation should be used to protect society from the fallibility and variability of humans - this requires a detailed analysis of the tasks which are proposed for man, the possible errors and the possible consequences. Areas of risk should be automated if this is practical, feasible and cost-effective.

(3) Automation should start with the most prescriptive procedural functions first - the boundary of automation is within the human component in the system and is likely to remain so for some time to come. Those manual functions that are memorised or performed prescriptively by detailed procedures should be automated when ever possible.

(4) Automation should be used to reduce human cognitive overload - humans can suffer from information overload and consequent mental overload. This can occur from high information rates, competing tasks or task complexity. Wherever the designer can predict this problem, or whenever operating experience demonstrates it to be so, automation should be used to relieve the human of that part of the function which causes the problem. Note that wholesale automation in such cases may not be at all appropriate.

(5) If possible, tasks which have been allocated to automation should not be designed to return to the man when the automation fails - in general, humans do not act effectively as a back-up to a machine. In most cases, the reason for using a machine is that a human capacity has been exceeded. Consequently, human back-up is unlikely to be appropriate. Machine performance is more consistent if not more available so humans make a poor substitute. Also, human capabilities grow stale with lack of use. To suddenly present a set of new tasks onto an unsuspecting operator when a machine fails is a prime example of poor design.

(6) The correct process for balancing human and machine actions should become an institutionalised part of system design. The right balance will not emerge until there are processes in place and in common use by designers, operators and management, which reflect the correct principles and embody proven practices. The evaluation should include consideration of the professional motivation and psychological well-being of the operator.

Systematic Design

Function, Task and Activity Analysis

The methodology proposed in the document for the allocation of functions is assumed to form part of a wider, overall design process which adopts a hierarchical, systems approach and incorporates a series of controlled iterations. The allocation method requires all necessary 'functions' which need to be performed for the correct operation of the plant to be identified and then subsequently allocated to humans or machines. Prior to allocation, the method deals with 'functions'. When these have been allocated, the resultant activities are referred to as 'tasks'.

A complete analysis will allow functions to be identified with sufficient resolution to enable tasks to be assigned to either humans or machines. In many cases, the depth of analysis required will be prohibitive or resource-limited. Conversely, lack of firm design data may preclude such detailed analysis in all areas of the plant. The proposed methodology recognises these problems by allowing for the concept of 'shared tasks', involving both man and machine, in order to simplify the required analysis. In many cases, the more detailed information required to complete the design of the automation and to determine operator job specifications, operating procedures, etc. will evolve as the overall plant design progresses. By adopting the proposed shared task definition, a simplified allocation process results.

Task Sharing

Many functions in nuclear power plants are achieved by a combination of human action and automation. A common example of this is the use of automation to detect and annunciate plant conditions, in the form of an operator information system. The human operator uses this information to make judgements, take decisions and execute control actions.

Increasingly, computer-based systems can be used to support operators in the performance of their tasks. There are many benefits which can accrue from the use of technology in this way but it is important to ensure that the design of the support system and of the operator's task places him in the correct role in relation to the machine; that is in a intellectually superior position, with the machine serving the operator. Technological advances such as those in artificial intelligence and expert systems suggest that automation of many tasks which was hitherto impractical is now a possibility. It is true that automation can be used to an increasing extent in the support of human tasks and to an extent, replace certain aspects of human involvement. However, considerations of system integrity, software validation and verification, consequences of error, etc. places limits on the extent to which critical functions can be placed in the control of automatic systems.

A systematic allocation of functions process requires four essential elements to be satisfactorily carried out:

- a detailed knowledge of the individual operations to be carried out for the safe and effective running of the system; the so-called functions.

- a knowledge of the capabilities and limitations of the human operator population which is to be employed for operation and maintenance of the system.

- an understanding of the capabilities and limitations of the available technology for design, manufacturing, and implementation of the system.

- criteria by which to determine how functions should be allocated between man and automation.

In practice, allocation of functions cannot be a simple and mechanistic process. Firstly, the information required to make the decisions may be incomplete or uncertain, particularly in the early stages of the project. Secondly, the criteria against which to make allocation decisions may not be absolute or may apply only conditionally. Thirdly, any individual allocation decision may interact with a previous one, necessitating re-examination and iteration of that decision leading to a revised decision. Thus the allocation of functions process is of necessity an iterative one and must be thought of as a balancing of the several factors which are involved rather than the meeting of a set of fixed design rules.

In the case of nuclear power plants, to ensure true complementary operation between the two components: man and machine, the designer must ensure that man's capabilities are properly employed; being neither exceeded or under-used. For instance, the size and complexity of many existing control rooms can lead to human capability limits being exceeded, in areas such as alarm presentation at high rates under abnormal plant conditions. Conversely, the provision of large amounts of computer control can reduce the role of a skilled operator to one of a disinterested machine minder. The team who design the system must therefore exercise caution and provide additional machine support to counter potential overload, and carefully define the operator's job to ensure that he remains in touch with the automatic process.

In many cases, it may be essential to employ automation to achieve the necessary degree of safety or reliability. In the event of such systems failing, manual intervention would not be practicable because the human performance would not be adequate. Therefore, complex, expensive engineering solutions are often necessary to provide the required system reliability and availability.

Humans are often expected to take over a machine function when automation fails. All those who create and use complex systems, must recognise that the use of automation may change the role of the operator in a system and may, for instance, result in him becoming decoupled from the workings of the process he is supervising. The operator may become de-skilled and therefore be unable to take over when the automatic feature fail.

In an ideal situation, the assignment process would consider all possible tasks in an exhaustive manner. In practice this is not possible due to the amount of effort which would be involved, the length of time it would take to carry out and the disproportionate use of resources which would be needed. There will be a need to limit the extent and depth of the analysis for the assignment process. These limits must ensure that the analysis is adequate to meet safety and operational needs and that it provides the necessary basis for justification of the design. It is recommended therefore that the analysis be top-down hierarchical and broad in nature, i.e. it should address all areas of the plant for its potential impact and consider all operational conditions, particularly fault situation. Where deciding on the required depth of analysis in any one area, the required guideline is that the analysis must be carried to a sufficient depth to allow all automatic features to be fully specified and to allow all operating staff tasks to be defined.

Influencing Factors

The following qualitative factors will modify the relative weighting used in allocating function. The order in which the factors are given does not imply any prioritisation, which must be determined by the user for each application.

(i) Existing Practices

The extent of automation depends on operational practices and the level of technological and experiential support that is available. For example, staff trained in computer maintenance may be required before a high degree of automation is possible.

(ii) Operational and Design Experience

Experience is often critical in establishing the confidence and justifications for further automation. For example, if an organisation has successfully implemented (design and operation) an automatic control function which has resulted in say fewer spurious plant shutdowns, that utility is more likely to consider more automation.

(iii) Regulatory Factors

Regulating bodies establish specific, inflexible rules which may restrict or conversely, require automation.

(iv) Feasibility

Sometimes, automation is not possible for practical reasons; for example, installation down time may preclude modification in an existing plant.

(v) Cost

There are very few cases where other factors will totally outweigh cost. A cost benefit must exist to justify most proposals to automate.

(vi) Technical Climate

Increasing capabilities of technology may facilitate automation. Unavailability of technology may limit what can be automated.

(vii) Policy Matters

An organisation may develop policies that encourage or discourage automation. For example, the decision to standardise on a type of plant design, hence level of automation.

(viii) Cultural and Social Aspects

For example, the reduced role of operator is a highly automated plant may represent a social problem for his that can lead to demotivation and significantly decreased performance.

These influencing factors can be taken as 'givens' in the assignment process. The various factors which exist may differ between projects and may be affected by whether a new design is being considered or a modification to an existing process through retrofit. In the latter case, the designer must expect more 'givens' and less flexibility, due to existing plant designs, operating practices, the need for replication, etc.

Required System Performance

There is frequently a need for the detailing of system level requirements that can be used as a basis for making decisions on the allocation of tasks and on the design of the user-system interface. Human performance requirements will not be established until tasks have been allocated either to humans or to machines. The performance of the total complex of men and equipment, working together to achieve task goals, can be assessed at a later stage by seeing how well established requirements are being met.

It is essential to know, therefore, what overall system performance is required, both as an average and as a minimum acceptable level, and in normal conditions and under adverse conditions.

The performance of software and hardware components can be described and measured by known techniques, using known measures such as speed, size, accuracy, reliability, or repeatability. Human performance can also be measured by known techniques, using measures such as speed, accuracy, processing time, production rate, error rate, training time to criterion level, or level of job satisfaction. Straight comparisons between humans or equipment in performance of a task have to be seen in the context of the associated tasks that are being performed and the total efficiency in job performance. There can be trade offs that influence the allocation process.

System performance levels will be influenced by the ways that the humans and the hardware/software components of the system interact dynamically. Information functions should be described systematically, with human-machine interactions mapped in accordance with human factors models. This will cater to information needs, capacities, feedback loops, and cognitive loading levels.

Human Performance Data

The design team requires access to relevant sources of human factors data, initially to provide a yardstick for general function allocation decisions, and subsequently for refinement of those decisions to meet system performance requirements. The general human factors literature includes recommendations on the effect on human performance of variation in areas such as:

- general user-system interface design
- information system display design
- computer-generated information presentation
- control system design and layout
- controls design and labelling
- human cognitive functioning (memory and perception)
- inter-person communications
- human error prevention and recovery
- design of documents and procedures
- workplace environmental variables
- design an use of protective clothing and equipment
- work design and organization
- work crew organization and functioning
- work shift scheduling.

Much of the data presented in the literature has been specified at a general level of applicability. That is, these data on human capabilities and limitations are population findings that may be modified for specific applications where situational variations move the data distribution in predictable ways.

Assigning The Functions

The methodology starts from three sources of information, global project objectives, statements of required system performance and a knowledge of human and machine performance. Although stated this way for brevity, in a practical situation, these three sets will represent a considerable amount of information. Complete data on required system performance, etc., may not be available at the outset. It will therefore be necessary to employ an iterative approach, taking what is available first and identifying what is outstanding and the need for certain source information may become apparent after initial allocations have been made.

Having identified the various functions which must be performed the designer should proceed to classify them as follows:

- functions which must be automated
- functions which are better automated
- functions which should be done by humans
- functions which should be shared

The main part of the allocation process consists of identifying these four types of function. At this stage, the lists can only be hypotheses since the design team may not have worked with complete information and may not have considered all interactions and all limiting factors.

In a second step each of the initial allocations must be re-examined in the context of all others in order to identify any inconsistencies. Where an allocation produces conflict with accepted human factors principles, the allocation must be reconsidered and revised. When these two categories of mis-match have been resolved it is then possible to proceed to optimise the allocation in order to achieve the best possible set of working tasks and machine specifications.

The results of the allocation process will be two sets of information which are fed into the overall design process. Firstly, there will be lists of tasks which have been assigned wholly to a single operator or to a group of operators, but because the process described allows tasks to be shared between humans and machines, the list will also need to contain such shared tasks. The list will be used subsequently to produce statements of staff requirements, training requirements, operating procedures, rules and supporting job-aids. The second output from the allocation process will be a set of statements of the required automation, information systems and man-machine interface design. These will be used in the design, in order to provide the necessary sensors, signals, etc. and in the detailed design of the man-machine interface including information displays, automatic control system interfaces, etc. The information will also be used to define the required manual control interfaces.

The process is completed by a final audit phase, to be carried out at a suitable time. The purpose of this phase is twofold. Firstly, it serves to validate the many decisions which have been taken during the allocation and project development phases and secondly, it provides an opportunity to ensure that documentation of those decisions is adequate to allow subsequent re-examination and possible revision.

Functions Which Must Be Automated

The first consideration must be to examine any functions for which automation is mandatory. It is desirable that any such task definitions would be justifiably based on human factors principles but this may not always be so where mandatory requirements are based on established custom and practice. The designer should understand the fundamental reason behind any such mandatory requirements to ensure they are appropriately and responsibly applied.

The designer must proceed to identify all the functions which, by virtue of their nature and their performance requirements, can only be achieved using automation. As a general statement, these can be defined as those which exceed the capabilities of humans to perform them. In determining whether a function falls into this category the design team must consider the long-term demands of the task, required performance under the worst possible conditions and the variability of human operator. Performance factors which will need to be addressed include; required task rate, accuracy, repeatability, and in particular, the consequences of error.

Functions which exceed the capacity or capabilities of humans include;-

- processing large quantities of data
- those tasks requiring high accuracy (processing or manipulative)
- those tasks requiring high repeatability
- those tasks requiring rapid performance
- where the consequences of error are severe
- where errors cannot readily be retrieved (corrected)

Typical applications in a nuclear power plant for which automation will be necessary will include: reactor and plant protection systems, closed-loop automatic control, extended sequence control, data recording, analysis and archive. Depending on the particular task performance requirements, in all such cases it will be easy to demonstrate that one or more human capabilities would be exceeded if the resulting task was performed manually. A consequence of the decision to automate a function is that it will have to be described in sufficient detail to enable the necessary machine function to be defined. This will usually require extensive detail to be identified. A common failing of automatic systems is the lack of sufficient design detail, particularly to cover abnormal circumstances and fault operation. Such detail may be supplied informally by the system implementer without due consideration of the effects on system behaviour. In the absence of such detail in the design of automatic systems it is sometimes necessary for humans to take over when the automation fails, a task for which they may be ill-prepared and ill-equipped.

When deciding to automate a funtion, consideration must be given to supplementary tasks, such as maintenance and testing activities, which are required to allow the automation to perform its role. It is important that the benefits of automation are not lost by assigning supporting functions to human actions where the performance of the automatic system would be degraded due to poor maintainability. A typical example of this would be the maintenance and testing of reactor protection equipment. Until recently, this function was often assigned to operating staff with a consequent risk of errors which could degrade the system and cause reactor scrams. Developments in the design of computer-based systems have now made it possible to apply automatic testing to such systems, providing a higher degree of system availability and performance.

Functions Which Are Better Automated

Certain functions may be identified which, although lying within the capability of humans to perform , may be better assigned to machine. These include those which are lengthy, require high consistency, high accuracy or which involve a degree of risk to an operator. Tasks which would result in boredom or monotony for an operator also fall into this category. Progressive increases in the capability of technology means that automation can be considered for more and more functions. The cost of such technological solutions is often seen to be falling in relative terms and automation becomes an increasing possibility. The point at which automation is regarded by users as necessary or a normal expectation changes as societal and work-place values change.

An additional benefit of automation is the potential improvement which it can bring to the design of jobs and working conditions by changing the role humans play in technology based systems. With careful job design significant improvements in operator roles can be achieved and there may be consequential improvements in overall system performance. If care is not exercised, or if basic human factors principles are not adhered to, adverse problems can be created.

Practical examples of automation being introduced to replace tedious or arduous human activities include the use of machines to carry out maintenance or surveillance activities, e.g. steam generator examination, tube leak plugging, bolt tightening, etc. Automation is also increasingly being used to carry out lengthy, repetitive testing, such as that for safety and protection systems. Not only does this improve the role of the operator but it also bring improvements in the consistency of testing and may allow it to be carried out more frequently. As with any funtion which is intended to be assigned to a machine, a firm, detailed task specification will be required.

Functions Which Should Be Allocated to Humans

Functions which, due to their need for heuristic or inferential knowledge, requirement for flexibility, etc. will need to be assigned to humans. In addition, there may be practical or technical constraints which make automation impractical and thus require human operation. In many cases, it will be possible to justify assignment of such functions to the human. However, there is a risk that functions will be so assigned simply because automation would prove difficult or non-economical in some way. Regrettably, a function may be assigned to a human simply because there is a lack of a precise specification or difficulty in producing one. It may prove possible to produce a workable system in this way but there is a risk that the result produced is an unsuitable or inappropriate set of tasks for the human.

A particular set of functions which must currently be left with the human are those which occur in extreme fault or accident situations, where human flexibility and high-level skills are essential and the unexpected nature of the task makes specifying automation difficult or impossible.

Hypothesised Task Assignments

The process described will produce two lists of tasks; tasks which should be performed by humans and those which must be automated. Depending on the level of detailed analysis, within the two lists there will be tasks which are shared. A suitable notation should be used to identify these and cross-reference the two lists. These initial lists will form the basis for subsequent iterations. Iteration is necessary because many task assignment decisions will have an impact on other ones. To resolve such questions, it may be necessary to obtain highly specific and detailed information and this may only become available midway through the plant design phase. The approach taken to task allocation must recognise these problems by providing an ongoing, iterative vehicle for examining design decisions in a structured manner.

Since, in order to automate a task, we need precise task specifications and criteria, whilst conversely, humans are capable of dealing in a flexible way with loosely specified tasks, there will always be a risk that the allocation process will favour manual execution of difficult tasks, in order to produce earlier results. There may exist countering influences in the form of technological and social trends towards increased automation. The assigner of functions should remain true to the necessary principle of task allocation according to best matching of task and performer within the given context.

possible.

Evaluation of Function Assignments

Evaluation of the adequacy of function allocations prior to plant operation is necessary. Since nuclear power plant design tends to be evolutionary rather than revolutionary, there is much benefit in obtaining feedback from appropriate existing designs and practices. The designer should utilise experienced operating personnel in the allocation process, since they can bring direct operating experience to bear on the matter. However, their experience must relate to plant of a similar generation, and the designer must ensure the operators fully appreciate what he is seeking to achieve in terms of design objectives and the constraints which apply to the work. Unquestioned repetition of even well-proven approaches can lead to unsatisfactory or even unsafe systems if feedback data is used inappropriately. If an inadequate allocation solution is chosen, it may reveal itself during testing or operation of the plant through reduced output, increased downtime, increased human error and may possible carry a higher than desired risk to safety. Whatever the parameter, in such cases there will be incentives to achieve an improved balance and as a result, more effective plant operation.

Whilst 'desk-top' analysis will be useful in evaluating design proposals, there is a need to consider temporal factors. The time available to an operator to perform a task or series of tasks can influence his performance, possibly in a decisive way. To address this, some form of simulation may be necessary. Simple simulators such as mock-ups are of proven worth. If simple time elements can be incorporated, basic evaluation can be carried out. Part-task simulations may also be of benefit. Maximum benefit will be obtained from a full-scope, replica simulator, incorporating a credible man-machine interface. For large projects, experience indicates that the full-scope simulators made significant contribution to man-machine interface evaluations. If these can be made available prior to design-freeze on the real man-machine interface design extensive evaluation is possible and subsequent project risk is significantly reduced. In addition to using plant operators in the design process, a valuable contribution will be made by involving training staff who are a valuable source of knowledge, experience and expertise.

Operator Task Specifications

One of the outputs from the process described will be statements of tasks to be carried out by operating staff, including tasks which are shared between men and machines. This information must now be expressed in terms of task descriptions, job descriptions and staff requirements specifications. For practical application to control and monitoring of the plant at the detailed level, operating staff tasks will usually be expressed in the form of operating and maintenance procedures, operating rules, technical schedules, etc. Notwithstanding this, a definition of the role of each member of the operating staff should be produced, which clearly defines the operator's role and responsibilities in both the maintenance of safety and in achieving production goals. At this stage, a check should be made that there is no conflict between the various safety and production goals which have been defined and that the goal definitions which exist are complete and consistent. Where any potential conflict is identified this must be fully analysed and task specifications revised accordingly. If it is not possible to eradicate such potential conflicts, the operating staff must be provided with adequate guidance to resolve these during operation of the plant. It may not be possible or practical to pre-define all actions which are required to cover all operating modes of the plant and all operating eventualities. However, the operating staff should be adequately supported by procedures during all conditions of operation, including normal, fault and accident conditions.

Operating staff task specifications will also provide a basis on which to confirm information and control interface needs. Examination of the detailed task statements will enable information display content and form to be determined as well as types of input, selection and control devices. From this information and a consideration of the context in which a task or tasks are performed, it may be possible to identify where additional operator support systems or job aids are required. This information will need to be fed into the design process for the man-machine interface and supporting facilities.

o many as s

Specifying Automation

Specifications of the tasks to be carried by machine, the automation component of the system, will form a major input to the design of plant systems and associated protection, control and instrumentation. They may also influence the design of plant components themselves. It will not be possible to consider automation requirements in isolation from operator tasks, since inevitably there will be some human involvement in automatic systems, albeit in the form of supervision, surveillance or maintenance activities. The two sets of task specifications, those of the operating staff and those allocated to automation, must be considered together, and appropriate account taken of the many interactions that there will be between them.

Implications of the Assignment Process

Use of a well-balanced allocation process will optimise the contribution of both men and machines to overall system performance. In practice, a truly optimum balance may be difficult to achieve, due to lack of precise information or uncertainties and assumptions which have had to be made. If it is necessary to make compromises during the assignment process, as it undoubtedly is in many practical situations, the designer must, above all, ensure that safety objectives are met at all times and under all conditions of operation.

In such cases the designer should select a set of allocations which best accord with proven experience and practice. Whatever solution is adopted, the designer should ensure that the basis for that choice is documented and understood by all who will use that information in the course of their subsequent work.

The overall objective of the allocation process is to obtain a satisfactory balance between automation and human actions, not a perfect one. Often, it will be found that a number of possible allocation patterns will prove equally adequate to meet the specified system needs.Experience in member states shows that a balance can be obtained with a range of solutions. Very rarely will a single, unique result be indicated, particularly when maintenance activities are also taken into account. Neither will a common approach be justified across the whole of the plant activities being considered. This is particularly so when considering safety-related questions, where overall system reliability and performance will constrain many of the available possibilities.

At all times, the operating staff must fully understand which functions are delegated to them and which are being handled by automation. Where it is safe, possible and operationally desirable, the operating staff should be provided with means of controlling this allocation, through appropriate selection and control devices. It must be possible for the operating staff to readily assess the state of such allocations at all times through the process information system. Where the allocation can be varied by automatic actions, such as the protection systems, which may trip functions to a manual state, the information system must unambiguously draw the operator's attention to such changes.

Final Audit

The allocation process will provide a documented basis for decisions on allocation of functions and tasks between men and machines in a system. Notwithstanding the iterations described and the inherent checks and balances which will result, there will be merit in carrying out a final audit of the resulting system. In the case of a modification to an existing plant or process, the audit should consider both the changed portion and the modified process to ensure completeness of analysis.

The audit process should check the extent to which the original objectives have been met and document any significant departure, anomalies or conflicts which can be identified. Judgement on the adequacy of the final system must rest with the end users, provided that compliance with safety and performance standards can be adequately demonstrated. Final audit can form part of a wider review of facilities and provisions. Again, if the allocation process has been well-documented, audit will be greatly assisted.

Operational Feedback

It is important to regularly examine feedback from operating experience with the system and other related systems to ensure that the original balance remains valid and to identify any need for revisions to the original allocations if operating experience so indicates.

IAEA PUBLICATION

The proposed methodology is presented in an IAEA Technical Document entitled "Balance Between Automation and Human Actions in Nuclear Power Plant Operation".

The document identifies a short fall in existing design guidelines and standards and in response it proposes a pragmatic but systematic approach which may overcome the problem which have been identified with other approaches.

The ultimate worth of the document will depend upon its practical application by designers and researchers to realistic problems. Feedback and comments from users will enable the Agency and the authors to refine the proposal and will enable future issues of the document to be more tailored to user needs. Comments on the document are therefore freely invited.

The document contains a summation of contributions from IAEA Member States and covers many of the factors involved in achieving a balanced man-machine design. In addition to proposing a method, the document discusses wider considerations of automation, system performance, including the performance of both the human and machine components, together with man-machine interaction.

Some approaches to automation which have been adopted by Member States are described and the question of performance data collection is discussed. Selected biographic references are included.

CONCLUSIONS

Correct allocation of functions to men and machines in nuclear power plants is a key factor in succesful and safe design and operations. Previous research has identified methods of achieving allocations based on relative capabilites of the two components. These methods are often found in practice to be either too coarse or conversely, too complex. The paper discusses an allocation methodology which has been produced by an International group of workers in the field. The proposed methodology builds upon earlier research but adopts a pragmatic approach which takes account of the logical constraints found in practical situations and several influencing factors which shape the allocation process.

Several important conclusions can be drawn from the developments described:

1) Increase of technology produces an increasing need for plant complexity together with advances in sound allocation of function between man and machine in nuclear plant systems. Also safety considerations require a more assured understanding of how human perform in such systems, particularly in abnormal events.

2) In contrast to other areas of nuclear power plant design there is a lack of practical, structured guidance on allocation of functions. A systematic, auditable approach is essential. Adequate attention to this problem must be paid, at appropriate points in the design process.

3) The design team performing the allocation process must contain the correct mixture of skilled individuals, with experience of plant design, plant operations and human factors. The design team must be trained to be aware of the strengths and limitations of of humans in the plant operations environment.

4) Automation should be used to provide an extension of man's physical and mental capabilities. Tasks which are rigidly prescriptive,

tedious and stressful should be automated, but care must be taken that the resulting job descriptions are such that operator capabilities are fully and properly utilised.

5) In general, tasks which are assigned to automatic systems should not revert back to the operator when automation fails. Systems should be designed to fail gradually, so that operators are not required to suddenly assume control in areas where they may have had little practice or experience. If the machine is not capable of cost-effective, reliable, safe shutdown on failure, then such tasks should not be automated.

6) To achieve good results, there must be several cycles of task identification, allocation and evaluation of the total interface.

7) Representatives of the plant operations management must be a party to the evaluation phase and in so doing establish the job descriptions for the key operations staff.

8) The proof of the proposed method will lie in practical application in a realistic design or audit situation.

It may be concluded that the Agency's objectives in setting up the various international meetings and the subsequent working group have been largely met. International cooperation has resulted in a review of the current situation with regard to achieving a balance between automation and human actions in nuclear power plant operation. The work has indicated where improvements in design guidance are desirable and where further research would be of benefit. Proposals, in the form of a methodology, have been made which might form the basis of further development work.

<u>Author's Affiliations</u>

W. BASTL

Process Control Division
Gesellschaft für Reaktorsicherheit
(GRS) mbH
Forschungsgelände
D-8046 Garching
Federal Republic of Germany

Tel.: 089-32004-231 or 232
Telex: 5215110 GRS MD
Telefax: 089-32004-300

J. JENKINSON

Human Factors Group
Nuclear Electric plc
Barnett Way, Barnwood
Gloucester GL4 7RS
United Kingdom

Tel.: 452-652883
Telex: 43501
Telefax: 0452-652776

A. KOSSILOV

Division of Nuclear Power
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

Tel.: 2360-2796
Telex: 1-12645
Telefax: 1-234564

R. OLMSTEAD

Control Centre Development
CANDU Operations
Atomic Energy of Canada Limited
Sheridan Park Research Community
Mississauga, Ontario L5K 1B2
Canada

Tel.: 416 823 9040 ext.: 5024
Telex: 06-982372
Telefax: 416-823-6120

outstan ing an
after initial allocations have been made.

A. OUDIZ

Laboratoire d'Etudes
du Facteur Humain
Departement d'Analyse de Sureté-IPSN
Centre d'Etudes Nucléaires de
Fontenay aux Roses
Boite Postale 6
F-92260 Fontenay aux Roses
France

Tel.: 331 465 48074
Telex: 270049 SURIN
Telefax: 331 425 5266

B. SUN

Control & Diagnostics Program
Nuclear Power Division
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, CA 94303
U S A

Tel.: 415-855-2119
Telex: 82977 EPRI UR
Telefax: 415-855-1026 or 2954

REFERENCES

[1] Status Report on Assistance to Operators of Nuclear Power Plants in emergency Situations in Europe, CEC Joint Research Centre Ispra Report 1980, (4 Volumes).

[2] IEC Standard 964, Design for Control Rooms of Nuclear Power Plants.

[3] Fitts, P.M. et al., 'Human Engineering for an Effective Air Navigation and Control System, 1951, Washington, D.C., N.R.C.

[4] Edwards and Lees, Man and Computer in Process Control, 1972.

[5] Chapanis, A., Man-machine Engineering, 1965.

[6] Kantowitz and Sorkin (in Handbook of Human Factors, Ed. Salvendy), Wiley, 1987.

[7] A Methodology for Allocating Nuclear Power Plant Control Functions to Human or Automatic Control, Pulliam, R., Price, H.E., et al., NUREG/CR-3331, 1983.

[8] The Allocation of Functions in Man-Machine Systems: A Perspective and Literature Review, Price, H.E., Maisano, R.E., Van Cott, H.P., NUREG/CR-2623, 1982.

- where errors cannot readily be retrieved (corrected)

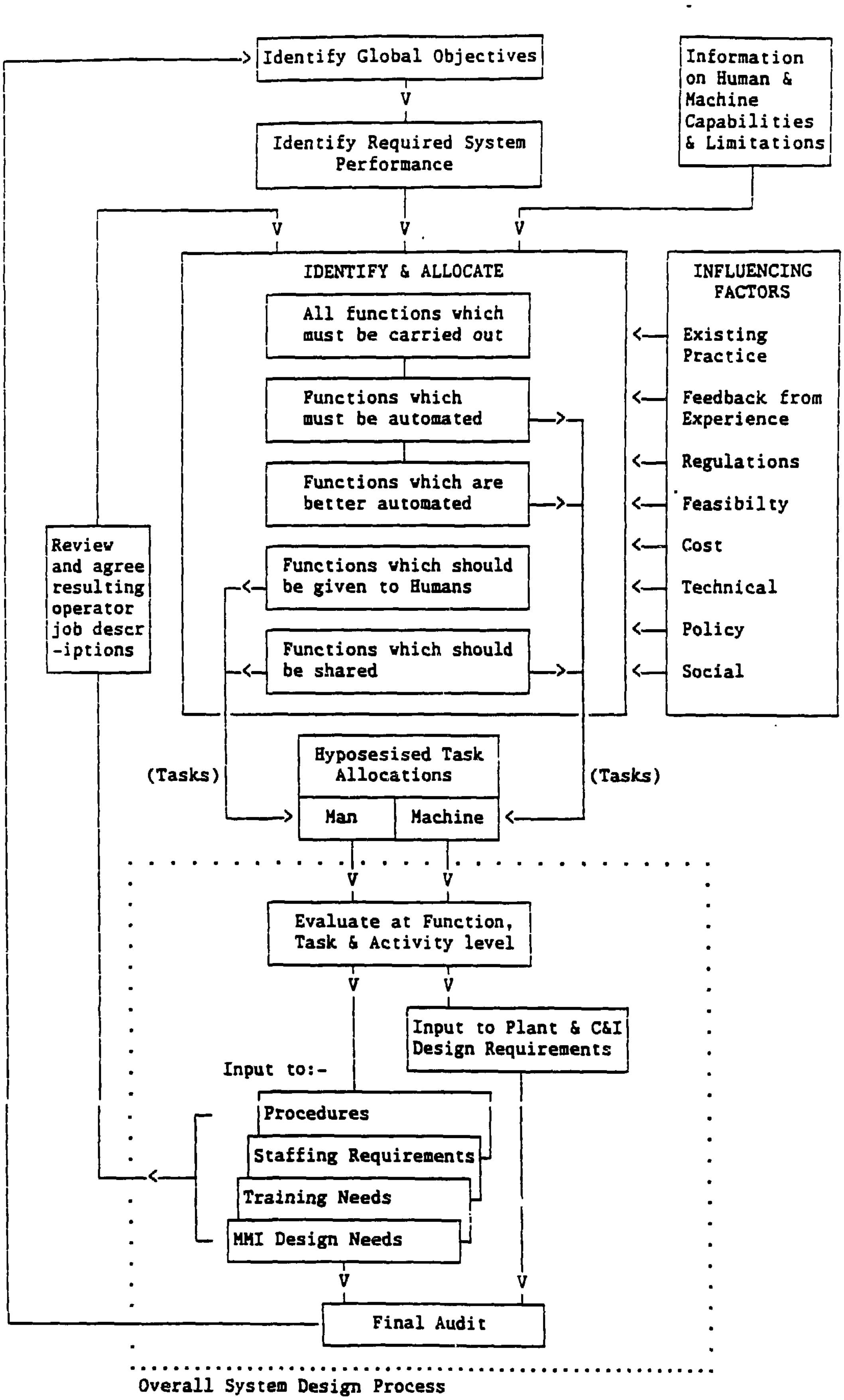

Figure 1, Allocation Methodology

which involve a degree of risk to an operator. Tasks which would result in

Octobre 1990

DESTINATAIRES

DIFFUSION CEA

M. Le Haut Commissaire
M. l'Inspecteur Général pour la Sûreté Nucléaire
DCS
DDSN
IPSN
OSSN : M. GUILLEMARD
DRSN : M. LIVOLANT
DAS/DIR
DERS Cadarache
SES Cadarache
SERE Cadarache
SESRU Cadarache
SRSC Valduc
SEMAR/FAR
SEMAR/Cadarache
DPS/FAR + DPS/DOC : Mme BEAU
DPT/FAR
CDSN/FAR : Mme PENNANEAC'H
DSMN/FAR
DRN Saclay
DRN/DER Cadarache
DRN/DEC Cadarache
DRN/DMT Saclay
DCC Saclay
DTA/Saclay
Service Documentation Saclay : Mme COTTON (3 ex.)
DERS/DOC Cadarache : Mme REY

DIFFUSION HORS CEA :

Le Secrétaire Général du Comité Interministériel de la Sécurité Nucléaire
Conseil Général des Mines : M. DE TORQUAT
Service Central de Sûreté des Installations Nucléaires : M. LAVERIE (3 ex.)
Service Central de Sûreté des Installations Nucléaires - FAR
Monsieur le Président du G.P.d. : M. GUILLAUMONT
Monsieur le Président du G.P.u. : M. MUXART
Direction Générale de l'Energie et des Matières Premières : M. LEVY
FRAMATOME : M. le Directeur Général
NOVATOME : M. le Directeur technique
TECHNICATOME : M. le Directeur Général
TECHNICATOME : Service Documentation
COGEMA : M. le Directeur de la Branche ENRICHISSEMENT
COGEMA : M. le Directeur de la Branche RETRAITEMENT
EDF : l'inspecteur général de la sûreté nucléaire : M. TANGUY
EDF/SEPTEN (2 ex.)
EDF/SPT
Société Générale pour les Techniques Nouvelles : M. JUSTIN
Mrs Marie-Aimée KHALIL : Vienna International Centre Library (2 ex.)
AIEA, Division de la Sûreté Nucléaire, Bureau d'Information sur la Sûreté :
- Mme Hulrike HERWIG
AEN/OCDE - Bibliothèque : Mme GODWIN
Bundes Ministerium für Umwelt, Naturschutz und Reaktorsicherheit - BONN (RFA) :
- M. HOHLEFELDER
- M. BREEST
Bundes Ministerium für Forschung und Technologie - BONN (RFA) : M. KREWER
Gesellschaft für Reaktorsicherheit - KOLN (RFA) :
- M. BIRKHOFER
- M. JAHNS

.../...

automation would prove difficult or non-economical in some way. Regrettably, a

Octobre 1990

U.S./N.R.C. - WASHINGTON (E.U.) :
- M. HAUBER
- USNRC, Attn : Library
Commission de Contrôle de l'Energie Atomique du Canada :
- M. LEVESQUE
- M. DIAMENSTEIN
Nuclear Installations Inspectorate - LONDON (G.B.) : M. J.S. MACLEOD
International Collaboration Branch UKAEA - Risley - WARRINGTON (G.B.) :
- M. J. BRAMMAN
Inspector for Nuclear Safety - WARRINGTON (G.B.) : M. J.G. TYROR
Consejo de Seguridad Nuclear - MADRID (ESPAGNE) :
- M. GONZALES
- M. JOSE DE CARLOS
Département de l'Environnement, Université d'Aveiro (PORTUGAL) : Dr C. BORREGO
Studsvik Energiteknik AB, Nuclear Division, Safety and System Analysis, NYKOPING (SUEDE) : M. E. HELLSTRAND
Direttore Centrale della Sicurezza Nucleara e della Protezione Sanitaria, ENEA, ROMA (ITALIE) : M. NASCHI
Direttore relazioni esterne e informazione, ENEA, ROMA (ITALIE) : M. P. VANNI
National Nuclear Safety Administration (CHINE) : M. LIN CHENGGE
Director of the Nuclear Electricity Office - CNNC (CHINE) : M. MA FUBANG
MITI (JAPON) : M. Hironori NAKANISHI
Science and Technology Agency, Director of the Nuclear Safety Bureau (JAPON) :
- M. KENICHI MURAKAMI
- M. HIROSHI HIROI
Center of Safety Research, JAERI (JAPON) : M. FUKETA
Secrétariat Général du Ministère de l'Energie et des Mines (MAROC) :
- M. Mohammed KARBID
- M. Abdelmajid CAOUI
I.V. Kurchatov Institute for Atomic Energy (MOSCOW):
- M. Nikolaï N. PONOMAREV-STEPNOI
USSR Academy of Science Institute of Nuclear Safety (MOSCOW):
- M. Leonid A. BOLSHOV

L'attaché près de l'Ambassade de France aux Etats-Unis : M. DE GALASSUS
L'attaché près de l'Ambassade de France en URSS : M. GOURDON
L'attaché "Energie" près de l'Ambassade de France en Corée : M. DURAND
L'attaché près de l'Ambassade de France au Japon : M. MORIETTE
Le Conseiller nucléaire auprès de l'Ambassade de France en Chine : M. LALERE

COPIE (SANS P.J.) :
SRDE
LEFH
BAIN
SASR
SACP
SAEP
SGNR
SAREP
SAPN
SASICC
SASLU
SASLU/VALRHO
SEC
SAET
SAED
STAS
SASC
SAEG
SAM
SPI

Le Conseiller nucléaire près de l'Ambassade de France en R.F.A. :
- M. GOURIEVIDIS