PROGRESS IN INSTRUMENTATION AND CONTROL INCLUDING THE MAN-MACHINE INTERFACE

B. WAHLSTRÖM
Technical Research Centre of Finland, VTT, Finland

T. PEDERSEN
ABB Atom, Västerås, Sweden

V. NEBOYAN
International Atomic Energy Agency, Vienna

Abstract

The paper discusses benefits and difficulties associated with the use of new digital instrumentation and control (I&C) systems for nuclear applications. The rapid development of information technology has not been used to the same extent in the nuclear industry as in conventional industries. The most important reason for this under-representation is a de-facto moratorium for construction of new plants. In old nuclear power plants (NPPs) the new technology is used in modernisation projects and valuable experience has been obtained. The licensing of programmable systems presents new challenges especially for safety systems where a very high integrity is required. The paper discusses various aspects related to the use of the new systems for nuclear applications, it gives references to ongoing work of international organisations and to research that is seen as an effort to solve problems related to implementation of the new systems for nuclear applications.

1 INTRODUCTION

The development in the fields of electronics, computers and software has been very rapid over the last two decades. New generations of equipment with improved performance have been introduced to the market at a very high rate. This development is also reflected in new and improved systems for instrumentation and control (I&C) in industrial plants as well as in power plants. The new systems take advantage of technological achievements to accommodate more sophisticated and efficient treatment of measurement and control signals, for high speed and reliability, but also for high flexibility and versatility.

The new technology has made its way into the major industries, including conventional power plants. The nuclear industry has been slow in its adoption, however, in spite of the advantages that the new technology can bring compared with systems currently installed at the operating nuclear power plants (NPPs). A likely reason for this under-representation is that only few new plants have been ordered during the eighties when the new I&C technology matured. Another reason is a lack of pressure to exchange the old systems with more modern ones. A third reason is the traditional conservatism within the nuclear industry with its calls for proven designs. The situation is now changing. Currently installed systems, which typically were designed in the late sixties and early seventies, are becoming obsolete and there is a need for functional upgrades. As a result modernisation efforts are underway in a large number of NPPs in the world.

For new reactor designs, which have been developed by various vendors, the use of the new technology is a rule rather than an exception. It may be assumed that new reactor projects will rely much more on utilisation of information technology than projects in the past. A vision for the future is that I&C design and implementation are integrated into a frame of plant information management in a plant life time perspective covering all aspects of instruments, cables, signal conditioning, control room, man-machine interfaces, control equipment, process computers and other real-time computers.

In IAEA(1999). Evolutionary water cooled reactors: Strategic issues, technologies and economic viability, IAEA-TECDOC-1117, International Atomic Energy Agency, Vienna.

2 DEVELOPMENT WITHIN INFORMATION TECHNOLOGY

2.1 Hardware

The development in electronics and computers has been tremendous during the last twenty years. The so-called Mores law predicts that the power of an electronics chip will double in 18 months, and this has come true over the whole period; computer hardware of today is four orders of magnitude more powerful than twenty years ago. The increased capability has be accompanied by a similar development also in hardware reliability and costs. As a result, the use of computers has expanded tremendously. In the fifties, people thought a handful computers would have enough computing power to solve all the computing problems of the world, but today computers are used everywhere, and even integrated in toys for children.

2.2 Software

Software has experienced a similar rapid development as the hardware. Some twenty years ago software systems could typically include a few thousands lines of code, while similar systems of today can contain millions of lines of code. Today, software systems of are built in several layers and new programming techniques have been introduced in a pursuit for better productivity in software projects. They are often characterised by overruns both in time schedules and costs, and techniques proposed have however not provided a remedy to this. A typical difficulty experienced in software projects is illustrated by the statement "whatever the size of the memory is, one would always need 50% more". New software issued typically contain bugs which often are only a nuisance, but sometimes also may have catastrophic impacts.

2.3 Networking

The development of information networks is closely connected to the development in hardware and software. From the early computers that were interconnected with 300 baud modem lines we are today speaking of communication at speeds of hundred megabits per second and in telecommunication technologies even more impressive performance is common. The development of networking has made it feasible to use distributed information processing where several computers communicate over a network. Computer networks may also be based on a large variety of media such as cables, optical fibres and wireless transmission. Networks make it possible to introduce systems redundancy in a simple way, but the network itself can be vulnerable for failures.

2.4 Implications for the systems

Rapid development is not always beneficial. A rapid introduction of new solutions tend to make earlier solutions obsolete and backwards compatibility of new systems is often poor. The degree of standardisation has been small and present systems often rely on de-facto standards that have developed from a market position. Many vendors have deliberately made their systems closed, resulting in interfacing difficulties between different systems. Spare parts for the systems are available only for a relatively short time. The driving mechanisms for modernising of computer systems is quite often not the functions themselves, but increasing problems in getting spares for obsolete computers. When the price for a new component in the old computer exceeds that of a new computer, an exchange becomes quite natural. The obsolescence has also a bearing to people since it may be difficult for an expert on one type of systems to be in a similar position only a few years later. Similarly it may be very difficult to find experts capable of fixing problems in the old systems.

2.5 Management of software design projects

The management of software design projects has become increasingly difficult with an increasing complexity of the systems. The project management methods created to remedy these problems have more been based on sound engineering practices and quality control, than on the use of specific tools. One important approach is to establish detailed specifications of the final system before starting the design. A development in modular steps, with a detailed testing in each step, is another important component of suc-

cessful design projects. A careful integration of the modules and testing of the whole system before its final release, makes it possible to avoid many problems in later phases of the life time of the software. After the release of a software system, a systematic collection of problem reports and modification management will be important. Documentation has an important role in all phases of a software design project.

3 IMPLICATIONS FOR I&C SYSTEMS

3.1 A transfer from analogue to digital

The use of computers for I&C systems has introduced a transfer from analogue to digital signal representations and the use of sampled data systems in the control loops. These changes have brought along new design requirements which to some extent have been put out of sight for the designers by the introduction of application programming languages. Compared with the mainly analogue systems, which were installed in the sixties and seventies, the new systems bring a number of benefits. The functions of the analogue systems were limited by both practical and economic constraints, while the new systems are far more flexible. Furthermore, the new systems have no drift and signal storage capacity is not limited by physical restrictions. It is also easy to reach a very high accuracy in various steps of computations, and signals do not need scaling. It is easy to duplicate signals between various applications, and the complexity of calculations is no hindrance in building them. A better functionality of a control room can be achieved by means of visual display units (VDU). Digital systems are more reliable than analogue systems, require less maintenance and they usually have a longer expected lifetime. Back-up functions can be built both on a component and system level making the solutions fault tolerant. Advanced diagnostics and self-checking features are also easily included.

3.2 Typical I&C systems

Digital I&C system typically consists of the following major components [1]:

- hardware,
- systems software,
- applications software,
- process interfaces,
- a communication network
- man-machine interfaces.

The hardware can be configured in many different ways to yield solutions that are both efficient and reliable. The software is often divided into systems and application software to make it easy to configure for different applications. The process interfaces contain analogue and binary inputs and outputs, and also specialised interfaces to process components such as pumps and valves. The communication network is used to exchange information between various nodes in the system. The man-machine interface is often arranged through specialised nodes by which various displays and control panels can be connected to the system. Controls for various purposes such as interlocks, automatics and control loops are sometimes located to separate units connected to the communication network, but more often they are integrated in nodes driving the process interface. Higher level control is sometimes integrated in the communications or man-machine interface nodes.

3.3 Complexity and unpredictability

Digital I&C systems are more unpredictable than analogue systems. This unpredictability is due to the complexity of the software and to the fact that a small change in inputs may result in a very large change in the outputs of the system. In practice this implies that it is not possible to use continuity arguments to predict in which range a certain output will be. The only way to predict the path that will be taken through some piece of software is to run it and observe the results. In practice it is very seldom possible to execute all possible paths of a certain piece of software, since these paths simply are too numer-

ous. Unpredictability is also introduced through the reliance on software tools such as assemblers, compilers, linkers, loaders, operating systems, etc. that also may contain various errors.

3.4 New functions included

The possibility of building complex functions in software-based systems to has been used in the modern digital I&C systems. Signals are represented directly in their engineering units, information can be stored for trend displays, advanced control algorithms can be utilised, alarm systems can include filtering, and various operator support systems can be built [2, 3]. Information can be duplicated to provide specialised displays for systems and plant states. It is possible to take an integrated approach towards information management and provide various personnel groups with the information they need. There are also possibilities to utilise new technology such as artificial intelligence, neural nets and fuzzy logic in an imitation of human reasoning.

3.5 Embedded systems

Another trend within I&C is to use computers embedded in various components. Various smart transmitters and intelligent valves and pumps are already used in the conventional industry, controlled by small computers embedded in the interface to the process component. The components can be connected to computer-based data concentrators through local communication buses and can be interfaced to local controls. Many systems such as access control, fire protection and ventilation system, which typically have not been a part of the I&C systems are now computerised and can easily be interfaced to the rest of the I&C. Computers are also used in stand-alone instruments used for various purposes. This provides a possibility to create special purpose interfaces, e.g. for communication between a calibrator and the calibrated component in exchanging messages of a successful calibration procedure.

3.6 Environmental compatibility

One specific concern related to new I&C systems is the environmental compatibility. The concern is raised through two mechanisms: on one hand modern electronic circuits are more sensitive to various disturbances; on the other hand they are using higher frequencies which may cause electromagnetic interference. Modern electronics is also more sensitive to environmental stress factors such as temperature, moisture and radiation. A remedy is to design robustness and to shield the components properly from various environmental impacts.

3.7 Commercial-off-the-shelf-systems

The nuclear power industry cannot be self contained with respect to its I&C solutions. Even if special nuclear grade systems are designed they will rely on electronics and software originally designed for other domains. In fact there is a trend to rely more and more on so called commercial-off-the-shelf systems (COTS). One can even say that a situation has emerged where one group of vendors are specialising on an integrating role and others on supplying components to be integrated into the systems. This specialisation gives a possibility for various vendors to concentrate on their core business, but it requires efficient communication between them to ensure that system requirements are appropriately reflected in the design of the COTS systems.

4 I&C APPLICATIONS IN NUCLEAR POWER PLANTS

4.1 General considerations

I&C system functions play an very important role in the operation and safety of NPPs. Proper initiating of safety functions depend on correct signalling and activation of various safety systems. The normal operations control has the task of preventing the plant state from moving into unsafe conditions. Correct and timely actions by the operators rely on correct and well presented information in the control room. In NPP applications, a distinction is made between safety systems, safety-relevant systems and non-safety-classed systems, and this yields a typical division into safety I&C, plant control systems and plant

classed systems, and this yields a typical division into safety I&C, plant control systems and plant information systems. The I&C for NPPs must be designed to meet the general safety principles such as defence-in-depth and the single failure criteria, and it must be possible to verify that the design criteria are fulfilled.

4.2 The new systems in NPP applications

The technological development in information technology and I&C will obviously influence also NPP projects. Until now this influence has been relatively minor. The most important reason for this is that very few new NPPs have been ordered during the last twenty years. Another reason is the safety requirements, which "prescribe" proven technology. The pace of development with very short-lived product generations has made it very difficult to establish a technology that can be considered proven. Another problem relates to the complexity of software-based systems which makes it difficult to generate the required evidence that the systems will perform correctly in all possible situations. One specific difficulty is that many of the I&C solutions have been created for the conventional industry, and the nuclear industry has had no or very little opportunity to bring in its own special concerns and requirements into the design process. One way for vendors to overcome this problem is to have two base system variations in which a subset of the software has been validated more extensively to meet requirements of a nuclear-grade system.

4.3 Modernisation projects

Operating NPPs are facing an increasing obsolescence of I&C systems and, at the same time requirements for improved competitiveness and safety [4]. Plants modernisation is a response to these changes in the environment. For the I&C systems, this covers a wide spectrum of approaches and strategies, ranging from ad hoc replacement of individual systems or functions to complete replacements, which in turn spans from one-to-one replacements, through an upgrading of old systems to an implementation of completely new systems. Experience from such projects e.g. in Finland, Germany, the Netherlands and Sweden shows that it is of paramount importance to establish a strategy for the remaining life-time of the plant. A choice has to be made between a gradual replacement of the old systems over a series of normal outages or a single extended shut down for a complete replacement of the old systems. Regardless of the selected strategy one has to plan for a certain co-existence of old and new systems. Modernisation projects may also require a regeneration of the plant design base in which new safety requirements should be reflected [5]. Implementation of new I&C systems may be attractive for new plants of a standard series. An example is the upgrades of the Korea Standard Nuclear Plant (KSNP) design for the Ulchin NPP Units 5 & 6 under construction. These upgrades involve introduction of new NSSS Control system duplication, Plant monitoring system, Digital plant protection system and Digital engineered safety features actuation system, and represent pilot cases with respect to licensing of such systems in Korea.

4.4 Two paths of systems development

Development of I&C systems for nuclear applications may follows two paths. One option is to build one-of-a-kind system very much from scratch, but relying on available assemblers, compilers, linkers and loaders. The other is to build on a well established I&C platform and implement system functions using an available application programming language. The first solution offers a possibility to gear the quality assurance to the special requirements of the nuclear industry, while the second solution provides the opportunity of having a far larger database of actual experience with the system. The first solution has the drawback that the experience with the system is minor, and problems of applying quality assurance to all parts of the software still exist. A problem with the second solution is that it may be impossible to gather necessary data for creating evidence that the system is good enough for its intended use.

4.5 Common-mode failures

Common-mode failures represent intrinsic difficulties for a design that aims at defence-in-depth; a coupling between redundant system that makes a common-mode failure possible, implies that the single failure criterion is not fulfilled. Common-mode failures can be avoided only if systems are truly independ-

ent. The potential for common-mode failures is much higher in software-based I&C than in analogue systems. Experience has shown that independence between software design projects is not sufficient, since specifications may contain errors that penetrate to the final code. Diversity is no solution to this problem, because the same type of electronic chips, the same compilers and the same thinking may have been used in creating the diverse systems. It has also been shown that an extensive base of experience from some applications does not necessarily ensure the reliability of the system in another application.

4.6 Verification and validation

The process of verification and validation (V&V) becomes crucial for the final quality of software-based systems. The complexity of the software makes it impractical to carry out the V&V process based only on testing of the final product. Instead the V&V process has to include inspection and review also of intermediate results and the processes behind them. In practice, this means that the V&V process should follow and have a close interaction with the design process. V&V can be facilitated by various tools by which the software can be checked automatically. One specific way of supporting the V&V process is to use formal specifications.

4.7 The main control room

The main control room requires special considerations in the design of a new I&C system [6]. The design of a computer-based control room is quite different from a conventional control room. One special consideration is to provide operators with an overview of the plant through the restricted window of a VDU. The allocation of control functions between the I&C and the control room operators is closely related to the level of automation. A high level of automation may ensure better repeatability and speed in the actions, but may leave the operator with tasks without a clear structure. Necessary information should be found easily in all operating situations, and in that context the structuring of information is important. Experience shows that it is highly recommended that the control room design be based on a detailed task analysis. Human factors engineering is another important aspect; various guidelines for performing control room design reviews are available [7].

4.8 Integrated plant information management

An integration of plant information is seen as a benefit from the new I&C systems. The information is functionally collected to a large database through one gate. Before information is entered into the database an extensive validation is made to ensure that the value of the signal is correct. If not the signal is marked unreliable. Information from the plant database can then be used anywhere without restrictions to place nor time. Interfaces will be arranged between the plant database and various applications. The configuration management can be supported by interfaces to design, work order and maintenance systems. Control room operators and maintenance personnel can be supported by providing interfaces to the document management system. The creation and maintaining of PSAs can be supported by interfaces to the configuration management and the maintenance systems, etc. The main difficulty in the creation of such an integrated plant data base is the establishment of standardised and open interfaces to which various vendors can interface their own systems.

4.9 Information management in a plant life-time perspective

The problem of information management can be extended to the whole plant life-time. An extensive use of computers during design and construction implies a computerised design base. This gives extended possibilities to use computerised tools in the V&V process. Reuse of specifications generated for one purpose as input for configuring software for an other application represent interesting new possibilities. Code and document generation can also be assumed to be relatively standard applications in future NPP projects. Possibilities of remote diagnosing and fault finding are already in use today. If suitable efforts are made to find invariants in the design of I&C systems it may also be possible to reuse the system specifications for other hard- and software platforms. Modern telecommunication provides an opportunity for co-operation between design teams separated by large geographical distances.

5 THE LICENSING PROCESS

5.1 Requirements for licensiability

The requirements depend on the safety importance of the system to be licensed, or qualified. Requirements may be placed even on non-safety systems when they are interfaced to safety or safety-related systems. With respect to requirements applicable to I&C systems we can separate between deterministic, probabilistic and human factors requirements. Due to the complexity of an I&C design process it is necessary to define requirements on the final product, intermediate products and the processes used to generate these products. Deterministic requirements are usually placed on solutions with limited design complexity, solutions for fault tolerance, spare capacity and quality control processes. Probabilistic requirements are often established to ensure that assumptions made in the PSA are valid both with respect to sequence modelling and reliability estimates. Human factor requirements are formulated to ensure that operators will be able to understand and operate the systems and that the first rapid state changes after the onset of an accident are automated. Requirements are also placed on the process of generating evidence that the licensing requirements are fulfilled.

5.2 Phases in the licensing process

The phases in a licensing process depend on legislation and regulatory practices. Early interaction between utility and regulator can be helpful. Typically, system architecture and design principles set the stage. Already at this phase, the regulator may require a V&V plan with descriptions of major project milestones and the quality systems to be used in the project. An assessment of specifications is often the next step in process. When testing is initiated, it is usual to require a comprehensive test plan. This includes both factory and site acceptance testing, which often are carried out in the presence of a representative of the regulator. A modern software quality control system includes several design reviews to be carried out when certain stages in the design have been completed. Some of these reviews may be performed by independent reviewers to ensure that also difficult questions can be brought into the open. If the software development process relies on the use of various tools such as code and documentation generators it may be necessary to license them in a separate process.

5.3 Collection of evidence

Typical software quality assurance procedures monitor process compliance more than direct product quality. The structure and implementation of these procedures represent one component in the compilation of evidence. Various intermediate products can also be assessed and reviewed in the course of the design project. Inspections of specifications, documentation and code can provide evidence that the underlying processes have been producing required quality. Special V&V tools such as machine code disassemblers, automated tools for inspection of assembly programs, tools for static and dynamic analyses of the software, etc. may be used to get evidence that the coding has been performed according to standards. The completeness of test programs can be assessed using various tools for instance to investigate sensitivity to artificial errors in the code. Statistical testing, either with random test inputs or inputs mimicking a certain usage profile can be used to collect quantitative evidence for the reliability of the software. Operational experience can provide some evidence, but the problem is to prove that the usage profiles of two different applications are similar enough.

5.4 Conditions for acceptability

To make the licensing process transparent it is important to have the conditions for accepting or rejecting certain solutions documented in a clear way. Regulatory requirements are not stable over time, because new experience may bring in needs for stricter acceptability criteria. Still, it is necessary to maintain consistency in the regulatory approaches. The safety importance for functions and components are reflected in the safety classification, but this is usually too crude to give clear guidance on the acceptability. Deterministic requirements can be checked by inspections, but the probabilistic requirements are more difficult. One possibility is to anchor acceptability conditions to a plant specific PSA where a certain reliability is required. Statistical testing can be used to collect evidence at some reliability level, but it be-

comes impractical for systems with a very high reliability requirement. For such systems it may not be possible to provide reliability estimates without relying on expert judgement. It is often beneficial to model software errors using some method like the Failure Modes and Effects Analysis (FMEA). A controversial issue in this context is requirements for diversity, since it can be very hard to verify the actual degree of independence.

5.5 Experience from licensing processes

Experience from software licensing has been obtained in Canada from the Darlington plant, in France from the so-called SPIN system and the N4 plants, in the United States from several upgrades of plant protection systems and in the UK from Sizewell B. Based on this experience the four regulators in Canada, France, USA and UK came together and developed their consensus on what should be included in the licensing process [8]. In Germany, the Siemens Teleperm XS system has recently been licensed in an extensive process involving several parties [9].

5.6 The Finnish YVL guides

One example of new licensing requirements for I&C is available in Finland. According to the Finnish regulatory system STUK issues detailed safety requirements. These requirements, the so-called YVL guides, govern the practical safety activities at the nuclear installations and the safety inspections carried out by STUK. The guides are updated regularly and presently some sixty plus guides are maintained. The guides are not mandatory, but represent a strong regulatory position. One of the guides, the YVL-5.5 on "Nuclear power plant automation systems and equipment" has recently gone through an extensive revision and the new document is now (11/98) almost finalised. The revision process was initiated by the need to issue detailed requirements on programmable automation systems. The main difficulty in writing the guide has been to find a proper balance in the details of the requirements. The guide should be consistent with other guides, but the burden of proof should not restrain a transfer from technically inferior solutions. The Finnish regulatory practice requires a pre-inspection of relevant documentation before a project is released for implementation. For programmable automation systems this review can be performed in two phases, where general design criteria and solutions in principle are covered in the first phase. In the second phase, detailed information on the selected systems and the design should be provided together with the V&V plan. Before the installation, STUK also reviews acceptance tests, inspects the installation and monitors the start up of the systems at the plant.

6 NEW PLANT DESIGNS

6.1 Development by reactor vendors in the world

All reactor vendors have prepared themselves for a move to new I&C systems. Many vendors have been involved in plant modernisation projects that have given them experience in the utilisation of the new systems. For new reactor concepts, the development of I&C systems has been on a more generic level. This is quite natural since final solutions will depend on the availability of specific systems at the time of construction. The new reactor designs generally fall into two categories: designs of evolutionary type and designs requiring substantial development [10]. The evolutionary designs will, to a large extent be configured and laid out in the same way as their forerunners, while the "developmental" types may incorporate significant conceptual changes, e.g. aimed at eliminating safety hazards and improving safety performance. The I&C solutions for the two categories do not differ very much, however. They are based on the same kind of digital distributed I&C systems and the control room is suggested to be compact and based on VDUs. The only difference between the two reactor designs categories is that some simplifications with respect to redundancy and physical independence are suggested for the "developmental" designs.

6.2 Similarities and differences in I&C solutions

When the I&C solutions proposed by various reactor vendors for their designs are compared, the differences are quite small. All reactor vendors move towards distributed digital systems. The control

rooms are based on computers and VDUs. The level of automation is relatively high. Most of the evolutionary reactor concepts rely on a 2/4 redundancy principle. The development work of the Korean industry on the Korean Next Generation Reactor (KNGR) based on the System 80+ of ABB Combustion Engineering can be taken as a typical example. The main control room is a compact work station design that implements the utility requirements of the EPRI URD, featuring three redundant operator consoles, a separate safety console, a Large Display Panel, and monitoring consoles for the supervisor and technical advisor of the shift. The man-machine interface is based on computerised operating procedures and soft controls, and the I&C design is a complete plant-wide integration of digital technology. The Plant Protection and Safety Component Control System are four-channel, programmable logic controller-based systems. Non-safety controls are implemented in a two-channel system using diverse processors; plant monitoring is also provided by two independent and diverse systems.

7 RESEARCH ACTIVITIES

7.1 National research activities

All nuclear countries have various research activities going on. The activities can be divided into two parts: the more or less public research, and research driven by the nuclear vendors. The way these activities are organised depends on the country. In the USA, U.S.NRC and EPRI are funding and coordinating much of the activities. In France, IPSN is performing a large amount of the regulatory research. In Finland, VTT carries out research projects for both the utilities and the national regulator.

7.2 A report on licensing of I&C systems

The U.S.NRC, the regulatory body in the USA, has experienced various problems in their approaches to the new systems. In an attempt to get outside guidance the National Research Council was asked to conduct a study on application of digital I&C technology to commercial NPP operations. The study was carried out in two phases in which the first identified important safety and reliability issues arising from the introduction of the new technology. In phase two the committee was asked to identify criteria for review and acceptance of digital I&C technology both in retrofitted and new reactors. In areas lacking sufficient scientific basis the committee was asked to suggest ways in which U.S.NRC could acquire the required information. The work of the committee resulted in a comprehensive report where many important issues were brought up and discussed [11].

7.3 The OECD Halden Reactor Project

The Halden Project is an undertaking of national organisations in 20 countries sponsoring a jointly financed programme under the auspices of OECD/NEA. Discussions are under way for enlarging the member circle. Collaborations with East-European countries in support of plant safety and reliability are also expanding. The programmes aim at generating key information for safety and licensing assessments on extended fuel utilisation, degradation of core materials and man-machine interactions research. The activities in the man-machine area are highly relevant for the I&C solutions and they include a new man-machine research laboratory, plant surveillance and operations systems, assessments of system quality and several projects on software verification and validation.

7.4 Research needs

Research needs can be divided into two areas licensing of programmable systems and human factors. For important safety systems there is a need in probabilistic terms is to go beyond a reliability of 10^{-3} per demand and this requirement is very hard to reach [12]. One important portion of the methods for V&V of software is the formal methods and one important research task is to collect evidence on their efficiency. In the human factors area human reliability, cognitive errors and team work are important subjects for research.

8 INTERNATIONAL CO-OPERATION

8.1 IAEA

In 1974, the IAEA launched the Nuclear Safety Standards (NUSS) programme for the purpose of establishing internationally agreed safety standards for nuclear power reactors. The resulting codes and guides were published in the IAEA Safety Series. Now the hierarchical structure for the Safety Series publications is Fundamentals, Requirements, and Guides. The activities related to I&C are located within the departments of Nuclear Power and Nuclear Safety. The I&C activities of the Department of Nuclear Power are co-ordinated through the International Working Group on Nuclear Power Plant Control and Instrumentation (IWG-NPPCI). Recent activities of IWG-NPPCI include the preparation of technical documents, specialists meetings and co-ordinated research programmes. An activity to identify IAEA publications in need of updating to reflect the new I&C systems has been initiated.

8.2 OECD/NEA

The Nuclear Energy Agency (NEA) of OECD is involved in I&C issues through activities within the Committee on Safety of Nuclear Installations (CSNI) and the Committee on Nuclear Regulatory Activities (CNRA). An International Workshop on the Technical Issues of Computer-Based Systems Important to Safety was arranged in March 1996 in Munich [13]. This workshop included several presentations on the state-of-the-art in the licensing of software-based systems. Within CSNI the Principal Working Group #1, on Operating Experience and Human Factors, has established a Task Group that has the objective to establish and develop a database on operational experience with Computer-Based Systems Important to Safety in NPPs [14]. OECD/NEA has also in a Senior Group of Experts on Safety Research (SESAR) identified research strategies and needs and in this work among other issues addressed Plant Control and Monitoring and Human Factors which are relevant within the I&C field.

8.3 The European Union

During 1994-98, research and technical development activities have been carried out under the Fourth Framework Programme and the parallel Euratom framework programme that covers research and activities in the nuclear sector. The Programme is implemented through 18 specific thematic programmes grouped under four priority areas. The total budget for the Programme has been more than 13 billion ECUs. Within the programme various projects related to nuclear power and I&C have been financed. A continuation of earlier programmes is proposed in the Fifth Framework Programme. The Programme itself has not yet been adopted, but in-depth discussions have been started on specific themes to be implemented from 1999 onwards. Also this programme is expected to contain activities related to nuclear power and I&C. In addition to these research-oriented activities, the European Commission sponsors various working groups that take a stand on important issues. One of these the Nuclear Regulator Working Group (NRWG), has prepared a Document on Regulators' Current Requirements and Practices, which discusses licensing of programmable systems.

8.4 Standardisation organisations

Many organisations prepare standards relevant for I&C in NPPs. The most important of these international standardisation organisations are IEC and ISO. IEC, the International Electrotechnical Commission, is an organisation of 50 countries involved in standardisation in the fields of electricity, electronics and related technologies. ISO, the International Organization for Standardization is a world-wide federation of national standards bodies from some 100 countries writes other standards. Most international standards are written by working groups that comprise technical experts from different countries. The experts are appointed by countries, but serve as individuals, and the expert's action in the group is not necessarily reflecting national positions. The working group draft may be approved as a draft standard, and can after that be accepted as an international standard, through voting by the official delegates of the IEC and ISO member countries. In addition IEEE, the Institute of Electrical and Electronic Engineers, is another important standardisation organisation working mainly in the USA. Some important standards for I&C in NPPs are IEC-880, ISO 9000, ISO 9000-3, IEEE 730, IEEE 1012, and IEEE7-4.3.2-1993.

8.5 Utility requirements

Utilities both in Europe and the USA have initiated work aimed at creating common utility requirements for new plants to be built. One rationale in the work has been to establish a common approach that could ease the licensing process. Another benefit of the work process is that it may help harmonising of views on crucial safety issues.

9 CONCLUSIONS

In assessing the overall situation it is evident that distributed digital systems are the only realistic I&C alternative for both modernisation and new NPP projects. The licensing issue of the new systems has not been completely resolved, however. A resolution would imply estimating in some believable way the reliability of a system containing both hardware and software. Before this can be accomplished, further research efforts are needed.

At present, the majority of concrete projects are I&C modernisations in operating NPPs. A major difficulty in these projects arises from the design constraints given by the actual layout and process configuration; this means that the full benefit of the new information technology remains to be realised in an NPP project. Among the modernisation projects, some have been relatively successful and others less successful. Some of the difficulties go back to the problems described in this paper.

With respect to I&C, the nuclear industry has to rely on solutions developed for other industries. This is necessary, to have a large enough experience database accumulated in the use of the systems. On the other hand, the nuclear industry obviously has some very special requirements with regard to the validation of selected solutions. In the development of new systems, these requirement may be reflected to some extent if arguments are presented in a convincing way and at the right moment. One problem in which the nuclear industry has to invest a considerable amount of thinking, concerns the adaptation of the rapid information technology development to the very long NPP lifetime. The nuclear industry would need a number of new plant projects to accomplish full utilisation the opportunities inherent in the new I&C systems.

10 REFERENCES

[1] IAEA (1997). Advanced control systems to improve nuclear power plant reliability and efficiency, TECDOC-952, International Atomic Energy, Vienna, July 1997.

[2] IAEA (1994). Operator support systems in nuclear power plants, TECDOC-762, International Atomic Energy, Vienna, September 1994.

[3] IAEA (1996). Computerized support systems in nuclear power plants, TECDOC-912, International Atomic Energy, Vienna, October 1996.

[4] IAEA (1998). Modernization of instrumentation and control in nuclear power plants, TECDOC-1016, International Atomic Energy, Vienna, May 1998.

[5] IAEA (1995). A common basis for judging the safety of nuclear power plants built to earlier standards, INSAG-8, International Atomic Energy Agency, Vienna.

[6] IAEA (1995). Control room systems design for nuclear power plants, TECDOC-812, International Atomic Energy, Vienna, July 1995.

[7] USNRC (1996). Human-system interface design review guideline, NUREG-0700, Rev.1, Vols. 1-3, Process and guidelines, Reviewer's checklist, Review software and user's guide, US Nuclear Regulatory Commission, Washington DC.

[8] AECB, DSIN/IPSN, NII, USNRC (1997). Four party regulatory consensus report on the safety case for computer-based systems in nuclear power plants, Health & Safety Executive, UK.

[9] IAEA Specialists' meeting on “Design and Assessment of Instrumentation and Control Systems in NPP; Coping with Rapid Technological Change”, 6 to 9 October 1998, Garching, Germany.

[10] IAEA (1997). Terms for describing new, advanced nuclear power plants, TECDOC-936, International Atomic Energy, Vienna, April 1997.

[11] NRC (1997). Committee on application of digital instrumentation and control in nuclear power plant operations. Safety and reliability issues, Final Report, National Research Council, Washington DC.

[12] U. Pulkkinen (1997). Programmable automation systems in PSA, Finnish Centre for Radiation and Nuclear Safety, STUK-YTO-TR 127, June.

[13] OECD/NEA (1997). Licensing of computer-based systems important to safety, Committee on Nuclear Regulatory Activities, NEA/CNRA/R(97)2, OECD Nuclear Energy Agency, OCDE/GD(97)90 and OCDE/GD(97)91.

[14] OECD/NEA (1998). Operating and maintenance experience with computer-based systems in nuclear power plants; a report by the PWG-1 Task Group on Computer-Based Systems, Committee on the Safety of Nuclear Installations, NEA/CSNI/R(97)23, OECD Nuclear Energy Agency.