An expansion of the training programmes is a natural result of the increased number of replica simulators available. The basic training will become more detailed and differentiated. The turbine operators will also receive more specific in-depth training on the turbine system and functions, at the expense of reduced reactor training. The retraining programme might also be changed toward more frequent training and reduced course time.

The retraining of a shift group or individual operators, which is required after a longer period away from control room work (leisure, illness, etc.), is presently met by a 3-4 hours talk-through session. This is generally not considered to give adequate up-dating. The use of simulators for that purpose would be an efficient way of refreshing the operators know-how, but the replica simulators are located too far from the stations, and the Compact Simulators are not yet adapted adequately to that need.

The Compact Simulators are being continuously developed to a higher degree of detail and flexibility. But there always seems to be a lag between the potential utilisation and the actual use of the simulators. The preparatory work required by the instructors appears to be a drag.

An expanded training programme for the maintenance staff is a recent requirement set by the safety authorities. Training on the Compact Simulators gives a useful contribution to this training programme, as changes of important parameters can be introduced easily and their consequences followed in transient studies.

NUCLEAR POWER PLANT CONTROL AND INSTRUMENTATION ACTIVITIES IN THE UNITED KINGDOM

A. GOODINGS
Atomic Energy Establishment Winfrith,
United Kingdom Atomic Energy Authority,
Dorchester, Dorset,
United Kingdom

Abstract

The paper describes the status of the NPP control and instrumentation in the United Kingdom. The general technology underlying most aspects of power reactor C&I in the UK has not altered since the last progress report although there have been many improvements in detail. In one field, however, that of computer applications, the change has almost been one of kind rather than degree.

The following fields are briefly described:

- the status of nuclear power in the UK,
- the development of sensors,
- the development of electronic equipment,
- signal processing - information technology,
- quality assurance and the validation and verification of software,
- expert systems,
- training simulators.

1. INTRODUCTION

The general technology underlying most aspects of power reactor C&I in the UK has not altered since the last progress report although there have been many improvements in detail. In one field, however, that of computer applications, the change has almost been one of kind rather than degree.

This paper cannot report progress on individual items but tries to cover the field as a whole with comment on the salient areas and on difficulties which have been encountered. The author is indebted to many colleagues for the information on which these comments are based but it is important to emphasise that they represent his own personal views and should not be taken in any way as a United Kingdom consensus.

2. THE STATUS OF NUCLEAR POWER IN THE UK

Nuclear power in Britain must be seen against the background of a large, well-established coal mining industry and the discovery of North Sea Oil. The commercial exploitation of nuclear power took place early but it contributes only about 20% of total electricity generation. Ten Magnox reactors were commissioned between 1962 and 1969 and between them represent a generating capacity of about 5,000 MWe but some are approaching the end of their economic lives and decommissioning has already started at Berkeley in Gloucestershire. The second phase of the UK Nuclear Power Programme used Advanced Gas-Cooled Reactors and there are, in effect, 7 of these Stations each comprising 2 reactors (a total of 8,588 MWe). The most recent are those at Torness and Heysham II which are now at design power after a relatively trouble-free commissioning period.

A decision was taken several years ago to switch from Gas-Cooled Reactors to PWRs and, following a long Public Enquiry, approval was obtained to build such a Station at Sizewell in Suffolk. This is now under construction and the Electricity Industry has expressed an intention to build a total of 4 PWR Stations in the current phase. A Public Enquiry for the one at Hinkley is in progress.

The Government intends to privatise the Electricity Industry and the effect of this on nuclear power in Britain is unclear. The Generation Companies will be obliged to generate a certain percentage of electricity by non-fossil means but will be free to choose their techniques and how this is done will depend on commercial decisions. The Government are strongly in favour of nuclear power but believe that R&D should be funded by the Industry and central funding for R&D has been drastically reduced. More and more of the work in, for example, the Atomic Energy Authority is therefore being backed by the Generating Boards or British Nuclear Fuels plc. but this, too, now depends on the outcome of privatisation. For example, of the £100M spent on Fast Reactor R&D and PFR operations in 1988, £30M was provided by the Generating Board who have said that, when privatised, they will not continue with this work.

3. THE DEVELOPMENT OF SENSORS

In general terms, conventional sensors are basically unchanged and there has been no widespread introduction of new technology such as, for example, light guide techniques. The development of nucleonic sensors has been dominated by the AGR and Fast Reactor programmes and has therefore continued to concentrate on operation at high temperatures and pressures.

The Heysham 2 and Torness stations have continued to use the DC12 gamma compensated wide range chamber and the DC14 fission chamber. Very large numbers of these designs have now been produced. They have established their reliability and it has only been necessary to consolidate production methods.

Diversification, however, led to a need for a wide range, combined pulse and current fluctuation system and a new chamber, called the P8, has consequently been developed. It was based on the long-established P7 to take advantage of its proven reliability but uses a new, laminated, mineral-insulated cable with special termination arrangements and a very low surface transfer impedance derived from superscreening techniques. This was necessary because current fluctuation systems work at centre frequencies of order 100 kHz and are particularly vulnerable to electrical interference under plant conditions. The opportunity was also taken to improve the electron collection time by a factor of about 3 to increase gamma rejection in the pulse mode. About 40 of these chambers have now been made with virtually 100% yield and are operating on site.

As would be expected on AGRs, interest in high reliability thermocouples has continued

4. THE DEVELOPMENT OF ELECTRONIC EQUIPMENT

Modern hardware is, of course, totally committed to transistors and integrated circuits but techniques such as surface mounting technology are not widely employed in dedicated equipments. Reliability is high and this, interestingly, is leading to skill availability difficulties in the maintenance field. These problems are exacerbated by the fact that younger staff tend to specialise in digital techniques and the underlying trend towards digitisation both within instruments and over the system as a whole is therefore being reinforced. However, much analogue equipment remains and the maintenance problems may well increase.

Digital techniques lend themselves to self-checking and applications of condition monitoring are increasing because of the cost of manual testing. This is influencing maintenance scheduling arguments and there is now a tendency not to visit plant on a fixed time basis.

5. SIGNAL PROCESSING - INFORMATION TECHNOLOGY

5.1 The new AGRs

The use of computing systems for on-line functions on UK power reactors is now perhaps 25 years old. In the past, extensive facilities were provided for data display and for logging functions and at that time the computing power required was often close to the limits of what was commercially available. These restrictions should have diminished with the introduction of modern computers but the applications have also increased to the extent that all of the UK AGRs (except Hunterston 'B') are now fitted with full, closed loop computer control, two of them having extensive automatic start-up features. Heysham 2 and Torness also have installed computer equipment which sequences the electrical loads after trip, to a degree, computing capacity is still a limiting factor.

The design intent for the two new stations was to repeat the successful Hinkley 'B' and Hunterston 'B' systems and an overall design objective was to limit changes to those necessary for safety or performance reasons. This argument could not, however be enforced in the C&I area because of the obsolescence of much of the original equipment. The hardware at Hinkley and Hunterston was designed in the late 1960s and early 1970s and between that time and 1982, when contracts were placed for the new stations, technology had advanced dramatically.

A number of other factors also increased computing needs and their importance:

(a) The C&I system was much larger than before. Segregation requirements had introduced many more cables, and seismic specifications demanded increased redundancy. More stringent licensing requirements increased the quantity of safety related plant (it has already been said that diverse nucleonic systems were required and this is also true in relation to the post trip cooling and waste handling systems) and there was also provision for more extensive monitoring to assist the operators, ensuring that the plant remains within design safety limits. An example of this is the seismic monitoring system. Furthermore, extra provisions were made to improve operational availability and these included more transducers on the plant and more extensive computer based systems for recording and analysis

(b) Requirements were also more complex with greatly increased inter-relation between signals. This arose partly from operational experience. In order to reduce the number of men in local plant areas, there was greater emphasis on centralised monitoring and control. This complexity was increased by the increased use of microprocessor-based instrumentation systems which offer advantages in cost and flexibility at the expense of increased communication.

(c) The contract strategies were also different. The first Stations were built under comprehensive contracts in which the same people were responsible for equipment and its instrumentation. On Heysham 2 & Torness however, the National Nuclear Corporation were responsible for particular plant areas whilst the generating boards retained responsibility for the rest. This demanded very precise definitions for the C&I because C&I systems tend not to follow the mechanical plant boundaries.

More details can be found in the literature [1] and it should be noted that the new reactor systems include reactor management packages with real time simulation to assist the operators. It is also worth noting that a programme is now in hand to replace the main data processing systems on the older AGR's. It follows extensive prototype, on-site trials and attempts to rationalise distinctions between safety and non-safety data.

5.2 The PWR at Sizewell 'B'

The main features of the C&I design for the Sizewell 'B' PWR are now fully worked out, contracts for reactor protection and associated instrumentation, process C&I and for the Integrated System for Centralised Operation (ISCO) have been placed. Site delivery and installation of these systems is targeted from the middle of 1990 to late 1991.

The C&I design integrates the Main Control Room (MCR) and Auxiliary Shutdown Room (ASR) with the Station Data Processing System (DPS). Multiplexed control is employed and has major advantages due to its inherent fail-to-safe characteristics in any potential Station fire. It also reduces cable costs and the time for cable installation.

The reactor protection system comprises 4 fully separated sub-systems with full parameter voting on a 2 out of 4 basis. It follows the basic approach which has prevailed for UK reactors for over 20 years and has 2 separate, diverse protection channels. These are the Primary Protection System (PPS) and the Secondary Protection System (SPS) and they operate from diverse parameters wherever practicable for all the more frequent faults of the Station design basis. The PPS also provides protection, generally using 2 parameters, for all the less frequent faults of the Station design basis. 4 trains of the essential plant needed to achieve hot shutdown are provided and 2 trains of plant are provided for mitigation of the low frequency potential faults of the Station's design basis (below 10^{-3}) per year.

The PPS design is based on microprocessors, and very careful attention is therefore being paid to the computer software of the system. This software is produced in accordance with the requirements of IEC 880 and the total design is being independently assessed for integrity using guidelines established for microprocessor systems for reactor protection duty. The SPS design is totally independent of microprocessors, and uses the range of fail-safe modules based on the "Laddic" magnetic logic module developed for earlier UK Stations.

The ISCO equipment uses 16 independent Station Data Network branches (SDNs), each SDN being internally redundant. They multiplex MCR and ASR controls and indications and operate input/output multiplexing cubicles in plant switchgear rooms. MCR switches are scanned by the multiplexer and switch status is checked by microprocessor logic, which then causes a message to be sent to the correct input/output multiplexer for switchgear or plant. The state of plant and measured values are similarly multiplexed and may be displayed on the control panels. Station closed-loop automatic control is performed by the computing equipment of the SDN branches, using appropriate algorithms. The allocation of the loop functions between different SDN branches protects against simultaneous failure of several control functions.

Four separate SDN branches are used to provide a safety classified Safety Information Display System. This receives the values of all PPS parameters plus some other parameters and provides the displays needed for monitoring safe shutdown. The ISCO equipment also includes the Station DPS, which receives data from the SDN branches. Separate DPS sub-systems are used for the reactor, the turbine and the electrical sections of the total Station plant. Each sub-system provides VDU displays for the MCR, and feeds information to a central "global" DPS and to a DPS for the separate technical support centre.

Criteria have been established for the maximum reliability which may be claimed for software-based systems. This is limited by the potential effect of common mode failures and to cater for this, a limited number of overview indicators and alarms and of controls for the Engineered Safety Features (via the PPS and SPS) have been provided in the MCR. As on past AGR Stations, a full-scale simulator of the MCR is being constructed. Close attention has been given to ergonomics in the design of the MCR and of the DPS displays and the simulator is intended to include these designs fully for the training of the Station operators.

5.3 Commentary on the use of computers

The use of computers for on-line, reactor C&I is continuing to expand and, although ultimate safety is not invested in such systems, they are important if only because they govern the envelope within which the plant is operated. Direct digital control is used but in a conservative, limited way at present although it will undoubtedly grow if that can be done securely. Having said that, it must be noted that applications of computers have sometimes met difficulties.

Some of these difficulties have been technical whilst others have arisen from attempting to use installations which are too small. There is probably no one reason for this but it is partly due to a lack of critical assessment of likely needs at the initial design stage. Requirements arise late and are not made clear enough, early enough. Input signals proliferate because we now record information which would previously have been ignored, perhaps because modern equipment suppliers provide status outputs which previously did not exist but which cannot be neglected. Engineered safety features have tended to increase and, to a degree, computing is perceived to be a safety answer as well as important to plant availability. The situation is made worse by the way in which software requirements are under estimated. Together, these phenomena tend to place C&I on the construction critical path.

Furthermore, the methodology of safety justification has proved awkward. UK Industry has responded to this by establishing collaboration between various bodies including those responsible for research, project interests within the Electricity Supply Industry, Civil Aviation, the Railway Industry and others. Document IEC880 has made a considerable and positive contribution but it is often less specific in its guidance than licensing authorities require and the theoretical studies of research groups into formal methods of software functional definition, based on mathematically consistent logic statements are often impractical for engineering use. Theoretical objections to the completeness and self-consistency of computer languages and of micro-chip functional design have considerable importance in safety justification.

6. QUALITY ASSURANCE AND THE VALIDATION AND VERIFICATION OF SOFTWARE

Formal quality assurance and the qualification of hardware is becoming more important. The current method is to use standards set by the electricity boards but this is likely to change as the result of European integration and will have considerable impact. Manufacturers will need to demonstrate quality and this could generate problems.

In the software field it is necessary to distinguish the system from the application. The former tends to be outside the control of our Industry and is not necessarily verified to adequate standards. Architecture is therefore very important. The UK practical approach has been to rely on comprehensive verification and validation, and the full and systematic use of prototypes and of on-site testing. UK experience has been that licensing problems are often based more on the potential deficiencies of the hardware and system functional design than the potential and perhaps theoretical problems of the software. The general Software Industry approach in the UK to high integrity systems, whether in the Nuclear Industry or elsewhere, has been to require an independent design assessment for systems of the highest perceived criticality. There is very active, on-going concern in the UK for software systems in nuclear power plants. This is shared by other nuclear nations, although sometimes to a lesser extent due to reduced

construction programmes. The UK has participated actively in IEC discussions on this aspect, and international support from IAEA for these activities would be welcomed. The IAEA may consider it of value, and in the international interest, to support directly the production of licensing guidance on the use of computer-based systems for safety critical applications in nuclear installations.

7. EXPERT SYSTEMS

Expert systems are not yet widely used in the UK although it is noted that they tend to be used, even in safety related roles, elsewhere in the world. This is probably because opinion in the UK is inclined to require proof of ability and that is very difficult to achieve. It is found that the expert system community is not sensitive to these needs.

One application of a partial system is found on Heysham and checks whether the plant is within the probabalistic safety net. It is particularly concerned with post trip cooling. Fuel route sequencers also have expert elements. They are concerned with plant which has many limits and in which it is necessary to diagnosis trips and failures quickly. Such systems are designed to provide a fault code for the operator and safety is not a problem because he has the last word. They are not operated on line.

An operating rule/technical specification compliance monitor is being developed for more general application. It will use an expert systems shell and portable, automatic plant data collection methods.

8. TRAINING SIMULATORS

Work in this field has continued to follow improvements as they are made on site, one novel item having been the upgrading of magnox simulation in which a single machine can be fitted with alternative panels and thereby reproduce a number of Stations.

The AGR simulators are design specific and will be upgraded with the plant. For example, the SSEB have separate Hunterston 'B' and Torness machines. The latter is not yet operational but was used during design and had the valuable task of verifying the Station Operating Instructions

A new simulator has been provided and installed at PFR.

9. INDIVIDUAL ITEMS OF INTEREST

(a) The installation of tripping from temperature on a single channel in the AGRs could, in some cases, improve availability and output considerably. There are obvious problems of reliability which may be solved by the use of the pulse coded logic systems developed by the UKAEA in the late 1970s and used on the Prototype Fast Reactor.

(b) Many interesting instrumentation problems arise from the concept of a dry fuel store. The main tasks for the system are simple, mainly inventory control, quality checking and the control of moisture but conservative design is necessary to ensure that safety does not depend on microprocessors. It is achieved by a mixture of relays, magnetic logic and programmable logic controllers.

(c) The presentation of information is improving. It is better processed and better presented for both operational and for maintenance purposes. This has been achieved by improved QA, closer examination of what is on each page, attention to appropriate skills and knowledge and the use of simulators for checking. Users are becoming more sensitive to the quality of processed data.

(d) Problems have arisen on the non-destructive examination of Fast Reactor fuel because of the non-availability of neutron generating tubes.

10. SUMMARY

As has been stated, the main recent changes in power reactor C&I in the UK have been those associated with information technology but it is difficult to summarise with precision. A number of points can, however, be made in an international context:

(a) It should be remembered that the computer systems which are being commissioned today were designed in about 1980. The technology which governs size is probably growing faster than requirements but it is still necessary to be critical of the need for particular applications.

(b) The application of computer technology has not been confined to reactors but has also taken place in related fields such as the fuel cycle area. On example is an inactive feed computer on the PFR plant which greatly improves the control of small flow reagents.

(c) The problems of software verification and validation are important.

(d) QA and standardisation should not be ignored because of their possible impact on international trade. In this context collaboration between the IAEA and the IEC and ISO is important.

(e) It is now necessary to think in terms of several suites of C&I during life of a plant - particularly in long-lived applications like the dry store

(f) There is a tendency to think C&I cheap but it is not, having many hidden costs - especially those associated with software.

REFERENCE

1. MITCHIE, R. E. and NEAL, R. "Control and instrumentation: Micros, minis and making them manage". Conference on the Project Management of the Heysham 2 and Torness Power Station Construction Programmes. BNES. Blackpool. 1988

MAIN PRINCIPLES OF MODERN CONTROL AND PROTECTION SYSTEM EQUIPMENT (CPSE) DEVELOPMENT FOR NUCLEAR RESEARCH REACTORS

V.S. ZHERNOV, M.S. KALENSKIJ, A.V. PRONYAKIN
Union Research Institute of Instrumentation,
State Committee for the Utilization of
Atomic Energy,
Moscow, Union of Soviet Socialist Republics

Abstract

The problem of developing unified control and protection system (CPS) hardware on the basis of modern elements is actual in the USSR. The main requirement for CPS is connected with a provision of reactor operation safety, besides, it is necessary to reduce duration of idle time. The further increase of I&C automation level should be considered as one of the most important way for solving the safety problems. In this connection the main principals of the control and protection system design based on microprocessors are considered.

The proposed CPS is divided into three subsystems: protection subsystem, control subsystem and monitoring sybsystem. Th control and monitoring subsystems receive information from the protection subsystem through galvanically insulated communication line. The transfer of information between subsystems is performed in dynamic mode.

Lately the problem of developing unified control and protection sytem (CPS) hardware on the basis of modern elements is actual in the USSR. It is performed with regard for long-term operation of such systems and present requirements of nuclear safety. The operated NRR CPSE complexes have been developed basically by a project way by using different devices which have been combined into separate measuring channels and formed CPSE complex as a whole. Only sets of used different devices have been improved for some time past without complex approach to CPSE development as a whole and it has influenced on quality of the systems under operation.

Regualtory measures on increasing safety and NRR usage efficiency developed at present in the USSR foresee, in particular, the following:

- development of unified CPS, automatic reactor monitoring and control systems and other equipment;