THE 4TH INTERNATIONAL TOPICAL MEETING ON
NUCLEAR THERMAL HYDRAULICS, OPERATIONS AND SAFETY
April 6-8, 1994, Taipei, Taiwan

Man-Machine Interface Systems for the Sizewell B Nuclear Power Station

D B Boettcher
PWR Project Group, Nuclear Electric plc
Booths Hall, Knutsford, Cheshire
WA16 8QG, United Kingdom.
Tel: (44) 565 650 066 FAX (44) 565 682 605

Abstract

Sizewell B is the first nuclear power station to be built in the United Kingdom using the Pressurised Water Reactor or PWR system. The design is based on stations operating in the United States, but many changes and new features have been introduced to bring it up to date, and to meet United Kingdom practice and regulatory requirements. The Man-Machine Interfaces (MMIs) in the control rooms have been newly designed from first principles, with special attention paid to human factors and the role of the operators. The instrumentation and control (I&C) systems which interface the MMIs to the process plant, and automate the operation of the station, use advanced technology to achieve high performance and availability. This paper describes the development of the control rooms and I&C systems, explaining the thinking that lay behind the principal decisions.

Introduction

Nuclear Electric (and its forerunner the Central Electricity Generating Board - CEGB) has been designing, constructing, and operating nuclear power stations for over 30 years. The Sizewell B power station, on the Suffolk coast of England, is the first British nuclear power station to use the Pressurised Water Reactor (PWR) system. It is currently being set to work before commercial operation later this year. Nuclear Electric were the Architect-Engineer and Project Manager for the construction of the station, and it is now their 23rd operational reactor. Work on site began in 1987, with first permanent structural concrete in August 1988.

The basic design of Sizewell B is similar to late generation American four loop PWR stations, particularly Callaway and Wolf Creek. However, numerous changes have been introduced to meet Nuclear Electric's requirements, and UK safety and licensing criteria. This is particularly noticeable in the areas of I&C and MMI, where there is a complete departure from existing American practice. The designs of the principal control rooms, the Main Control Room (MCR) and Auxiliary Shutdown Room (ASR) are entirely new, as is the design of the I&C systems.

Historical Perspective

In the 1960s, the CEGB led the world in the design of power station control rooms, and was among the first to apply human engineering and ergonomics principles to the design of MMIs. The CEGB also pioneered the use of computers[1], and remained amongst the leaders in increasing their use.

The increasing use of computers for culminated in the backfit of a "soft desk" at the Didcot coal fired power station in the late 1980s. This enabled the operators to monitor and control the plant entirely via the computer. Dedicated controls and instruments were provided on back-up panels. It was found[2] that the operators resorted to using these back panels when plant conditions were changing quickly, and they needed rapid access to information. Although the experiment at Didcot was generally considered successful, the difficulty of ensuring sufficiently rapid and comprehensive access to information stored in a computer was recognised.

Incidents at the Heysham 1 and Hartlepool AGR stations in the early 1980s indicated that operators had difficulty in extracting important information from a mass presented to them in a serial form by a computer. Although computer displays can be improved, e.g. by the use of more screens, task based displays, and direct key access ("hot key") to important data, It was recognised that when things are happening rapidly, it can be difficult for an operator to build up quickly a mental picture because retrieving several items from the computer may need several actions, involving a number of formats. The need to manipulate (manage) the information system intrudes into the information gathering process.

Aspects of Plant Design

Sizewell B is the first nuclear power station to have its design process guided by a probabilistic safety assessment, in addition to deterministic rules. Stringent reliability requirements were imposed from the risk targets. This led to a considerable increase in the level of redundancy compared to existing American PWR stations. Limits on reliability due to considerations of common mode failure led to a corresponding increase in

the level of diversity. These factors, together with a rigorous approach to fire hazards resulted in four segregated divisions for the I&C essential to safety. Each division is adequate to maintain safety after a fault. These four divisions are supplemented by two divisions for equipment significant to safety, and non-safety. The amount of equipment, its diversity, and segregation, placed further demands on the design of the MMI systems to ensure that the operators could cope with the information while maintaining awareness of the whole plant status.

Fundamentals of Control Room Design

The Main Control Room (MCR) is the central operational location. The Auxiliary Shutdown Room (ASR) provides the remote shutdown facility. Throughout the design processes for both the MCR and ASR, the aim has been to ensure that the highest levels of integrated human-machine reliability and performance will be achieved; both in normal conditions and in the event of a fault.

To support normal operation of the station by a small complement of staff, computer driven displays on Visual Display Units (VDUs) provide flexible access to information. Displays use graphic mimics with embedded alarms, trends, histograms, and alarm lists. Because experience had shown that easy access to large quantities of information via VDUs is at the expense of information access times, it was concluded that conventional dedicated controls would be used, with dedicated displays (meters, lamps). These controls and monitoring devices are mounted on control panels, which provide near instantaneous plant wide monitoring and aid unambiguous and rapid identification of devices. An additional benefit of using conventional control panels is that concentration upon the plant state is not distracted by any needs to manage the MMI itself - the interface is transparent to the user. The dedicated control and display devices also enable safety actions to be carried out if the VDUs are not available.

Design Process for the Main Control Rooms

The design process for both the MCR and the ASR considered requirements for optimal human performance in the context of normal operation, plant faults, technical breakdowns, maintenance, and modifications. During the design process, in addition to technical specialists, up to seven professional human factors specialists and twelve operators were involved.

Consideration was given to general human performance characteristics, as well as those specific to the likely population of users. This included explicit consideration of allocation of function between man and machine, the physical environment, space and reach requirements, the psychological environment, and the particular control and information needs of tasks. The design processes were supported by the use of:

- Internationally recognised codes, guidelines, standards and checklists.
- International PWR operational experience and feedback.
- Quality assurance and design methods that take account of the human factors issues involved in designing large complex systems.
- Research and development where necessary, particularly when no adequate norms exist; for example in VDU based MMI design.
- Task analysis to identify operational needs for control and information with respect to form, quantity, type, etc., and to explore mental models of the processes and plant.
- Verification and validation of the resultant environmental and equipment designs,
- Verification and validation of the operating procedures used to control and monitor the plant, particularly following the onset of a fault.
- A high fidelity full-scope simulator to thoroughly train and retrain control room personnel.

A full scale mock-up of the control room, first built in the early 1980s, was used to test ideas of desk and panel shapes, locations of computer displays, lighting schemes, etc. This has proved to be an invaluable tool for allowing the rapid prototyping of different ideas, and in facilitating debate. Figure 1 gives an overview of the development programme for the control room, the control room panels and VDU formats, and also the training simulator. The regulator required the training simulator be available one year before fuel load, so it was constructed two years early to allow time for the instructors to become familiar with it before training began.

Implementation of the Main Control Room

The man-machine interface was designed by an integrated multidisciplinary team. An objective was to deliver information to the operators with high reliability, via appropriate technology, and at the appropriate location. Where required for reasons of safety, sufficient levels of redundancy and diversity have been incorporated to ensure that the necessary information will be available, even in the presence of failures.

The operator and supervisor monitor operation of the plant under automatic control from central desks. High resolution colour VDUs are provided on the operator's and supervisor's desks to enable them to monitor normal operation of the plant from a seated position. The VDUs are recessed into the desks to allow line of sight viewing of the large plant mimics on the control panels (Figure 2), and are angled to allow viewing of the screen near to the normal line of sight.

Panels carrying functional and mimic diagrams surround the desks, and give an overview of conditions. The relative positions of the panels minimise the need for the operators to walk around; this was verified by task and link analysis. All panel layouts received extensive operator and ergonomics input to their design, and have been extensively verified and validated. This was done using

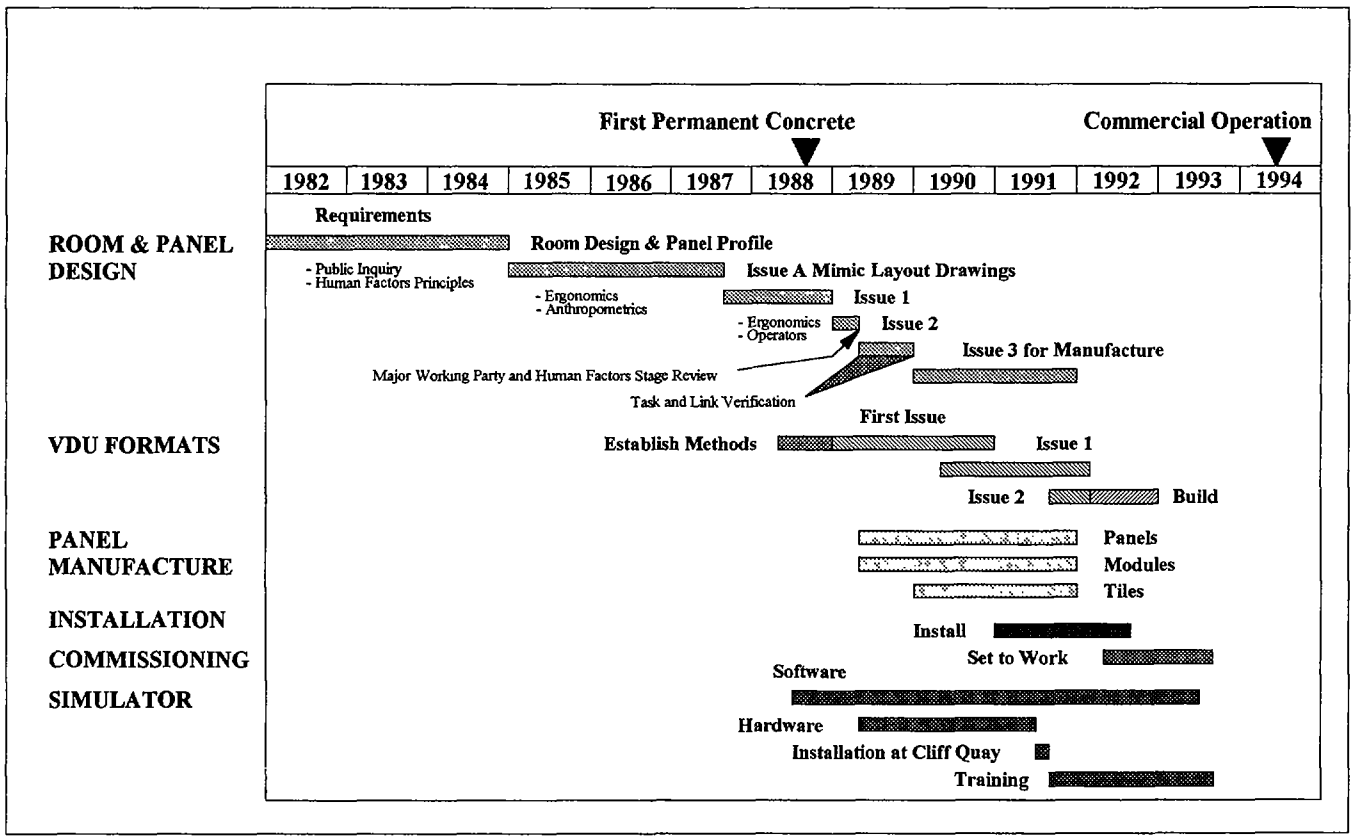

Figure 1: Overview of Control Room Development

both the mock-up and the simulator. The panels have VDUs mounted above them to allow monitoring and alarm handling whilst working at the control panel. All plant information is accessible via any of the VDUs in the control room.

Advanced User Interface

The computer generated displays take advantage of the advanced technology provided by modern computer workstations. The users interact with the system via graphical windows, icons, menus, and pointers - a WIMP environment. The SUN Microsystems OpenWindows interface is used. Employing advanced display techniques such as these means that the ease of access to information within the computer is enhanced, because the organisation of the information displays allows flexible navigation through the display structure.

Each physical workstation has two VDU's acting together to form the display interface. The graphical pointer travels continuously from one VDU to the other, and the position of the pointer dictates which VDU is affected by the keyboard. There are four windows for process mimics, distributed across the two VDU's forming a workstation. The number of process mimic windows is restricted to four, for ergonomics and time response reasons. The operator interacts with the system using a keyboard with integrated graphical pointer control via a trackerball. The user interface is designed such that the primary interaction will be using the graphic pointer. The keypad also provides a QWERTY style keyboard for direct data entry. A set of function keys ("hot keys") gives direct access to important or frequently used displays and functions.

The information display formats are structured in a shallow and wide hierarchy, supplemented by pop up windows. There are about 450 pages of system mimics, which map onto sections of the physical control panels to provide coherency. A further set of around 50 task based formats group information needed for particular tasks. Each format contains navigational "targets", giving immediate access to associated formats. This facility is used to access formats related in an operational sense, and to move up and down the format hierarchy. A soft button on each format brings up a menu of the previous eight selections within that window. The ease of use of the system has been verified by ergonomic investigations involving operators.

The system also provides full alarm handling, either directly from the mimic formats, or from lists of alarms. The choice of whether mimics or lists are used is at the discretion of the operator. Alarm signals can be dynamically assigned a *significance*, based on the current plant mode. Those alarms that are not significant are handled in a less obtrusive manner than urgent alarms.

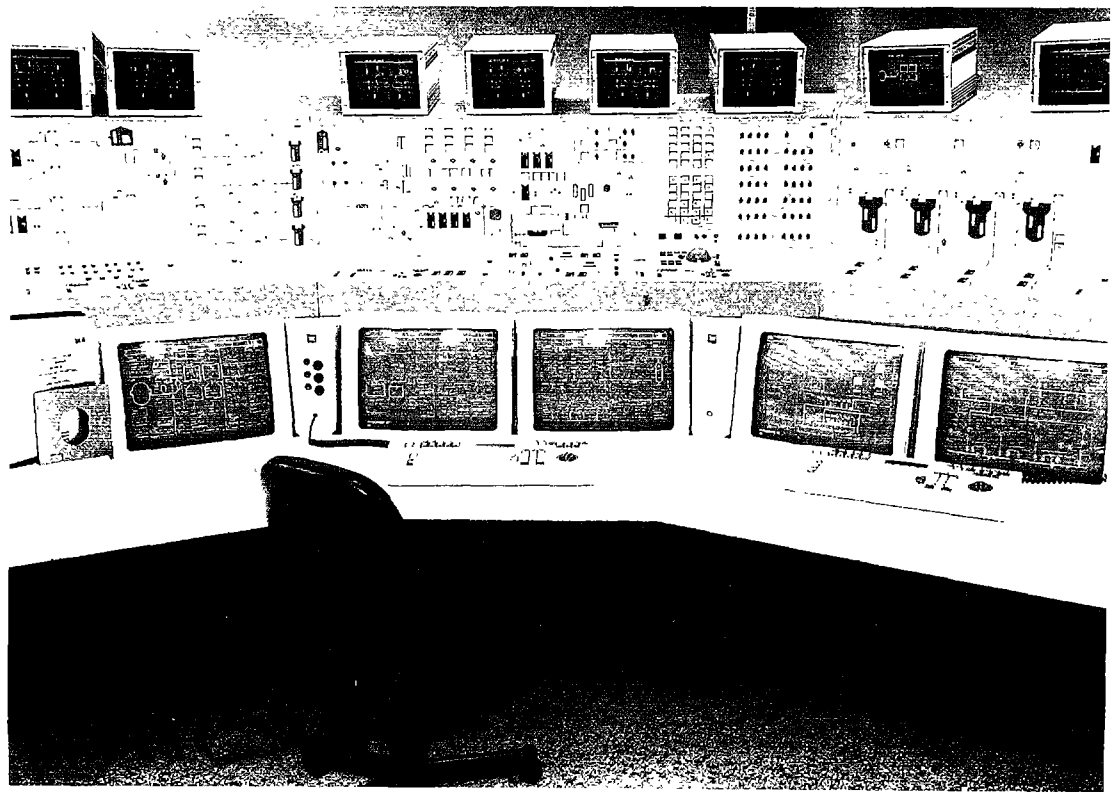

Figure 2: Operator's Desk

Fundamentals of I&C Design

Robust system design principles are used to achieve high reliability and protection against the propagation of failures. These include segregation of major I&C functions into separate electrical groups, separation of redundant equipment with those electrical separation groups, and the use of fault tolerant equipment. Standardisation of hardware and software, and modularity of design, is used to simplify both the design process and maintenance of equipment. Modularity also provides protection against obsolescence by allowing the modular introduction of new or updated technology.

Digital systems are used because they have high accuracy, resistance to drift, ability to perform self diagnosis, and the ability to provide user-friendly interfaces for operation and maintenance. On-line test features perform continuous self diagnosis of hardware and signal paths, and alert the operators to equipment failures. Multiplexed data communications reduce the number of cable runs throughout the plant, easing installation and reducing combustible loading.

Implementation of the I&C Systems

Figure 3 shows the general architecture of the I&C systems supporting the MMI. A distributed computer architecture is used to provide a flexible and extensible system, without overloading the data communication highways. Communication between remote processors takes place over local area networks, and data processing takes place as close as possible to the point of acquisition or requirement, with data only transmitted over the network if it is required by a remote processor. Figure 3 does not show the reactor protection systems, or a small set of instrumentation that is hard-wired for safety.

High Integrity and Process Control Systems

The HICS provides the majority of the safety classified man-machine interface. It interfaces manual controls on the MCR and ASR control panels, drives discrete panel meters and lamps, and displays data on four, seismically qualified, plasma display units in the Main Control Room. The HICS also passes data to the Distributed Computer System (DCS). It is subdivided into four separate networks, each network being redundant to the others for safety functions, as well as being electrically independent and segregated from them. In addition to the

redundancy provided by the four redundant HICS networks, internal redundancy is incorporated into HICS data highways and processors where high reliability is required. On line diagnostics provide early detection of failures, and redundancy allows maintenance staff to change a failed component before functionality is affected.

The Process Control System provides data acquisition and control functions that are not safety classified, but which can either make a contribution to safety, or have no safety role. It interfaces between the control panels and the plant, and passes data to the DCS for processing and display. The PCS is subdivided into two separate networks, each of which is similar in architecture to a HICS network. The PCS is a well established commercial product with a successful history of operation in over 500 applications world-wide. The PCS required no software development for the Sizewell B application, and so credit was taken for this operational history as evidence that the software was fit for purpose.

Distributed Computer System

The DCS uses advanced workstation technology. DCS functions are distributed among individual processing units (or "drops"), linked by three highways. The three highways comprise two deterministic WestnetII Highways, one for category 1 and one for category 2 data, and an Ethernet information highway. The individual processors are Sun SPARC based workstations, using commercially available Sun processors with the UNIX operating system. The unmodified Sun SPARC processor boards are assembled into a cubicle of Westinghouse design.

On-line redundancy is provided at all levels. The WestnetII and Information Highways are dual redundant for data acquisition and communication purposes, and use a deterministic protocol when handling important data. All operator stations have access to the same data, and therefore the multiple workstations are redundant to each other. The VDUs shown in the picture (Figure 2) are all Distributed Computer System drops from the Westnet data highways shown schematically in Figure 3. The large number of VDUs on top of the control panels is ensure that an operator working at the panel has easy access to information via the Distributed Computer System.

Software Engineering

Software quality is ensured by following structured software engineering methodologies, with comprehensive documentation, and independent verification and validation. The Process Control System is a pre-existent system used in over 500 applications world wide. The High Integrity Control System software has been written using the same methodology as employed for the Sizewell

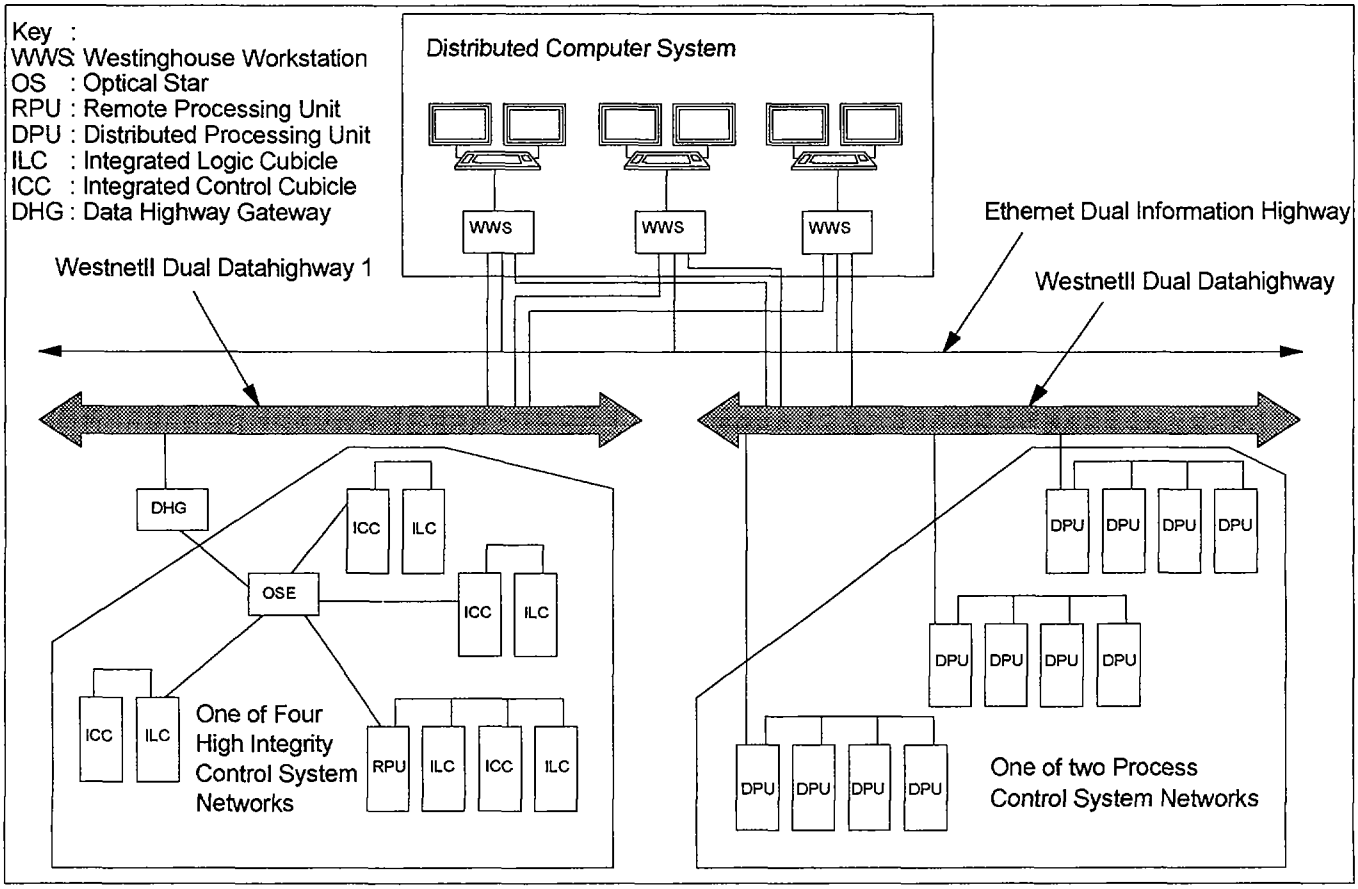

Figure 3: Overview of I&C Systems

Primary Protection System, and on numerous other safety grade systems supplied by Westinghouse. The Distributed Computer System software has been written using the Structured Analysis / Structured Design (SA/SD) tools from the Cadre Technologies Teamwork™ toolset. Reliability is estimated by Functional Block Analysis (similar to Failure Modes and Effects Analysis but applicable to microprocessor systems) and Fault Tree Analysis techniques.

Conclusions

Nuclear Electric plc has over 30 years of experience in the construction and operation of nuclear power stations, and Sizewell B is the latest embodiment of that experience. Amongst the novel features introduced at Sizewell B are entirely new designs for the Main Control Room and Auxiliary Shutdown Room, and the extensive use of distributed computer technology to provide a reliable and user friendly Man-machine Interface.

Expert attention was applied to both the human and technological characteristics of the Man-machine Interface to ensure that the highest levels of integrated human-machine reliability and performance will be achieved, with the operators having a clear understanding of current plant conditions, and being able to control the plant to provide high levels of availability and safety, with low levels of human error, at all times.

Digital systems have been used extensively because of their high accuracy, resistance to drift, ability to perform self diagnosis, and powerful user-friendly interfaces. Robust system design principles have been pursued to achieve high reliability and protection against the propagation of failures.

Nuclear Electric is very proud of the design of the Sizewell B instrumentation and control systems, and the achievements that have been made on site to date. The design team at Knutsford are confident that their efforts will be rewarded by the safe and economical production of electricity from Sizewell B.

References

1. B R Welch, "Computer Systems in CEGB Nuclear Power Stations," Nuclear Engineering International, January 1973.
2. C S Reiersen and J V F Berman, "An Operational Evaluation of the 'Soft Desk' at Didcot Power Station," CIDOCS 1698, Nuclear Electric Projects Division, February 1990.