OPERATIONAL EXPERIENCE WITH THE SIZEWELL B INTEGRATED
PLANT COMPUTER SYSTEM

J.E.J. Ladner, N.C. Alexander, J.A. Fitzpatrick

Messrs Ladner and Alexander are employed by Nuclear Electric at Sizewell B
Miss Fitzpatrick is employed by Westinghouse Process Control Division in the USA

SYSTEM DESCRIPTION

The Westinghouse Integrated System for Centralised Operation (WISCO) built by
the Westinghouse Electric Corporation Process Control Division in Pittsburgh, USA
is the primary plant control system at Sizewell B Power Station. This system is based
on the original ISCO design from Nuclear Electrics PWR Project Group (PPG) which
called for a distributed computer system to implement the majority of reactor and
support systems control. This implementation included all plant data acquisition and
display through the use of both VDU process diagrams, or formats, and the more
conventional desk indications.

WISCO comprises three subsystems; the High Integrity Control System (HICS), the
Process Control System (PCS) and the Distributed Computer System (DCS).

High Integrity Control System

The High Integrity Control System is based on the Westinghouse Eagle Series
control technology and performs the control and data acquisition of the category 1
(i.e. nuclear safety significant) plant systems. It also provides the category 2 Station
Automatic Control System (SACS). The HICS is distributed across the four essential
electrical separation groups. Redundancy is provided within individual cubicles by
the provision of two processors. Data is communicated between cubicles within each
separation group via redundant fibre-optic data highways. Data is also received from
other alien systems such as the Primary Protection System. Data from the HICS
which is required either for display to the operator or for use by the PCS is passed to
these systems via transmit only fibre optic links to the DCS.

All the HICS controls are held in firmware. On line changes and software
interrogation is via a dedicated serial interface.

Process Control System

The Process Control System is based on the Westinghouse Distributed Processing
Family (WDPF) technology which uses redundant Data Processing Unit (DPU) pairs.
Each processing unit consists of a 386 processor, shared memory and data highway
controller. Each processing pair is connected to its own distributed I/O bus to which
a variety of I/O cards can be connected.
Each DPU is connected to a redundant data highway which also has direct connection to the DCS for data display. Software maintenance of the PCS is achieved by a suite of applications available on the DCS.

Distributed Computer System

The Distributed Computer System is built around a number of Sun Sparc workstations and servers, otherwise known as drops, running the Solaris 2.1 operating system. These communicate with each other over a standard ethernet. The workstations provide the man machine interface facilities to the Main Control Room, while the servers provide supporting services such as logging, historical storage and retrieval, special computations, etc. A software server is employed as a master software source from which all other drops, including PCS DPU's are loaded with their application software. All the drops are connected to the two redundant data highways which pass data from the HICS, PCS and other alien links.

MAINTENANCE STRATEGIES

The maintenance requirements for every plant system at Sizewell B are covered by a Maintenance Strategy Report (MSR). In the case of computer based systems there is also a Computer Strategy Report, covering additional aspects such as software and data maintenance and system security. The MSRs can be broken down into the following areas:

a) a description of the system and its function
b) a description of its relation to nuclear or other safety
c) detailed maintenance requirements as set out by
   i) the stations safety case, eg equipment qualification
   ii) the manufacturers operation and maintenance manuals
   iii) worldwide best practices and experience
d) a complete listing of all maintenance activity routines.

Having established the requirements through the production of the MSR, routine activities are scheduled through the Passport maintenance database system, with details of the work to be done set out in Plant Maintenance Instructions (PMI). Routine WISCO maintenance is minimised to reduce the potential for maintenance induced defects. It is largely restricted to work of a non-intrusive nature, and includes filter cleaning, power supply checks/calibration and dynamic RAM battery replacement. Such work is carried out with the reactor at power wherever possible to avoid impacting the refuelling outage programme. All other hardware maintenance is carried out as a result of breakdowns. This approach is possible due to the redundancy built into the systems, and the comprehensive on board diagnostics. The redundancy mitigates failures, and the diagnostics allow rapid identification of, and response to, defects. The impact of all work whether the reactor is on load or not is carefully assessed before being performed, and written impact statements are provided to the operators, to aid decision making in the release of systems.

Maintenance work associated with WISCO was originally performed by Westinghouse staff. This responsibility has gradually transferred to station staff after
they had received specialist training from the supplier. Some of the non-intrusive routine work has now been transferred to full time maintenance contract staff. This has allowed station staff to spend more time attending to more detailed investigation and defect work.

Spares

A comprehensive spares holding has been set up with a proportionate number of spares for each circuit board or unit type to cover the majority of failures. It is particularly important to ensure that any spares held are of the correct revision; this generally being related to the installed firmware.

SYSTEM PERFORMANCE

Hardware

The system has performed exceptionally well over the first Cycle. The designed mean time between failure (MTBF) statistics were very pessimistic in comparison to the actual MTBFs encountered. The rate of component failure has in general been proportional to the number of such components installed in the system. HICS failures place a greater onus on the station to effect a speedy repair since this subsystem is governed by the stations Technical Specifications. These prescribe availability and time constraints on specific plant breakdowns before other action must be taken to mitigate any nuclear safety implications. In general due to the diagnostic information presented by the HICS problems can normally be resolved within 24 hours.

Component failure rate statistics have been collated for the three subsystems and are shown in graphical form in figures A, B and C.

Loss of Facilities

The number of occasions when functionality has been lost has been very low. The failure of a DCS hard drive recently caused a failure of continuous printed logs local to the Main Control Room and the loss of alarm and event archiving for some hours. This failure took some time to correct since not only did the drive have to be changed but a full reload of the affected drop’s operating system and application software was required.

Another, potentially more serious, event affected a hybrid HICS/PCS cubicle, which forms the physical link between the MCR desk instrumentation and controls and the WISCO. A circuit board on one subsystem failed, but the subsystem did not fail over to its redundant partner. This was identified as a shortfall in the software design for the cubicle which has since been modified to failover if such an event were to reoccur.
MODIFICATIONS

There have been a number of modifications to the WISCO over the first fuel cycle, resulting from commissioning and early operating experience. These have in the main been software changes to support modifications to other plant systems. Such system modifications have various impacts on WISCO, ranging from alarm setpoint changes to a full redesign of a control loop.

There are currently some 200 outstanding modifications. Until the present time all modifications have been implemented by Westinghouse with Nuclear Electric’s (NEL) Engineering Division (previously PPG) performing the engineering aspects of the modifications. NEL currently have a number of engineers training with Westinghouse, to allow them to implement future application changes.

Two major modifications which are currently in progress are the Alarm Optimisation scheme which aims to optimise alarm presentation to the operator (covered in a separate paper), and “bouncing meters”. The latter modification is being introduced to resolve a problem with panel mounted meters which fail to the “zero” position when the input signal to WISCO goes to Bad Quality, ie out of range (generally 4 - 20 mA). This has presented operators with a situation where they cannot determine by solely looking at a meter that it is faulty. The modification proposes to drive the meters between 0 and 15 % of their full range at a predetermined frequency to indicate a bad quality signal. This will give a clear unambiguous indication to the operator.

Modification Procedure

Whatever the scope of a WISCO software modification, the same procedures are used to design, test and implement it.

NEL Engineering Division in conjunction with Westinghouse have built up a suite of procedures for the development of new software. Since Sizewell B became an operational site these procedures have been brought under the station’s own procedures.

All modifications at Sizewell B are initiated through a Modification Approval Form (MAF). This requires that the modification is assessed for its significance and impact on nuclear safety, in line with the requirements of the Nuclear Site Licence. For software changes, following approval of the MAF, a Functional Software Specification (FSS) is produced. This is in two parts; part A defines the functional requirements while part B defines the method by which these requirements are to be implemented. A Detailed Design Specification is also produced or updated in conjunction with the new software.

Testing of any new or modified software is performed on the off-line WISCO Maintenance and Test System (MTS). This can be configured to represent any part of the on-line WISCO system since it comprises a number of cubicles from each subsystem. The MTS will remain in Pittsburgh until late 1996 when it will be broken up, shipped and recommissioned at Sizewell B. From this point, the implementation of the majority of new modifications will be performed jointly between NEL Engineering Division and station staff.