INTRODUCTION of HFE for HUMAN INTERFACE DESIGNS

A cornerstone philosophy for the CANDU 9 design program utilizes ***proven*** CANDU features and concepts which have contributed to the world leading performance of operating CANDU stations. This design strategy is important to ensure that:

- the final design achieves the functional ***safety & economic project goals*** and targets
- the ***station licensing*** process proceeds in a scheduled and predictable manner
- project costs are maintained to the estimated values (or decreased where practicable)
- project construction & commissioning ***schedules*** can be adhered to
- possible ***risk factors*** associated with the implementation of new concepts are ***eliminated***
- operation, maintenance and administrative ***costs are minimized***

The CANDU 9 Control Centre design includes the ***proven functionality*** of existing CANDU control centres, those characteristics identified by systematic design with human factors ***analysis of operations requirements*** and the advanced features needed to ***improve station operability*** which are made possible by the application of new technology.

The design strategy is to preserve the main control room (MCR) operator work area as ***unchanged as possible*** to facilitate the inclusion of past features and operational experience while incorporating new operability requirements. Consequently, the CANDU 9 MCR panel base area will be similar to that of the CANDU 6.

Recent statistics show that high numbers of plant significant events are attributable to human errors. Consequently, special attention is given to ***human factors engineering*** (HFE) during the design of the CANDU 9 project in general and Control Centres in particular. The CANDU 9 design process follows a ***systematic analytical approach*** to system design to define ***operator information*** and ***information presentation*** requirements. The resultant operator display, annunciation and control information is then ***verified*** against the system design requirements to provide a high confidence level that adequate and correct information is being provided necessary to support the operational tasks.

PROVEN BASIS for CANDU CONTROL CENTER DESIGN

The basis for initiating the design of the CANDU 9 Control Centres was the well-known information and operations requirements of the operating CANDU 6 power plants. In addition, Wolsong 2, 3, and 4 CANDU 6 Control Centre improvements, such as the Emergency Core Cooling panels and complementary operations features adapted from the Darlington CANDU multi-unit station were assimilated into the design.

The relatively unchanged MCR panel base area has the advantage of ***retaining proven operability features*** from previous CANDUs as well as allowing the resultant design to be ***retrofitted*** in an existing CANDU station as part of a station rehabilitation program.

The control panel area/system interface ***recognition factor*** will assist construction, commissioning, technical, maintenance and operations staff through construction, commissioning and operations phases.

It is expected that there will be some time savings and human error reduction achieved by maintaining this common CANDU Control Centre panel orientation as well as maintaining the very strong safety grouping separation for cables and equipment. An early significant economic benefit will be realized during startup by the ***operational effectiveness*** and efficiency achieved with the familiar systems and user friendly panel interfaces during first-unit operations.

The ability to compare the CANDU 9 panels and system displays to previous CANDU installations will facilitate the tasks needed to ensure ***completeness and correctness*** by the designer, construction contractor, client utility technical and operating staff as well as the regulators.

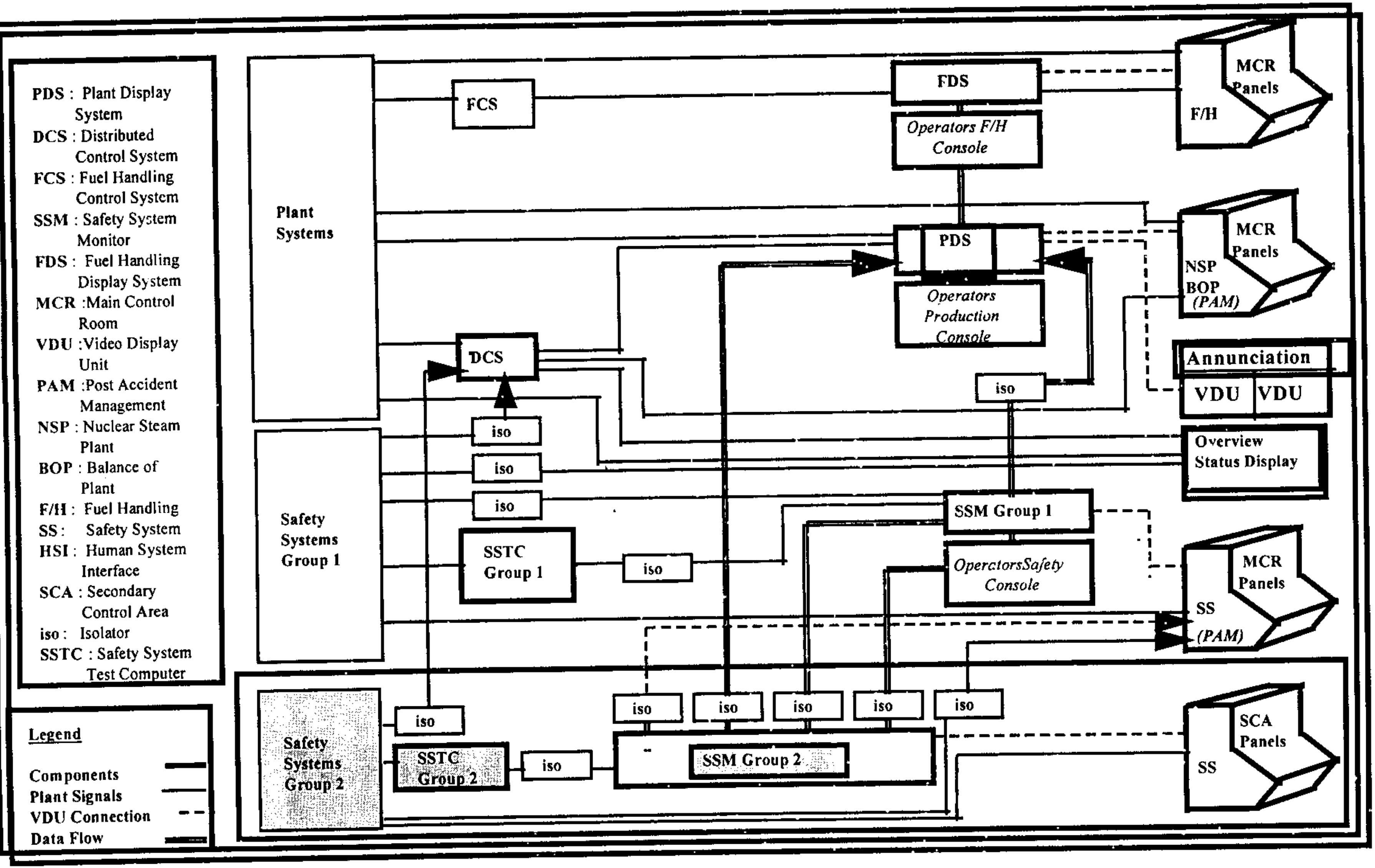


Figure 1: CANDU 9 Control Centre Functional Organization

SYSTEMATIC DESIGN WITH HUMAN FACTORS ENGINEERING

Recent statistics show that up to 70% of plant significant events can have a root cause attributable to the human from such sources as the operation of complex systems, mis-interpreted interfaces, procedures, maintenance and management practices. Consequently, special attention is given to Human Factors Engineering (HFE) during the design of the CANDU 9 Control Centre.

The goal of the CANDU 9 Control Centre design team is to ***successfully integrate*** all control room interfaces into one functional system including control room staff, support facilities, human-system interfaces, operating procedures, and shift management. This synergistic system will allow the CANDU 9 nuclear power plant to be operated safely and efficiently over all plant operating regions.

AECL staff believe that the HFE discipline provides an opportunity to apply a thorough, ***systematic and traceable design methodology*** for a design initiative.

Without an HFE basis, a design is vulnerable to unique designer inputs which are dependent upon the individual designer's education, experience, knowledge, personal preferences and perceived project goals.

AECL minimizes these potential design input variances by establishing an HFE design process basis (starting with the project ***HFE Program Plan*** - HFEPP) and integrating this HFE process into the project design to interface all designers from all disciplines.

The CANDU 9 design process follows a systematic analytical approach (involving designers from safety, process systems, controls, electrical, civil, control center, HFE, etc.) to system design with requirements definition, function analysis, function allocation and task analysis, combined within a verification and validation (i.e. V&V) cycle, to define operator information and information presentation requirements in the Control Centres.

SYSTEMATIC DESIGN WITH HUMAN FACTORS ENGINEERING....continued

Initially, the CANDU 9 HFE staff prepared the project HFEPP to provide a framework and guidance for the design and verification process to be used for the project.

This HFEPP was reviewed and modified by project staff, management and executive prior to being submitted to the Atomic Energy Control

Board (AECB), the Canadian Nuclear regulatory authority. Regulatory feedback required further modifications to the HFEPP to improve clarity and address omissions.

Once the CANDU 9 HFEPP was approved, project documents called up by this plan were prepared. These underpinning documents are ***project-wide*** in nature in that all designers from all disciplines can be affected to various extents.

Documents such as project ***procedures*** governing the manner of preparation for design requirements and design descriptions were revised, reviewed and approved. The HFE components of these procedures were distributed across the entire document rather than being constrained to one section.

The HFE section of these design documents is more of a ***summary and cross reference*** to the HFE components throughout that document. In addition, these procedures provide a means of integrating HFE into the design process from the start with an increasing scope as the design proceeds.

For example, at the early stages of the design, it is sufficient that the designer identifies and documents the high level functions and interfaces as well as the high level allocations for those functions. As the design proceeds, this information can be revisited and completed to a greater level of detail so that such details as **Automatic/Manual**, **location** in Main Control Room/Secondary Control Area, Process/**Safety**/Post Accident Monitoring/Critical Safety Parameters, VDU (Video Display Unit)-based or **hardwired**, plant operating regions, etc. can be addressed.

HUMAN FACTORS ENGINEERING DESIGN GUIDANCE DOCUMENTS
To assist in this systematic design process, the CANDU 9 HFE staff also developed project HFE ***Assessment Documents*** and ***Design guides*** as required by the HFEPP to provide further guidance to all project designers to better follow the procedural instructions. These HFE guidance documents provide specific detailed information necessary to implement particular aspects of the design.

CANDU 9 HFE ***Design Guides*** address project topics such as:

- Function Analysis
- Task Analysis
- Maintenance, Testing and Inspection
- Computerized Display & Control
- Annunciation

- Panel Layout & Device Selection

The system designers refer to these design guides for increasing levels of design detail or ***methodology*** as the design for that system proceeds. The designer has the reference plant functional and operational bases, the operational feedback input, the project procedures, and the HFE design guides as guiding mechanisms for the content and methodology for that portion of the design.

Traditional discipline oriented design techniques are followed, but these are ***directed*** and ***standardized*** by the mechanisms mentioned to achieve a functional, consistent design product from design discipline to discipline and from designer to designer.

HUMAN FACTORS ENGINEERING IMPLEMENTATION

Function allocation is considered early in the requirements definition stage as designers are guided to consider, for example, if the function should be performed automatically or manually (i.e. allocated to machine or human) and if automatic, should that function be performed by computer or hardwired devices.

The procedures, design guides and the reference plant bases assessment documents aid the designers in this allocation. Further function allocation details are defined as the system design description is prepared. A ***function analysis*** design guide is used by the CANDU 9 designer to progress the on-going design review/evaluation process to ensure that required operational sequences can be conducted effectively and efficiently.

Not all operational sequences will be subjected to the ***task analysis*** process. Task analyses will be completed for those operational tasks which are identified as having ***high risk*** and/or a ***high degree of difficulty*** for completion, or those tasks which are ***new*** in comparison to the reference plant.

Any operational tasks from the reference plant for which ***concerns are raised during the V&V*** process will also be subjected to a task analysis and review to ensure that the optimum achievable task sequence is implemented for the CANDU 9.

The resultant operator display, annunciation and control information is verified against the system design requirements to provide a high confidence level that adequate and correct information is provided, necessary for the operational task at hand.

This verification process includes the traditional supervisory and peer document reviews, CADDS reviews, procedural walk-throughs moving to validation by utilizing the physical full scale panel mockup facility which is supported by the PC-based CANDU 9 plant simulation.

HUMAN FACTORS ENGINEERING IMPLEMENTATION...continued

At early stages of the design, system designers are responsible for the collection and evaluation of ***Operational Experience Review*** (OER) information as well as participation in operational feedback sessions with utilities.

The OER information collected highlights design features and attributes which demonstrate high performance levels and hence are worthy of retention or those which demonstrate lower performance levels and are possible candidates for review, analysis and re-design.

The CANDU 9 control centres operational experience review meeting included operations and design staff who had instrumentation and control, computers, control centres, plant display, annunciation, HFE and plant electrical expertise.

The simulation supported mockup of the panels and consoles at AECL's design facilities will be used for V&V of the Control Centre features, displays and operator interactions. The CANDU 9 Control Centre mockup exists both as a 3D CADD model and as a full scale physical mockup facility.

The 3D CADD model is a scaled representation of the equipment to be located in the mockup room. The 3D CADD model has been evolved from the reference Control Centre design to the proposed CANDU 9 layout providing designers with a retrievable design record.

Once confidence for a particular design detail is obtained from the evaluation of the CADD model, that change can be incorporated into the physical mockup for full scale replica testing and evaluation.

HUMAN FACTORS ENGINEERING IMPLEMENTATION...continued

The Control Centre mockup serves as a designer tool to verify that the individual system designs conform to HFE principles, ensuring acceptable performance of specified operational tasks.

The functionality of the Control Centre mockup provides a mechanism for V&V design activities such as the panel or console attributes, displays, annunciations and operator/ maintainer interfaces.

The CANDU 9 system designers utilize the mockup throughout the entire project design life-cycle.

GENERAL CONTROL CENTRE DESIGN FEATURES FOR IMPROVED OPERABILITY

The CANDU 9 Control Centre provides plant staff with improved operability capabilities due to the combination of proveness, systematic design with HFE and enhanced operating features. A major evolutionary change from previous CANDUs is the ***separation*** of the ***Control*** and ***Display/Annunciation*** features formerly provided by the digital control computers (DCC). This CANDU 9 function separation provides control in the distributed control system (***DCS***) and display/annunciation in the plant display system (***PDS***). This strategy allows powerful computers without practical application memory constraints or execution limits to provide extensive control, display or annunciation enhancements within an ***open architecture***.

Significant design aspects which contribute to improved operability include:

- improved operator work station interfacing
- standardization
- improved operator awareness of station state
- enhanced data presentation
- workplace stress reduction

GENERAL CONTROL CENTRE DESIGN FEATURES FOR IMPROVED OPERABILITY

Operator Workstation Interfacing

The CANDU 9 station can be monitored at most times from the main operations console (MOC) which is centrally located before the MCR panels U-shaped layout.

The correct and continued operator work station performance assumes more significance for the CANDU 9 to ensure that the unit economic production goals are achieved and maintained.

Provision of central extensive information access and control implementation capabilities from the consoles (including safety system monitoring, testing, annunciation, plant control displays, critical safety parameters, critical production indicators, etc.) is such that the ***power range operation*** and evaluation of the plant status can be conducted by the operator from the MOC.

Redundant operator work stations are configured to allow ***multiple fallback*** operating stations in the unlikely event that the MOC becomes unavailable, to allow uninterrupted plant control without exceptional demands being placed upon the operator.

The same orientation of VDUs for the user with the same interfaces is provided for each of the operator work station sets.

This information presentation and control implementation ***standardization*** minimizes the opportunity for ***operating errors*** under off-normal conditions once a back-up work station has been enabled for full control capability following the failure of the principle work station.

GENERAL CONTROL CENTRE DESIGN FEATURES FOR IMPROVED OPERABILITY

Standardization

Standardization of the operator ***interface*** to plant systems is crucial for an efficient Control Centre design. During plant manoeuvring conditions, it must be possible for an operator to move from system to system interface with a ***minimum of conflicting data presentation*** methods, alarm formats or control implementation methods.

Standard panels for the entire CANDU 9 plant (NSP, BOP, F/H) will be provided with a ***standard display/presentation philosophy*** which provides operators with a consistent appearance from system to system.

The design goal for this Control Centre aspect is that the general ***appearance, meaning and operability*** of the key indicators and controls will be ***immediately apparent*** to the operator.

The device location on each panel, colours, light status, handswitch positions, VDU display features and so forth are standardized so that operator data assimilation time without perception errors is minimized.

Another important aspect of standardization is the application of a ***consistent allocation philosophy*** for plant functions to a hardwired system (referred to as a ***hard system***) or a computer-based software system (referred to as a ***soft system***). This philosophy is based primarily upon station ***safety requirements*** with a secondary evaluation of ***potential economic benefits*** provided that the safety constraints are satisfied.

If a control/indicating/annunciation function is required to manoeuvre the station from an event end point following a potential failure of a soft system, then that function must be provided by a hard system.

GENERAL CONTROL CENTRE DESIGN FEATURES FOR IMPROVED OPERABILITY

Standardization.....continued

The ***hard system*** for the CANDU 9 will be unequivocal such that functions designated as requiring a hardwired configuration will be 100% hardwired, discrete devices.

For example, the plant system functions required to safely take the unit from a soft system ***failure end point*** (e.g. zero power hot state) to the cold shutdown state will be hardwired with no necessary data transmissions via computer devices.

A hard/soft ***allocation review*** will be conducted for those hard system functions which are presently provided in the reference plant but which are not restricted by safety constraints.

GENERAL CONTROL CENTRE DESIGN FEATURES FOR IMPROVED OPERABILITY

Improved Operator Awareness

An extracted information set presented to the power plant operators can be used to facilitate overall system or station state ***awareness*** and ***comprehension***. The CANDU 9 ***annunciation system*** has been designed to alert the operators of potential off-normal conditions, to clearly indicate the ***plant state*** and ***system event*** occurrences and to provide a fast, user friendly procedural action follow-up aid.

Combining the comprehensive plant parameter database with powerful computer processing and the station operating procedures database provides the opportunity to create a unique annunciation system. Adequate information is available to assess the plant and system state for a wide variety of conditions.

The ***overview display*** is an operating convenience which also facilitates operating staff awareness. The centrally located overview display indicates the status of the major station systems so that the general state of the plant is immediately recognized by operating staff upon first visual scan.

Large scale indications ensure readability from a distance of ten meters. Such conditions as operating at power, energy mismatches, shutdown hot, shutdown cold, guarantied shutdown and the associated transition states will be emphasized and presented in an obvious manner.

The overview display presents the unit status in a simple format so that comprehensive unit awareness is immediate and uncomplicated for operating staff.

GENERAL CONTROL CENTRE DESIGN FEATURES FOR IMPROVED OPERABILITY

Improved Operator Awareness....continued

Operability is further enhanced by a functional display system ***navigation philosophy*** which facilitates the operator's task of ***accessing*** and ***assimilating*** necessary plant data.

Due design consideration has been given to the logical and relational parameters of interfacing systems so that operators can easily move laterally or vertically through the ***display hierarchy*** to call-up the desired display.

Display action points are presented as device icons, menus, flowsheet connectors, parameters or action buttons to accommodate operator personal preferences.

The utilization of a flexible navigation system for the VDU-based plant display system allows custom information displays to be accessed in a repeatable, simple, direct, convenient and logical manner by operations staff.

GENERAL CONTROL CENTRE DESIGN FEATURES FOR IMPROVED OPERABILITY

Enhanced Data Presentations

The CANDU 9 design provides one common plant parameter database so that all plant signals are accessible for computerized monitoring, checking, display and annunciation much more extensively than was possible in previous designs.

This feature largely unloads the operators from routine parameter ***cross checks*** and ***panel checks*** in that diverse parameters (suitably buffered) for a common system can be automatically compared on a low frequency background basis.

Any unexpected deviation from these similar parameter values (or previously stored parameter values associated with that plant operating state, called "***signature values***") will be annunciated to immediately alert the operator of a ***potential off-normal condition***. This common historical database will also be of use to technical staff for event diagnosis or for plant optimization analysis activities.

The ***powerful calculation*** capabilities of the CANDU 9 plant display system service computers with access to the ***plant-wide database*** provides selectable output data on a high frequency basis to ensure that ***plant state*** information and ***plant state change*** information is immediately available and available in a format which is discriminatory, recognizable and readable.

GENERAL CONTROL CENTRE DESIGN FEATURES FOR IMPROVED OPERABILITY

Enhanced Data Presentations...continued

One simple example of such an application is the ***continuous calculation*** of the primary heat transport system ***heavy water inventory*** including coolant hold-up volumes.

This routine allows ***small inventory loss annunciations*** to be made very early in an event prior to any significant level changes in the heavy water storage tank or the pressurizer.

The operator can then call-up associated displays and trends (with special scaling applied due to the focus of the alarm) to ***confirm*** the actual heat transport status, leakage rates and operating margin deterioration rates.

The provision of this type of ***early information*** allows a very orderly operator response to abnormal unit conditions with adequate lead times to minimize potential associated consequential damages.

GENERAL CONTROL CENTRE DESIGN FEATURES FOR IMPROVED OPERABILITY

Reduced Workplace Stress

The reduction of operator stress in the CANDU 9 plant operation is another important Control Centre design strategy basis.

This strategy considers fundamental workplace requirements such as:
- providing the ***necessary information*** in the ***correct presentation*** format within the ***needed time context***,
- providing a ***physical*** (heat, light, sound, space) and ***social*** environment (traffic patterns, communication, interactions)
  conducive to the tasks and goals at hand,
- including the recognition of shift ***worker light deprivation*** conditions, and
- providing a ***shift coffee room*** in close proximity to the panel operations area.

COMPUTER BASED HUMAN SYSTEM INTERFACE DESIGN CONSIDERATIONS - The CANDU 9 APPLICATION EXAMPLE

HSI INTRODUCTION

The design of the human-system interfaces (HSI) for CANDU 9 is based on the proven operational features of existing CANDU 6 stations, complemented by the functional HSI enhancements of the more recent Darlington CANDU station as well as improvements allowed by current technology.

The design strategy is to preserve the functionality of the existing control/monitoring/annunciation systems while providing enhancements that result in improved ***operability*** and ***maintenance*** capabilities.

Such considerations as reduced human error opportunities, correct and complete display information sets and information presentation methods and operational state context recognition are included in the design implementation sequence.

An extensive series of Human Factors Engineering ***Design Guides*** has been developed to support process system, process control and control centre design staff to more effectively implement the systematic CANDU 9 design process.

This integrated information will be used to define operational and maintenance information, presentation and annunciation requirements, and then to ***translate these requirements*** into status, diagnostic and control PDS displays.

HSI INTRODUCTION

The CANDU 9 control centre provides plant operations, maintenance and technical staff with improved ***technical surveillance*** and ***predictive maintenance capabilities*** due to the combination of plant wide data integration, systematic parameter cross checking, comprehensive signal degradation detection and dynamic device performance verification tests.

Three design goals have been identified to ensure that the design meets product needs in the areas of ***licensability***, ***operability***, ***maintainability*** as well as reducing the ***capital and OM&A costs.***

- *Safety* - The control centre must be designed to support the operation of the plant safely in all operational states to maintain safety of the public and the facility staff. The control centre must be licensable and be able to maintain licensability over its intended life.

- *Capital Cost* - The control centre should be designed to minimize the cost of design, procurement, construction, and commissioning (including the costs of equipment and schedule).

- *Operability/Maintainability* - The design of the control centre and the design process should:
  1. provide an assignment of functions that effectively utilizes operator or automatic system capabilities to achieve operational objectives,
  2. ensure the availability of plant functions when they are needed,
  3. accommodate the planning and scheduling of maintenance and testing based on plant performance, and permit necessary system/equipment maintenance safely, quickly, and cost-effectively, and
  4. minimize the cost of operating and maintaining the plant.

GENERAL HSI DESIGN FEATURES

The key human systems interface for the CANDU 9 is the VDU based Plant Display System (PDS) which provides utility operations and maintenance staff with a centrally located, integrated control/ monitoring/ diagnostic/ annunciation interface to the plant processes.

These features are provided through a combination of proveness, systematic design with human factors engineering and enhanced operating features which applies ***available*** and ***mature*** technologies to identified design features.

The CANDU 9 design includes a major evolutionary design change from previous CANDUs, the ***separation of the plant control and display/annunciation features*** formerly provided by the central digital control computers (DCC).

This CANDU 9 control/display/ annunciation function separation provides control in the Distributed Control System (DCS) and display/computerised annunciation in the plant display system (PDS).

This strategy allows powerful non-proprietary computers without any practical application ***memory constraints*** or ***execution limits*** to provide extensive control, display, diagnostic and computerised annunciation enhancements within an ***open architecture***.

A further advantage of this design approach is to allow approved and administered ***display and annunciation software changes*** to be implemented during plant operations, without causing any impact upon the plant control software by the inadvertent introduction of control problems ***minimising the extent of necessary software reviews*** and validation checks.

GENERAL HSI DESIGN FEATURES....continued

The following two figures depict the evolution from past display and control practice to the present CANDU 9 design:

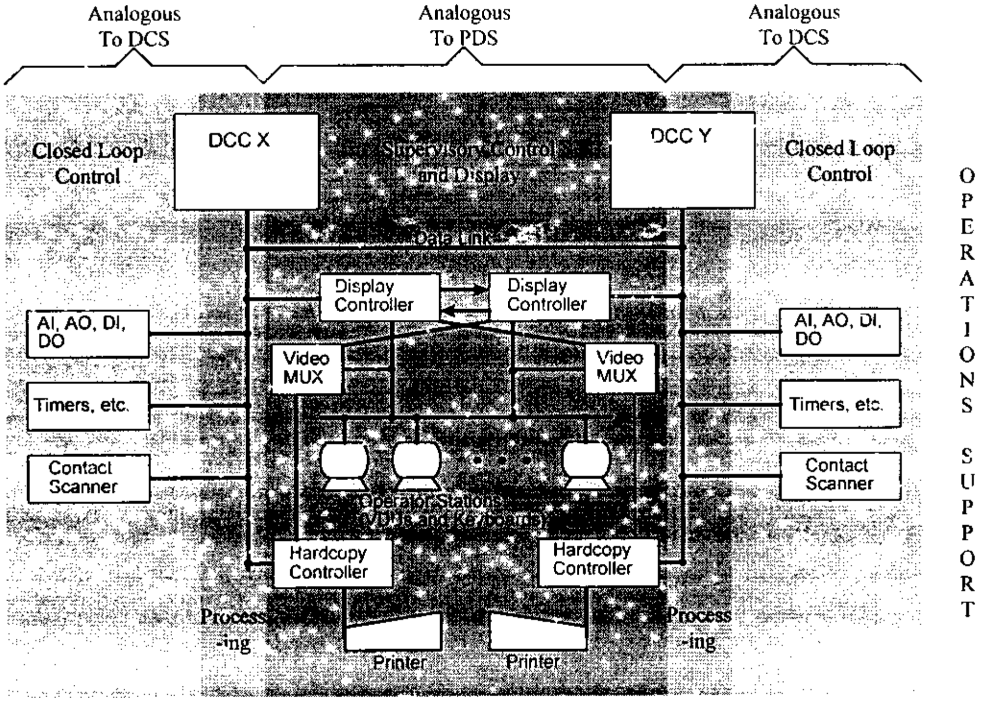
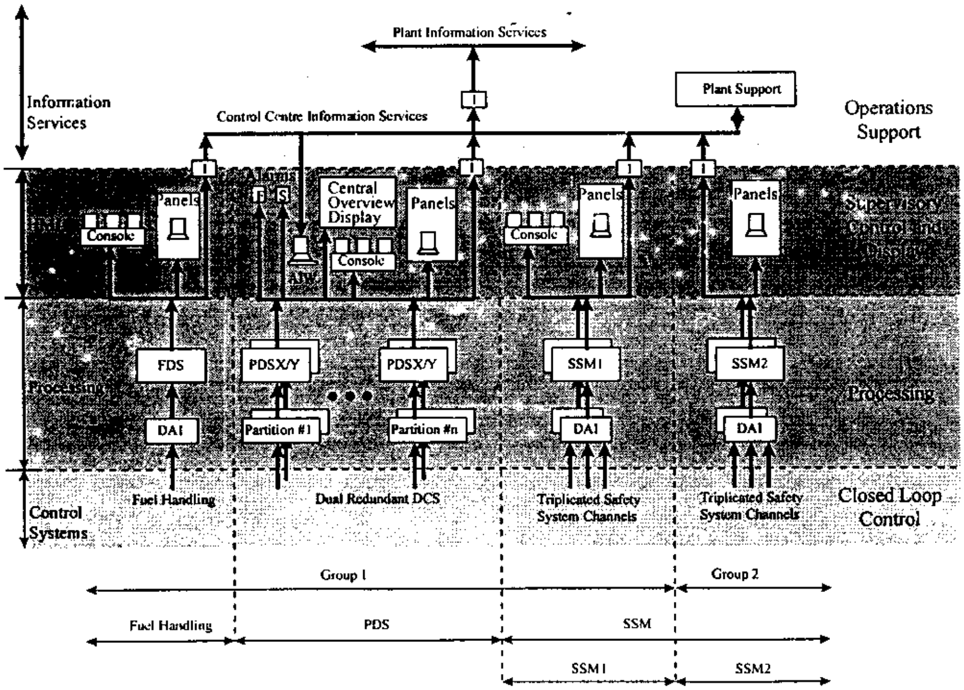


Figure 1: DCC Configuration



*DAI = Data Acquisition and Control System Interface

Figure 2: CANDU 9 HMI Configuration

GENERAL HSI DESIGN FEATURES.......continued

Significant CANDU 9 PDS design features

It is worth considering some of the key features of a display system to better understand the integrated functionality of the final HSI components.

- **Console Displays** The main control room consoles, (main operators console & shift annunciation interrogation console), consists of an integrated display hierarchy combined with user friendly navigational tools which provides efficient and convenient access to all plant data.

- **Panel VDU Displays** Panel PDS VDU's are provided to primarily present overview displays of the plant system(s) allocated to that panel area. However, alternate (non-default) displays can be invoked by operator choice with no display restrictions applied.

- **Plant-wide parameter signal database** A common plant-wide database (with necessary signal buffering to ensure signal integrity while preventing fault propogation) is provided to allow systematic inter-system data comparisons, monitoring, diagnostics, displays and computerised annunciation.

- **Extensive cross checking capability** To check similar process parameters amongst themselves, with the buffered, counterpart safety system parameters and as well as with historically stored unit state dependent 'signature' values obtained from previous known steady state conditions.

Significant CANDU 9 PDS design features.......continued

- **Powerful and flexible annunciation system** To provide multiple (and easily recognized) alarm levels with alarm filtering, prioritising and interrogation to facilitate staff recognition of events, event conditions and the resultant plant state.

- **Predictive Maintenance Capability** To provide the capability to minimise unplanned outages due to unrecognized or unanticipated plant process equipment failures.

- **Computer 'System Health' Displays** Displays provided so that the occurrence and location of a faulted computer device can immediately be confirmed by the operator/maintainer so that problems associated with the computer system are easily recognized and discriminated from problems associated with the application system.

- **Redundancy Features** Redundancy for all major functional parts of the PDS will allow continued operation in the event of a single failed hardware or software component

- **Commissioning/Maintenance support** The PDS will provide flexible access to historical and structured plant data for plant commissioning or maintenance outage planning and implementation uses.

Console Displays

The CANDU 9 control centre design includes a seated ***main operator console*** (MOC) located in front of the NSSS and BOP main control room panels with a shift interrogation console (SIC), which is a stand-up console located behind the MOC.

Three PDS VDUs mounted on the MOC are used to display current or short term historical ***operational or annunciation data***, and are also used for most power range ***operator control actions***. Each of these VDU display workstations are controlled from their own function keyboard and trackball allowing optimum flexibility in their use.

These VDUs can be used to display any ***combination of data*** , in a user friendly and convenient manner, from the various DCS partitions, PDS , plant logged data interfaces, annunciation information, calculated values, and values transferred from the Fuel Handling Display System (FDS) and the Safety System Monitors (SSM).

Note that the intention here is to access the buffered SSM data for comparison purposes only, the SSM displays will not be replicated within PDS.

The SIC is functionally identical to the MOC, with the exception that control actions from this console are normally inhibited. ***Back-up control*** capabilities at the SIC can be enabled by an ***annunciated keyswitch***, allowing this console to act as a full function back-up to the MOC in case that console is unavailable.

A fourth VDU display is also located on each of these consoles. This VDU, which is connected to the control centre information services, can be used for ***alarm interrogation***, and to display any data in medium term historical data storage, and various plant reports and logs. This VDU can also display current or historical data received from other plant systems such as chemistry lab data, meteorological data, radiological data, site surveys, etc.

Panel VDU Displays

The design mission, or default status of the ***panel VDU*** displays is to normally present detailed or overview displays of the plant system(s) allocated to that panel area. However, any panel VDU is capable of displaying any operator selected data from the PDS data base, in the same manner as the console VDU displays are able to.

A large, centrally located VDU is provided on the Main Control Room (MCR) panel 07 and is referred to as the ***central overview display***. The central overview display facilitates increased operating staff ***awareness of plant state*** and event conditions.

The centrally located, simplified overview display indicates the status of the major station systems so that the ***general state*** of the plant is immediately recognised by operating staff upon first visual scan (e.g., following first entry to the MCR or glancing up from the MOC).

Large scale indications ensure ***readability*** by staff in the control room from a distance of ten meters away from the panel mounted screen. Such conditions as power range operation, energy mismatches, shutdown hot, shutdown cold, guaranteed shutdown and the associated transition states are emphasised and presented in an obvious manner.

The overview display presents the unit status in a ***simple format*** so that comprehensive unit awareness is ***immediate and uncomplicated*** for operating staff who are able to concentrate on key indicators without 'tunnel vision' limitations which can occur with VDU monitoring.

Panel VDU Displays....continued

It is important that operating staff always maintain a ***'heads-up'*** attitude when in the operating area to avoid narrowly focussing on one issue with the possible opportunity to miss a subsequent or variant issue occurence.

Certain critical or important panel VDU displays form an integral part of the data gathering functionality from the ***Distributed Control System*** (or DCS) and/or plant data logging interfaces.

In case of a ***Plant Display System*** (or PDS) communication failure, which makes it impossible to communicate over the main PDS local area network (LAN(s)) thus rendering the MOC and SIC inoperable, these panel displays, which are interfaced directly to the DCS or interface stations, can continue to operate, but will only be able to display that data which is obtained from that connected interface station.

The operator will still be able to monitor and control each major plant system in this fashion from the respective system panel VDU displays allowing maintenance time for the full integrated PDS functionality to be restored.

Plant-wide Parameter Signal Database

The Plant Display System design provides one ***common plant-wide*** parameter database so that all safety (suitably buffered) and production plant signals are accessible for monitoring, checking, display and annunciation much more extensively than was possible in previous designs.

This feature can largely unload the operators from routine parameter ***cross comparisons*** and ***panel checks*** in that diverse parameters for a system can be automatically compared on a ***low frequency*** background basis (that is low frequency for a computer - say every 20 or 30 seconds, which would be impossible for a human to achieve).

However, the operational strategy would still include ***routine panel checks*** and comparisons by the operator as an ***independent data confirmation*** means. The signals input to this common database will be suitably buffered (datawise and electrically) so that the database can not present a ***common cause failure*** source.

In this manner, signals from ***safety*** systems, ***process*** systems, plant ***electrical*** and so forth can be assessed for event reconstruction or analysis. This common database information will also be available upon request from a higher level plant LAN for use by plant technical staff for event ***diagnosis***, ***root cause*** assessments or for plant ***optimisation*** analysis activities.

Access to this plant-wide data for service calculation purposes will allow extensive on-line or off-line support for such applications as ***system chemical controls***, ***heat sink management*** and electrical ***load management*** activities.

NAVIGATION

Operability is further enhanced by a functional display system ***navigation*** philosophy which facilitates the operator's task of ***accessing and assimilating*** necessary plant information from the plant-wide database.

Due design consideration has been given to the ***logical and relational*** parameters of interfacing systems so that operators can easily move laterally or vertically through the ***display hierarchy*** to call-up the desired display.

The operator can navigate from plant overview to system to parameter/ device levels directly as well as moving from system to system, from associated device to device or from associated parameter to parameter.

Display ***action points*** are presented as device icons, menus, flowsheet connectors, parameters or action buttons to accommodate operator personal preferences.

The utilisation of a flexible navigation system for the plant display system allows custom information displays to be accessed in a simple, direct, convenient and logical manner by operations ,maintenance and technical staff.

Data items associated with ***out-of-service*** equipment or systems, shall be appropriately flagged in the database, based on work order information entered by operations/ maintenance personnel when equipment is taken out of service or returned to service.

This information will be presented by the plant display system to ensure that signal quality is appropriately maintained, with respect to out of service equipment, in the database. It shall be obvious when viewing these signals on VDU displays that the equipment is out of service through the use of a special tag, graphic symbol or icon. The display of these signals is clear and unambiguous on all VDU displays.

Extensive Cross Checking

The CANDU 9 common database design provides plant maintenance and technical staff with an improved technical surveillance and predictive maintenance capability due to the combination of plant wide data integration, systematic parameter cross checking, comprehensive signal degradation detection and dynamic device performance verification tests.

Note that this approach does not replace the existing manual practices of call-ups and shiftly panel checks. Rather, this approach supplements the manual activities to enhance the composite knowledge of the station components and unit status.

Any unexpected deviations (based on ***magnitudes*** and/or ***frequencies*** with selectable, tuneable values) of similar parameter values (or current values from previously stored parameter values associated with that plant operating state, called "***signature values***") can be configured to annunciate immediately alerting the operator, or maintainer as appropriate, of a ***potential off-normal condition***.

This extensive cross checking of similar process parameters amongst themselves, with the counterpart safety system parameters (suitably buffered) and as well as with 'signature' values obtained from known steady state conditions, detects ***apparently minor*** but ***potentially significant*** parameter signal ***degradations*** or ***deviations*** prior to failure consequences.

The ***extensive calculation*** capabilities of the plant display system service computers with access to the ***plant-wide database*** provides selectable output data on a high frequency basis to ensure that ***plant state*** information and ***plant state change*** information is immediately available and available in a format which is discriminatory, recognisable and readable.

The provision of this type of early information allows very orderly station staff responses to impending abnormal unit conditions with ***adequate lead times*** for maintenance or operations tasks to minimise the potential associated outage times or consequential damages.

REPORT GENERATION

Immediate ***follow-up reports*** summarising the parameter discrepancies and the extent of the variances can be produced automatically to facilitate maintenance tasks and/or alternate operation strategies.

Configurable report generation allows operations and maintenance personnel to monitor and retain a permanent record of plant and equipment status.

Off-line analysis of these reports will enable plant personal to observe any measurable degradation of equipment or process parameters (that may be very difficult for on operator to notice on a day by day gradual change basis) well in advance of potential failure thereby avoiding plant outages.

Free format configuration capabilities allow all database points (current data, historical data, calculated data, etc.) to be included in the report specification.

Page layouts including titles, time, date, operator or maintainer name and so forth can be customised to meet any foreseeable formatting requirements. Printing of reports can be periodically scheduled or initiated on demand. The types of reports currently anticipated include:

- alarm summaries
- station logs (e.g. shift logs)
- event reports
- calibration reports
- test reports
- predictive/anticipatory reports
- historical data reports
- maintenance recommendation reports

Powerful and Flexible Annunciation System

The CANDU 9 computerised annunciation system has been designed to alert the operators of ***potential off-normal*** conditions, to clearly indicate the ***plant state*** and ***system event*** occurrences while providing a fast, user friendly procedural action follow-up aid.

Two centrally located, large screen VDUs are provided for computerised annunciation purposes. One screen provides unit ***state change*** alarms while the second provides ***fault message*** annunciations.

Multiple ***prioritised*** alarms with multiple setpoints (e.g. first warning, significant deviation, imminent actions, etc.) with pre-set ***filtering*** features provides extensive annunciation capabilities.

Combining the comprehensive ***plant-wide parameter database*** with ***powerful computer processing*** and the station ***operating procedures database*** provides the opportunity to create a unique annunciation system.

Adequate information is available to assess the plant and system state for a wide variety of conditions. A considerable portion of the event diagnosis that is completed during event evaluation and recognition for annunciation processing allows the option of high confidence action ***operating strategy entry point recommendations*** to be made.

As well, this feature provides data compilation that can be used to ***assess device performance*** and ***parameter validity*** when fed into a ***maintenance diagnostic analysis***.

This reliable, user friendly and powerful annunciation system with alarm filtering, prioritising and ***interrogation*** features facilitates the recognition of events, plant state and the corresponding required corrective procedural actions by operations or maintenance staff.

Predictive Maintenance

The CANDU 9 Control Centre design provides improved maintenance/diagnostic checks to give early information with adequate lead time to allow systematic issue resolution prior to unit operability impact.

By applying a combination of the previously discussed features of the PDS (e.g. plant-wide data integration, systematic parameter cross-checking, comprehensive signal degradation detection and dynamic device performance verification tests), the PDS can provide plant maintenance and technical staff with the capability for improved ***technical surveillance*** and ***predictive maintenance***.

For example, the annunciation and documentation of an ***apparently minor*** signal degradation allows the follow-up implementation of a proactive maintenance and operations strategy well before unit production goals are challenged so as to be able to maintain the desired ***plant operating margins***.

The PDS service computers have ***powerful calculation*** capabilities and, when using values from the plant-wide database, can provide immediate recognisable and readable output data on ***plant state information*** and apparently minor ***parameter change information***.

Historical data storage retrieval (HDSR) will provide operations and maintenance personnel with up to a year's worth of data which can be used in various report and display formats.

Mathematical and statistical ***analysis*** can be performed on this data, identifying possible ***process trends***, changes in equipment performance or ***status***, recording ***duty cycles*** data for equipment, etc. This data will be periodically distributed across a higher level plant LAN which allows further off-line analysis of the plant data.

Predictive Maintenance....continued

Automatically generated ***Maintenance Recommendation Reports*** (MRRs) can also be prepared on a scheduled basis or can be initiated on ***quantity*** or ***severity*** of the apparent discrepancies.

This continual computerised plant data scrutiny can provide a reduction in station staff work load for system surveillance activities while ***improving the quality*** of the surveillance completed and ***minimising the time*** needed to produce the related follow-up reports.

Providing access to the plant-wide database for diagnosis purposes allows a structured evaluation of relational data sets to facilitate the identification of, apparently relatively minor performance degradations.

This type of data review involves:

- comparing key device parameters against preset tunable limits,
- checking values for similar devices installed in like applications,
- checking parameters against inference values, and
- checking average values against device 'signature' values previously stored in the HDSR facility for that particular plant operating state (Full Power, Zero Power Hot, Cold Shutdown State, etc.).

Identified off-specification values initiate detailed annunciation messages for the maintainer and/or operator depending upon the perceived degradation importance. This occurrence is also archived for future assessment by operators, maintainers or technical support staff.

Predictive Maintenance Review Considerations

A simple example will assist in demonstrating this point. Checking device parameter values against preset tuneable limits is the traditional alarm concept such that once the measured variable exceeds a defined threshold, an ***exception state*** is identified.

Using the example of a level control valve, if the ***valve position*** should differ (absolute value) from the ***characterised control*** signal , or the characterised valve position from the resultant ***flow***, or both, by more than a tuneable preset percent value (W%), then a ***degradation condition*** exists (i.e. dc#1) and can be annunciated.

This discrepancy would be logged in the HDSR database in time relation to all other plant parameters for future evaluation.

Checking values for similar devices installed in like applications provides a ***cross-check*** which demonstrates that this particular device is not performing differently from its peers.

Continuing with the level control valve example, one valve position can be compared to the ***average position of all similar valves*** , say boiler level valves, so that if this valve position differs(absolute value) from the average by more than a tuneable preset percent value (X%), then another degradation condition exists (i.e. dc#2) and could also be annunciated.

Checking parameters against ***inference values*** provides a gross check that this particular device is performing as expected for prevailing operating conditions.

Predictive Maintenance Review Considerations....continued

Further exploiting the level control valve example, the approximate valve position can be calculated as a function of a related parameter, say boiler level valve position as a function of ***steam flow***.

If the actual valve position differs (absolute value) from the inferred value by more than a tuneable preset percent value (Y%), then another degradation condition exists (i.e. dc#3) and could be annunciated.

Checking parameters against previously stored historical 'signature' values for that parameter at that plant operating state provides a unique discrepancy check that this particular device ***is performing as it had previously*** (***or not***) for the prevailing operating conditions.

Utilising the level control valve example one last time, if the present valve position differs (absolute value) from the ***'signature'*** value (i.e. previously stored historical value) by more than a tuneable preset percent value (Z%), then another degradation condition exists (ie dc#4) and could be annunciated.

Having the opportunity to consider four, in this example, separate alarm inputs provides ***high confidence*** that a problem does exist and that corrective action should be taken.

Individual experience would indicate the ***trigger values*** (i.e. action points) that should be used to initiate ***non-nuisance alarms*** and the minimum degradation condition alarm combination upon which operator or maintainer action should be based.

Predictive Maintenance Review Considerations....continued

In this simple example, there were four degradation condition alarm cases (dc#1-4) which when considered could be assessed to indicate such condition changes as:

- ***drifted positioner calibration***, ***air supply*** problems,
- ***valve plug*** installation problems,
- bent ***valve stems***,
- actuator ***diaphragm leaks***,
- pneumatic ***transducer calibration*** drift,
- ***pump discharge pressure*** control problems,
- pump ***recirculation control*** problems,
- gross ***heat exchange/balance shifts***,
- control signal ***ground faults***,
- changes in piping ***hydraulic coupling***,
- ***seat erosion*** problems and so forth.

Certainly in this example, any one of the degradation conditions should be investigated, perhaps each with different time frames, since any of these discrepancies is not immediately justifiable and provides a solid indication that something has changed in the plant (e.g. not achieving expected flow for a given valve position) which has altered the previous known balanced condition.

This design feature provides improved maintenance/diagnostic checks to give early information with adequate lead time to allow systematic issue resolution prior to unit operability impact.

Computer 'System Health' Displays

The CANDU 9 Control Centre computer systems (i.e. control, plant display, testing, communications, etc.) are provided with ***'system health'*** displays so that the ***occurrence*** and ***location*** of a faulted control or display computer or communications device can immediately be confirmed by the operator.

For example, if a ***redundant*** processor failed, the ***standby*** processor would assume control and the ***master/standby transfer*** would be annunciated on both the operation and the maintenance terminals.

The background diagnostics routine would detect the processor failure and set a diagnostic status word linked to the processor address identifying both the ***device*** and the ***apparent fault***.

The details of this diagnosis which can be accessed from the maintenance terminal are not of interest to the operator. However, the faulted device address is scanned by the 'system health' routine to ***identify and indicate*** to the operator that the particular failed device is now unavailable.

In human terms, once the initial master/ standby transfer alarm annunciates, the operator could call-up the associated 'system health' display to identify that the control/display processor for a specific control segment has failed.

The provision of maintenance diagnostic features providing control and display system information which facilitates the rapid ***recognition***, ***identification***, ***location, confirmation*** and ***correction*** of system faults reduces the mean time to repair (MTTR) for that system.

In this manner, plant display system problems are ***immediately recognised*** (e.g. not masked as a process system problem) facilitating the implementation of ***alternate operating strategies*** and the achievement of low MTTR targets while minimising the chance of unplanned outages.

Redundancy Features

Numerous operator display system redundancy measures have been provided to ensure that the PDS operates reliably.

First of all, the PDS is divided into two major parts, a critical 'lower' layer which provides all ***essential*** operator functions such as annunciation, display and control entry, and a non-critical 'upper' layer which performs ***non-essential*** functions which may be unavailable for some period of time without adversely affecting the safe operation of the plant.

All equipment performing essential functions is redundant. Some examples of this PDS redundancy are as follows:

- Two interfaces are provided to each DCS partition.
- Two fully functional consoles are provided in the main control room, the MOC and the SIC
- Panel VDU control/operation strategy: In case of unavailability of the MOC and SIC, (perhaps due to some kind of global PDS LAN communication failure), the VDUs on the main control room panels can be used to replace the failed console functionality.
- Critical Communication components are dual redundant
- Support calculations are performed in dual redundant processors. This includes the processing related to computerised annunciation, as well as general plant calculations.
- Dual power supplies, either ***odd*** or ***even***, for redundant components to ensure that loss of any one channel of electrical power will not disable the entire PDS.

The PDS system is designed for ***graceful degradation***. In the highly unlikely event that the main PDS should ***'collapse'*** (e.g. to lose all communication capability amongst the various PDS components), there is sufficient functionality provided by the panel VDU displays to guarantee continued individual basic monitoring and control capability for those interfaces connected directly with the major station systems.

Commissioning/Maintenance support

The Plant Display System design provides the capability for ***connecting portable display VDU's*** temporarily, providing additional convenient access to plant data for operators or technical staff.

The primary purpose for these ***temporary displays*** is to aid operating staff during commissioning and other busy times (e.g. planned plant maintenance outages), when additional users in the control room need access to plant information or the operator may be in a non-standard operating location (i.e. at one control panel) for an extended period of time .

These portable display monitors can be used for many functions, such as viewing of alarm data, point data, lists, procedures, reports and other text or graphical information.

The portable monitor (i.e. ***roving*** VDU) is connected to the non-critical 'upper' level which restricts its role to monitoring; no control interactions are possible.

This arrangement minimises any risk to the critical layer of PDS, either physical (e.g. not disturbing the PDS LAN when the mobile station is connected or disconnected) or functional (e.g. modifying control parameters).

The latter is important because the display may be out of the main operator's line of view, and thus beyond his or her direct control.

The control centre design will provide for a number of connections for this type of roving station, at various MCR panels as well as at the control consoles, maximising the location flexibility, and making provision for more than one such portable display to be connected at one time, as necessary.