CANDU 9 OPERATOR PLANT DISPLAY SYSTEM

R. Trueman and A. Webster

Atomic Energy of Canada Limited
2251 Speakman Drive,
Mississauga, Ontario,
Canada, L5K 1B2

M.J. MacBeth

Institute for Advanced Engineering/Ajou University
Energy Systems Research Center
Yongin, Republic of Korea

ABSTRACT

To meet evolving client and regulatory needs, AECL has adopted an evolutionary approach to the design of the CANDU 9 control centre. That is, the design incorporates feedback from existing stations, reflects the growing diversity in the roles and responsibilities of the operating staff, and reduces costs associated with plant capital and operations, maintenance and administration (OM&A), through the appropriate introduction of new technologies. Underlying this approach is a refined engineering design process that cost-effectively integrates operational feedback and human factors engineering to define the operating staff information and information presentation requirements. Based on this approach, the CANDU 9 control centre will provide utility operating staff with the means to achieve improved operations and reduced OM&A costs. One of the design features that will contribute to the improved operational capabilities of the control centre is a new Plant Display System (PDS) that is separate from the digital control system. The PDS will be used to implement non-safety panel, and console video display systems within the CANDU 9 main control room (MCR)[1].

This paper presents a detailed description of the CANDU 9 Plant Display System and features that provide increased operational capabilities.

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

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.

As part of the CANDU 9 design process, a physical, full-scale mock-up of the control centre panels and consoles, including all PDS computers and peripherals, is being used for conceptual evaluation, rapid prototyping, design decision-making, and for the verification and validation of the design features, displays and operator interactions[3]. The functionality of the simulation supported control centre mock-up provides a dynamic project design mechanism for the on-going verification and validation activities. The mock-up is used extensively to verify the design of the PDS including, display attributes, display configurations, display completeness and functionality within an operational context, display standardization, navigation scheme, and the integration of the computerized annunciation messages with other annunciation means.

ADVANCED DESIGN FEATURES

The CANDU 9 PDS 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 function separation provides control in the Distributed Control System (DCS)[4] and display/computerised annunciation in the plant display system (PDS). This strategy allows powerful non-proprietary computers without 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. The following two figures depict the evolution from past practice to the present CANDU 9 design:

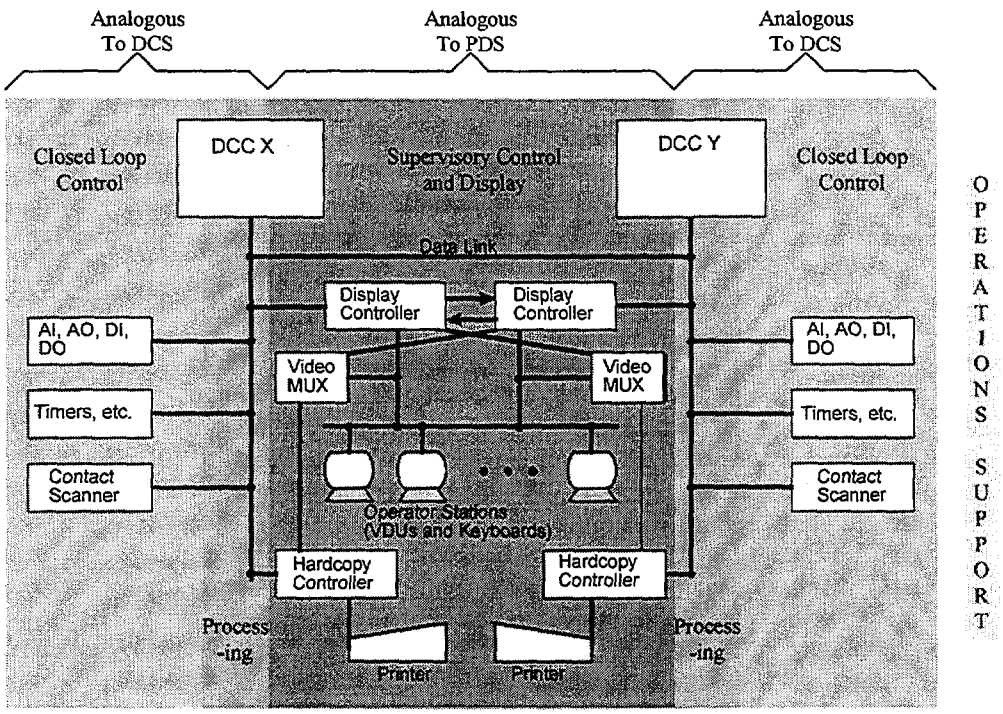

Figure 1: DCC Configuration

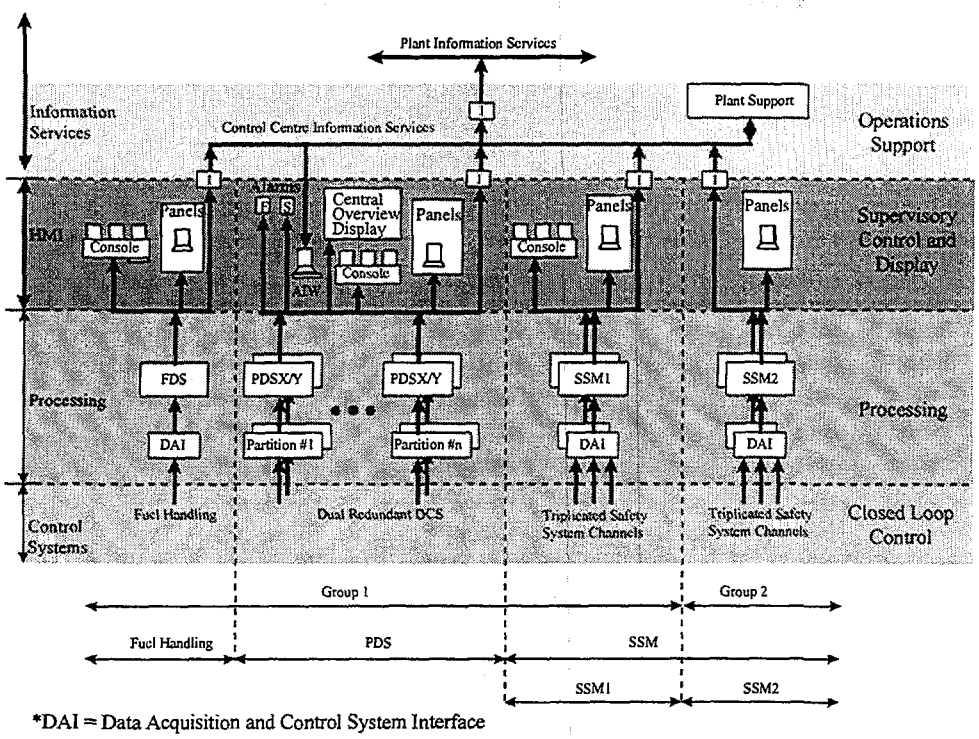

Figure 2: CANDU 9 HMI Configuration

Significant CANDU 9 PDS design features include:

- Console Displays: The main control room consoles, (main operators console & shift interrogation console), consists of an integrated display hierarchy combined with user friendly navigational tools which provides efficient access to all plant data.
- Panel VDU Displays: Panel PDS VDU's are provided to present overview displays of the plant system(s) allocated to that panel area.
- Plant-wide parameter signal database: A common plant-wide database (with necessary signal buffering) for systematic inter-system 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 unit state dependent 'signature' values obtained from previous known steady state conditions.
- Powerful and flexible annunciation system: To provide multiple alarm levels with alarm filtering, prioritising and interrogation to facilitate staff recognition of events and plant state.
- Predictive Maintenance Capability: To provide the capability to minimise unplanned outages due to 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.
- Redundancy Features: Redundancy for all major functional parts of the PDS will allow continued operation in the event of a failed hardware or software component
- Commissioning/Maintenance support: The PDS will provide flexible access to plant data for plant commissioning or maintenance outage uses

Console Displays

The CANDU 9 control centre design includes a 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[1] . Three PDS VDUs mounted on the MOC are used to display current or short term historical 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 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.

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 forth 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 displays is to normally present overview displays of the plant system(s) allocated to that panel area. However, each panel VDU is capable of displaying any data in the PDS data base, just like the console VDU displays.

A large centrally located VDU is provided on MCR panel 07 and is referred to as the central overview display. The central overview display facilitates increased operating staff awareness of plant state. The centrally located 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 operating at power, energy mismatches, shutdown hot, shutdown cold, guaranteed shutdown and the associated transition states will be 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.

Certain critical panel VDU displays form an integral part of the data gathering functionality from the DCS and/or plant data logging interfaces. In case of a PDS communication failure, which makes it impossible to communicate over the main PDS 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 data obtained from that connected interface station. The operator will still be able to monitor and control each major plant systems in this fashion from the respective system panel VDU displays allowing time for full integrated PDS functionality to be restored.

Plant-wide Parameter Signal Database

The PDS 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. 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 database will be suitably buffered so that the database does 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 on 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 chemical controls, heat sink management and electrical load management activities.

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.

Extensive Cross Checking

Any unexpected deviations (magnitudes and/or frequencies) (i.e. 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. Immediate follow-up reports summarising the parameter discrepancies, occurrence frequency/history and the extent of the variances is produced automatically to facilitate maintenance tasks and/or alternate operation strategies.

The extensive calculation capabilities of the plant display system 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 operator 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.

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 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[5] .

Predictive Maintenance

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 [2]. The PDS design provides the required

device performance data thus allowing for the capability of improved maintenance/diagnostic checks to give early information with adequate lead time to allow systematic issue resolution prior to unit operability impact. 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 design has 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. 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 report.

Computer 'System Health' Displays

The plant display system will be configured with 'system health' routines and displays so that the occurrence and location of a faulted control/display device can immediately be confirmed by the operator or maintainer. 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 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 flag that particular device as 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 and correction of system faults reduces the mean time to repair (MTTR) for that system. The CANDU 9 design strategy is to provide the immediate identification and diagnosis means, for the operator and maintenance staff, for the computer platforms. 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 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 performs all essential operator functions, 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. Examples of this 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, (through some kind of global PDS LAN communication failure), the VDUs on the main control room panels can be used as a replacement console.
- 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. As described in the panel VDU displays section above, if the main PDS should 'collapse', e.g. to lose all communication capability amongst the various PDS

components, there is sufficient functionality in the panel VDU displays to guarantee continued basic monitoring and control capability with the DCS.

Commissioning/Maintenance support

The PDS design provides the capability for connecting portable display VDU's temporarily, providing access to plant data. The primary purpose for these displays is to aid during commissioning and other busy times (e.g. planned plant maintenance outages), when additional users in the control room need access to plant information. These portable display monitors can be used for many functions, such as viewing of alarm data, point data, lists, procedures, reports and other text information.

The portable computer is connected to the non-critical 'upper' level which restricts its role to monitoring; no control is possible. This arrangement minimises any risk to the critical layer of PDS, either physical (e.g. 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 outside his or her direct control.

The control centre design will provide for a number of connections for this type of 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, if necessary. The PDS system is designed to allow these portable display monitor(s) to be freely disconnected and reconnected with no impact on the operating network.

CONCLUSIONS

The advanced CANDU 9 PDS design provides utility operations and maintenance staff with the means to achieve improved operability and maintainability due to the combination of proveness, systematic design with human factors engineering and enhanced operating features which apply available and mature technologies. The presentation of the necessary plant information set and the data presentation methods within a functional environment that addresses operator and maintainer performance goals (e.g. the right information in the necessary format within the needed time frame) ensures the correctness and completeness of the advanced control centre human-system interface design. The successful completion of the extensive pre-project licensing review by the Canadian nuclear regulator provides a high level of confidence that PDS related human factors issues for operations and maintenance will not present any licensing barriers for CANDU 9 stations. The CANDU 9 PDS design concept can also be applied to older stations for retrofit purposes.

The enhanced design features of the CANDU 9 operator plant display system will be a significant contributor to the safe, effective and efficient operation of future CANDU power plants.

REFERENCES

1. M.J. MacBeth and N.M. Ichiyen, "Advanced CANDU Control Centre", Proceedings of the 5th International Topical Meeting on Nuclear Thermal Hydraulics, Operations, & Safety, Beijing, China, 1997 April.
2. A. Webster, R. Trueman and M.J. MacBeth, "The CANDU 9 Control Centre - Inherent Design for Predictive Maintenance", Proceedings of the CANDU Owners Group CANDU Systems & Equipment Surveillance Programs Workshop, Toronto, Ontario, 1996 November.
3. A. Webster and M.J. MacBeth, "CANDU 9 Control Centre Mockup", Proceedings of the 17th Annual Canadian Nuclear Society Conference, Fredericton, New Brunswick, 1996 June.
4. J. Harber, M. Kattan and M.J. MacBeth, "Distributed Control System for CANDU 9 Nuclear Power Plant", Proceedings of the 17th Annual Canadian Nuclear Society Conference, Fredericton, New Brunswick, 1996 June.
5. M.P. Feher and E.C. Davey, "Annunciation Improvements - Assessment Approaches and Lessons Learned", Proceedings of the American Nuclear Society Meeting, Philadelphia USA, 1995.