Separating Display and Control: A DCC Perspective

T. Rector, H. Storey, L. Yu, J. Carmody, R. Doucet, and D. Trask
Atomic Energy of Canada Limited, Mississauga, Ontario, Canada

Abstract

Digital Computer Controllers (DCCs) have been used in CANDU® plants for over 25 years to perform both control and HMI display/annunciation functions. AECL is now developing new technology to separate display and control in order to take advantage of modern plant display systems such as AECL's Advanced Control Centre Information System (ACCIS) product for existing and new-build CANDU plants.

This paper presents an overview of recent control and display system interface development work performed at AECL to connect such disparate technologies. It includes an examination of key issues; a review of architectural options that use 'commercial off-the-shelf' (COTS) hardware; a discussion of potential migration strategies to DCS-based control systems; and a description of recent AECL control and display system testbed work.

1. Introduction

CANDUs using computerized control have been operating reliably for over 30 years. In fact, the control computers have changed little since then, and the benefits of technological and human performance improvements have not been fully realized. With CANDU life extensions and new builds expected, there is an opportunity to capitalize on technological advancements and significantly improve how information is presented to the operator.

AECL has developed a plant display system (PDS) called the Advanced Control Centre Information System (ACCIS), which can seamlessly interface to DCCs and modern controllers. ACCIS is sufficiently flexible to provide displays that have the same "look and feel" of existing DCC displays, as well as modern interactive displays with higher information density and supervisory control, regardless of the underlying control system. Utilities can phase in changes to minimize licensing and scheduling risks while realizing the benefits of a modern display system for the life of the plant.

This paper includes a brief description of AECL's plant display system and how it can be combined with Varian® or SSCI® DCCs to extend the system's capabilities, add value for operators and system engineers, and provide a path forward for utilities.

There are many interfaces to the DCCs available today that are implemented differently at each reactor site; this new DCC/PDS interface uses modern COTS hardware rather than custom hardware, and provides greater throughput and bidirectional communication. The new interface could potentially be used to transfer the display/annunciation functionality of the DCCs to ACCIS. A possible path forward for migrating from DCCs to a modern distributed control system is also described.

2. ACCIS

ACCIS is a modern Plant Display System (PDS) product designed specifically to meet the requirements of high performance and highly reliable real-time applications that have long product lifecycles (i.e., over 20 years). In particular, ACCIS is developed to meet the human system interface requirements of safety-related systems such as CANDU control and PWR 1E systems. Where possible, ACCIS takes advantage of proven technologies available in industry by integrating COTS hardware and software products into its configuration. ACCIS uses the QNX® real-time operating system for system services. QNX operating system technology has powered the world's most reliable systems in manufacturing and process control for over 25 years. Global industrial leaders depend on QNX Software Systems to help them build reliable, scalable, and high-performance applications in the telecommunications, automotive, medical instrumentation, automation, security, and nuclear industries.

ACCIS is currently installed in two units of the Qinshan CANDU station in China as supplemental plant display systems, providing real-time data to the operators that is received from the DCCs, the Emergency Response Centre, and the reactor shutdown data acquisition system. The implementation includes Critical Safety Parameter Monitoring, advanced annunciation capabilities, operator-configurable displays, historical data archiving and trending, and several overview displays that all contribute to meeting safety and performance goals.

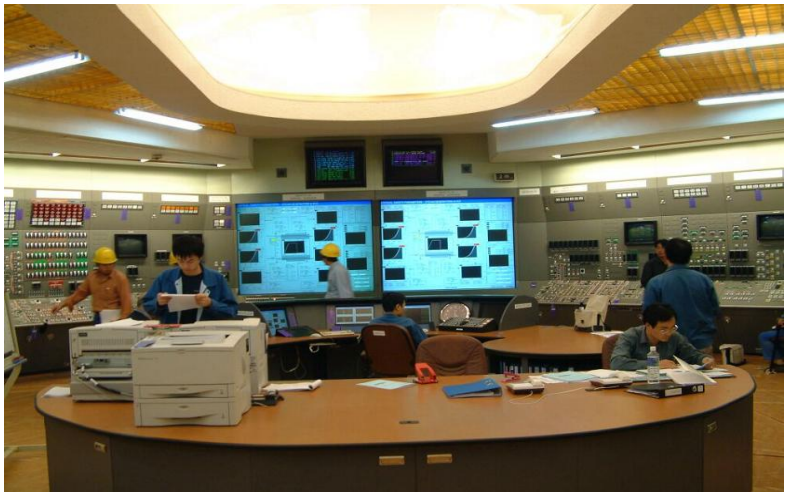

Figure 1 Qinshan CANDU Control Room showing ACCIS Process Displays on Central Projection Screens

Since ACCIS was installed in China in 2002, AECL has continued to invest in its ongoing development and has included ACCIS as the plant display system for all new-build CANDU designs. AECL is pursuing qualification of the product to nuclear-specific International Electrotechnical Commission (IEC) I&C standards for use in safety-related applications. In fact, ACCIS has recently been sought out by a major supplier of safety-critical controllers to be the Human-System Interface (HSI) for their systems.

2.1 ACCIS Features

ACCIS is a collection of display, monitoring, and supervisory control services that can be configured and deployed across a distributed computing environment to meet the needs of a

given application. ACCIS is scalable, as it can be configured to run on a single computer for small applications, and in a distributed multi-node environment for larger, more complex applications. System behaviours are largely configured via data files; this design minimizes the costs associated with the development of custom software and allows the user to have greater control over the behavioural attributes of the system. Configurable aspects of ACCIS include data sampling and storage rates; display appearance and behaviour; alarm annunciation features; and system health check functions.

The ACCIS HMI supports numerous features that enable it to be a highly effective and reliable tool for the operator to monitor and interact with the plant. Some key features are summarized below:

Data Retrieval and Storage

a) It supports the fast, robust retrieval and storage of all real-time data; well over 100,000 samples per second can be obtained and custom calculations can be performed in real-time.
b) Systems can be synchronized to Coordinated Universal Time (UTC) with input signals from the Global Positioning System.
c) For implementations that are interfaced to DCCs, it supports the acquisition of all DCC analog, digital, contact, calculated (DTAB), and alarm data. This data is the basis of the PDS displays, data historians, and the alarm annunciation features included within the PDS. It supports 'Display Demand Functions' (DDFs), which are analogous to DCC Demand Programs
d) It supports short-term, medium-term, and life-of-plant historian functionality.
e) Sequence-of Event monitoring is supported.
f) It has provisions for the acquisition of site meteorological and radiation data from an off-site Emergency Response Centre (ERC) and for the supply of Critical Safety Parameters and other emergency-related parameters to the ERC.

Display Services

a) ACCIS can support a variety of process displays such as those shown in Figure 2 and can also be configured to mimic DCC displays and thus minimize operator retraining.
b) Operator configurable displays including trends, bar charts and digital and analog readouts are supported. Operator configurations can be saved and loaded from any workstation.
c) Real-time and historical trending includes pan, zoom and scaling capabilities with selectable minimum and maximum value traces to identify peaks and valleys.
d) On-line changes to point and alarm data configurations are supported.
e) Remote display capability through TCP/IP is supported.
f) The ACCIS graphical configuration tool is an 'easy-to-use' visual programming environment for the specification of display objects, and supports both process and alarm information to be included on a given display. Display maintenance is facilitated by ACCIS templating capabilities: display objects only need to be updated once, and displays referencing this object are automatically updated.

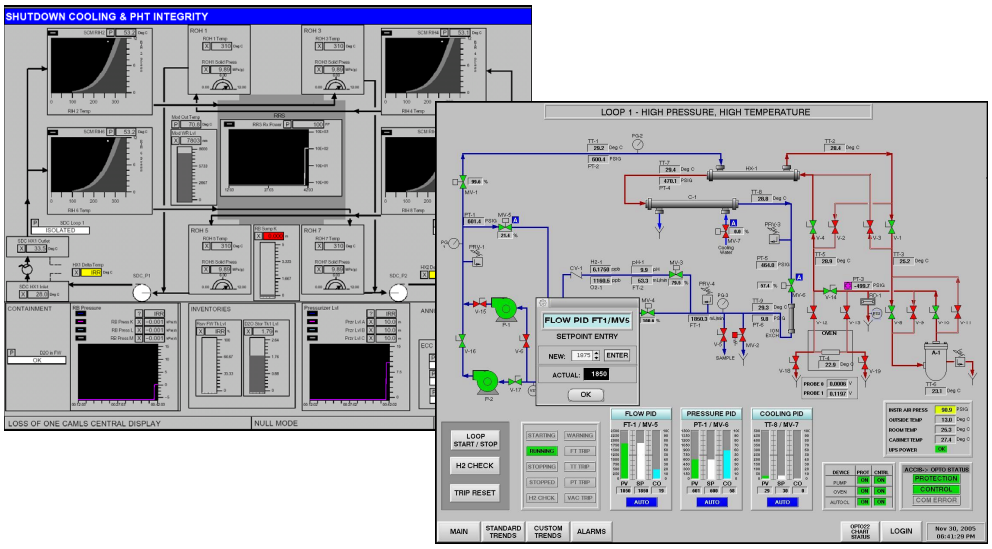

Figure 2 Sample ACCIS Process Displays

Alarm Annunciation

ACCIS includes a sophisticated alarm annunciation system called CAMLS – Computerized Annunciation Message List System that meets the key principles of IEC 62241 (Nuclear power plants – Main control room – Alarm functions and presentation. CAMLS can be configured with basic or advanced functionality. In order to optimize benefit to the operator, it is recommended that some or all of its more advanced features be utilized in order to reduce alarm flooding during upsets, and to make the annunciation system more useable and effective during all aspects of plant operation. Features that are available include:

a) Dynamic prioritization of alarms based on plant operating regions (e.g., an alarm might be high priority at full power steady state but low priority during startup).

b) Separation of alarms about problems (i.e., faults) from alarms about successful changes in plant state (i.e., status). Supporting this distinction removes the need for operators to mentally sort the alarm stream in real-time. During upset conditions when operator workload is high, time is of essence, and reliance on memory should be avoided; dedicated centrally located displays of the fault alarm messages serve to apprise the operator of plant conditions according to urgency. Meanwhile, status (by time) messages provide information regarding process status and current plant configuration. This information is essential for planning and prioritizing the response to impending or current faults.

c) Advanced real-time data suppression algorithms to filter consequence events so that the operator can focus on root-cause events.

d) An alarm interrogation interface that supports sorting, filtering, logging, and printing capabilities, etc.

CAMLS can be configured to duplicate DCC central annunciation, and simultaneously support advanced annunciation features.

3. DCC/PDS Separation using ACCIS (also known as 'ACCIS for a DCC')

The flexibility of the ACCIS PDS allows it to interface with DCCs in a more comprehensive manner than was achieved at Qinshan. The complete separation of display and control requires an additional low-level interface infrastructure that connects the PDS and DCC. The main difference between the Qinshan implementation and the system extension under development is that the Qinshan implementation is display only; the data flow is unidirectional from the DCCs to the PDS. This system extension provides a more interactive structure where most operator interface tasks are handled by ACCIS, rather than by the DCC.

This will form the basis of a versatile product that can be configured to suit the needs of plants with differing requirements. This migration to separate control and operator interface equipment is consistent with the way that virtually all modern DCS products work. The separation has many advantages in that:

a) DCC capabilities can be extended with modern display technology to improve information organization, presentation and interrogation.
b) Display software can be migrated from the DCC to a modern display system in pace with operator training and plant procedures.
c) Once separated, the operator interface, training and procedures can be retained whether or not the DCCs are maintained, replaced or augmented with modern controllers.
d) It could be a major step toward the replacement of DCC infrastructure, since more than 50% of the DCC software is dedicated to human-system interface functionality.
e) The operator interface can be modified as desired using ACCIS configuration tools rather than assembly language coding.
f) Changes made to the operator interface are on a separate system layer, thus any changes introduced by future modifications to the operator interface will not affect the critical control functionality implemented in the DCC.

3.1 Display and Operator Interface Flexibility

As an example of the flexibility of the ACCIS for a DCC system, the following operator interface configurations are possible:

a) Functional Near Equivalence: ACCIS can render versions of the screens currently used. This would require minimal operator retraining in that the displays have the same 'look and feel' as the DCC displays, and generally respond identically to the DCC function keyboard keystroke sequences.
b) Modern: All displays could be updated to have a modern appearance and enhanced capabilities (e.g., display more information, present more choices, incorporate full human factors considerations) while retaining the same basic look and functionality of the original displays. If desired, completely different displays could be created and the entire 'look and feel' of the operator interface could be changed.
c) Hybrid: ACCIS could render some DCC displays unchanged and some displays in a more modern format. Displays could be updated and replaced over a period of time as station needs and operator familiarity dictated. This might be the preferred operational approach because it would minimize station documentation and training changes, and would permit more of a phased upgrade.

DCC and modern versions of the 'Numerical Variables' display, both of which can be generated by ACCIS, are shown in Figure 4.

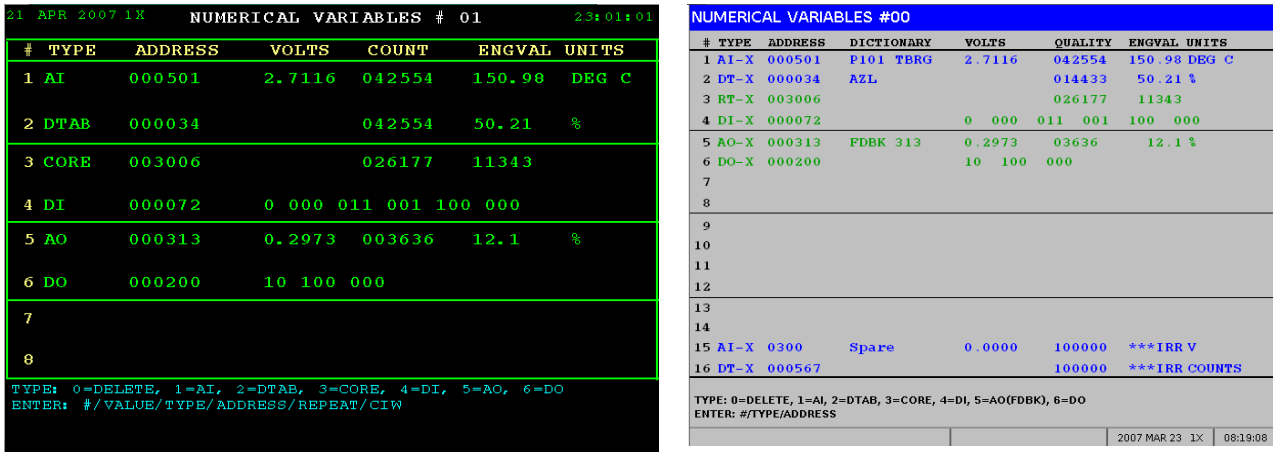

Figure 3 DCC and Modern Numerical Variables Displays

3.2 Design Architecture

The architecture of the ACCIS for a DCC system is depicted in Figure 5. The architecture and components were chosen to address the following important design goals for the system:

a) Redundancy.
   1) Redundant gateways and low-level DCC interface components ensure the same or better redundancy as compared to the DCC to display system interface.
   2) The ACCIS PDS system itself is highly redundant and has redundant and distributed LAN interconnections.

b) Scalability and Configurability.
   1) The system can be scaled from the Qinshan DCC interface that conveys DCC display and alarm data to the PDS, to a fully integrated HMI where almost all DCC software except the reactor and process control programs are removed and ported to the PDS.
   2) Relatively few changes are required to DCC software even with a full ACCIS implementation. Assembly language DCC software can be optionally removed post-commissioning.
   3) The ACCIS PDS can be readily interfaced to new process control and monitoring equipment as a station is modernized and upgraded.
   4) All ACCIS features are configurable via data files as opposed to software changes requiring re-compilation. Full-featured configuration tools support this capability.

c) Reliability, Maintainability and Quality
   1) The QNX operating system is a highly reliable, POSIX-compliant, and mature real-time operating system.
   2) ACCIS is maintainable, and is primarily based on proven, high-volume COTS software from QNX Software Systems Limited that is being qualified for use in safety-related SIL 2 systems.

3) ACCIS is currently being upgraded to comply with IEC 61513 [2] and IEC 62138 [3]. These international standards address the quality assurance requirements for software development in safety-related applications in nuclear power stations. In addition, key aspects of the ACCIS annunciation system meet IEC 62241 [1] – Alarm Functions and Presentation in the Main Control Room of Nuclear Power Plants.

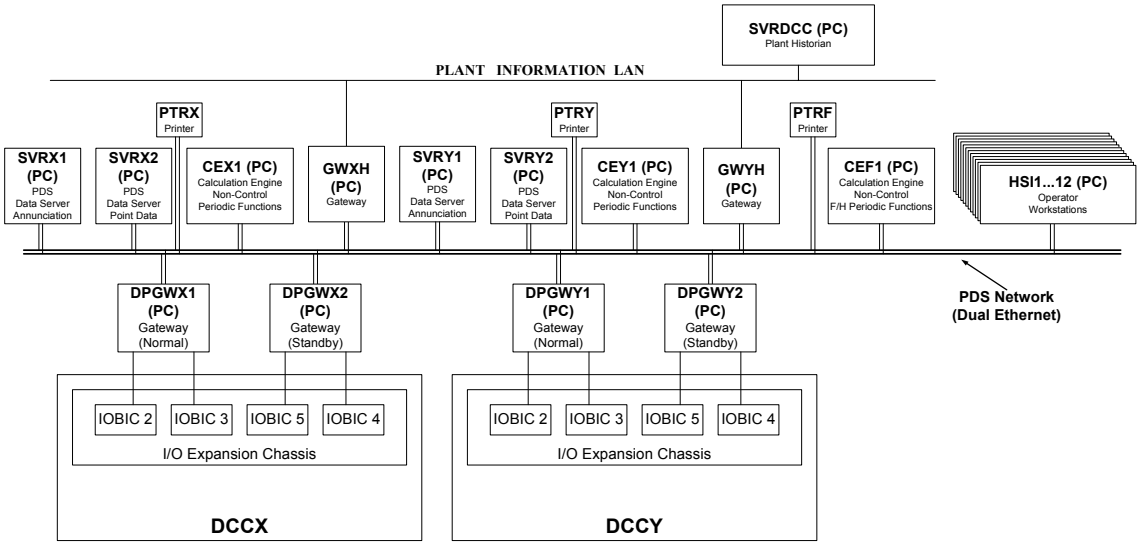

Figure 5 High-Level ACCIS DCC/PDS Hardware Configuration

3.3 Design Components

The following describes some of the major components of the system, most of which are shown in Figure 5:

a) Keyboards (which are connected directly to DCCX and DCCY and are not shown in Figure 5): The system is designed to accept operator input from the original function keyboards with no DCC modifications other than a small patch to the DCC keyboard driver application, to route each 'keypress event' to the PDS. Input could alternatively come from touch-sensitive screens. For DCCZ, inputs can also come from a standard PC keyboard and from test script files.

b) DCC/PDS Gateways: DCC/PDS Gateways (DPGWs) act as firewalls between the DCCs and the PDS. DPGWs accept requests for actions to be performed on the target DCC from the PDS. Gateways validate and prioritize these requests, sending them serially (i.e., one at a time) to the target DCC via standard DCC Input Output Buffered Interlace Controller (IOBIC) cards. The DPGWs forward each DCC Response Packet back to the PDS node that initiated the command.

c) Human-System Interface (HSI) workstations: These are Main Control Room (MCR) operator interfaces. Modern flat panel displays will replace the current VDUs. Obsolete display generation hardware (e.g., RAMTEK, Data Disc) will be replaced by modern industrial grade PC-based equipment that resides in the HSI workstations.

d) Calculation Engines: Calculation engines are tasked with gathering data from Physical/Core or Bulk DCC memory, converting it to engineering units (if applicable), and making it available to the operators. Annunciation messages also pass through the calculation engines. The calculation engines are meant to replace existing DCC software whose function is to read data that other programs have left in memory and display or archive it. The calculation engines will also have the ability to execute non-control periodic programs such as Channel Temperature Monitoring (TPM), and the non-control functions of the Calculation Status Monitor (CSTAT).

e) Data Servers: Data Servers are high performance databases that act as repositories for data needed by operators and/or other PDS resources. Data servers can provide real time data or archived data.

f) Station Printers. These serve the same function as current station printers; to print alarm messages and produce display hardcopies.

g) Plant Historian: The plant historian archives data for routine or post-event analysis. It will be interfaced to the PDS via gateways that have firewall functionalities.

4. Low Level PDS/DCC Interface

Figure 6 shows the interface between the DCC and the PDS via the DPGW. The gateway side of the interface is implemented via a COTS digital I/O card that uses Field Programmable Gate Array (FPGA) technology. The DCC side uses two IOBICs.

One IOBIC is used as a high-speed bidirectional data link between the DPGW and the DCC. Hardware level handshaking is performed using IOBIC sense and pulse lines, rather than via interrupts. This eliminates the possibility of spurious interrupts and simplifies DCC Executive® software modifications.

A DCC composer module named DPA (DCC/PDS Actions) has been developed that is effectively an Application Programming Interface (API) for the DCC. DPA consists of:

a) A root module that performs Cyclical Redundancy Check (CRC) and other error detection tests and calculations for inbound and outbound packets, and

b) A collection of 'overlay' modules that DPA loads from DCC bulk memory to service the particular command specified in a received packet. These overlay modules can be developed as needed to implement the desired level of DCC/PDS integration. DPA uses a simple set of DCC Executive modules to communicate with the gateway computer via the IOBIC.

The gateway/DCC interface uses a master/slave request/reply protocol. The gateway passes Command Packets from PDS nodes, and DPA returns Response Packets containing the requested data and/or confirmation information and error conditions.

The second IOBIC implements DCC keyboard interface logic. The logic in each DCC's keyboard driver detects keypress events and forwards them via the gateway to the appropriate HSI workstation. Separate IOBICs are used to ensure fidelity.

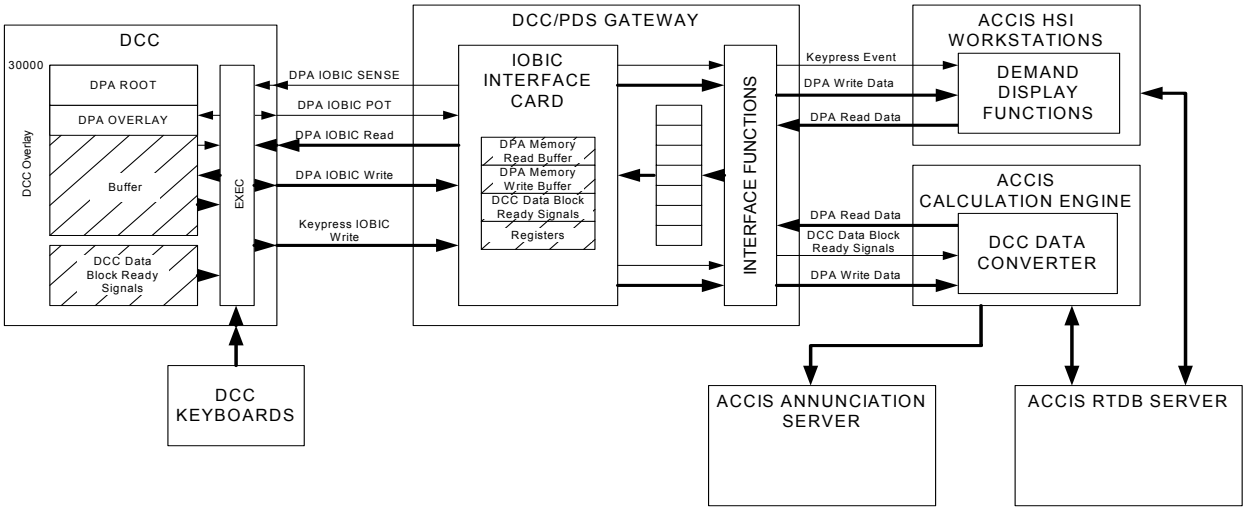

Figure 6 PDS/DCC Interface

5. DCC Software Modifications

A major design goal of the system is to minimize the amount of additional DCC assembly language code that must be written and to avoid any major alterations to the DCC Executive. Most of the DCC software modifications consist of removal of code such as display and routine data gathering services that have been made redundant by the PDS. Table 1 gives an overview of DCC software changes required to implement a system where only the control and data acquisition programs, and the DCC Message Assembler (MESA), and the DCC Executive remain in the DCC.

Table 1 DCC Software Program Functionality Changes

Program Type	Name	Program Description	Change Description
DCC Executive	EXLP	Background DCC Executive Loop	Modify Existing Program
DCC Executive	DPGWT	DPA Driver	New DCC Executive Module
DCC Executive	DPGWB	DCC Datablock Ready Driver	New DCC Executive Module
DCC Executive	KBDRV	Keyboard Driver	Modify Existing Program
–	MESA	Message Assembler	Modify Existing Program
Composer	DPA	DCC/PDS Actions	New Program
DCC Executive	<Various>	All display, printer and DCC-to-DCC data link drivers, etc.	Remove/Make Spare modules
Composer	<Various>	All display and printer-related composer programs	Remove Programs (Optional)
Demand	<Various>	All display-related demand programs	Remove Programs (Optional)
Periodic	<Various>	Most periodic programs without AOs and DOs associated with them	Remove Programs (Optional)

6. Work to Date

Work to date includes the development of the following:

a) DCC software including:

1) The DPA root module, which implements the DCC side of the PDS/DCC interface
2) The DPA DCC Executive modules and requisite DCC patches
3) Several DPA overlay modules

b) DCC/PDS Gateway functionality including:
1) The hardware interface between the gateway I/O card and the DCC IOBICs
2) Low-level gateway functions such as the device driver for the gateway I/O card

c) ACCIS PDS programs with associated display screens
1) A 'Menus' function that implements logic that is similar to the DCC 'Call Any Function' module and that also enables the operator to call up any DCC HSI function from a menu
2) A 'Setpoints' function that enables the operator to modify DCC setpoints
3) A 'Numerical Variables' function that allows the operator to display any combination of real-time database elements which includes all DCC AIs, DIs, AOs, DOs, DTABs, etc. that periodically get transmitted to the PDS via DPA packets. In addition, Numerical Variables has the ability to display any DCC physical/core and bulk memory locations that on demand get selectively transmitted via DPA packets to the real-time database.

In short, much of the low-level and DCC aspects of the system have been developed and specified. This work was undertaken first since it involved the most unknowns. Debugging and testing have been carried out on both the DCCα and DCCβ SSCI-890 machines in AECL Sheridan Park, Mississauga, Ontario.

7. Migration to DCS

The benefits of separating display and control can be realised without migrating to a DCS, however, upgrading to the ACCIS HSI is a great first step when moving from the DCC to a modern Distributed Control System (DCS). One possible strategy for making the transition from DCC to DCS is outlined below:

a) Install ACCIS for a DCC. With a modern flexible HSI in place, other parts of the system can be more easily upgraded. The implementation can initially involve DCC display emulation, where DCC RAMTEK or Data Disc data blocks are rendered by ACCIS.
b) Replace some or all of the DCC Demand and Display programs with ACCIS 'Demand Display Functions'.
c) Migrate all input-only components, such as analog alarm scanning and channel temperature monitoring to ACCIS.
d) Migrate contact scanner functionality to a Sequence-of-Events scanner that is constructed with modern DCS hardware and interfaced to ACCIS. Alternatively an ACCIS interface to the existing contact scanner can be developed.
e) Replace the DCC-based Fuel Handling control system with a separate DCS that is controlled and monitored via ACCIS.
f) Finally, the remaining DCC control functions can be upgraded to a modern DCS.

Many of the changes listed above can be performed while the station is operating at power, but it will be necessary to perform some of the changes during scheduled plant maintenance outages. During this entire process, new HSI displays and other ACCIS components can be generated and

configured to keep pace with changing equipment capabilities. Thus ACCIS provides a flexible core subsystem from which the station can be seamlessly upgraded in a risk-mitigating and phased manner.

8. Conclusion

Work to date has demonstrated a robust and practical low-level PDS/DCC interface using a configurable digital I/O module to interface modern PC hardware to the DCCs via the DCC IOBIC cards. Further, using a configurable, mature and field-tested PDS system such as ACCIS, it is possible to add modern operator interface and display capabilities to the DCCs in a phased manner to any level of integration desired.

9. Acknowledgements

The authors would like to acknowledge Ross A. Judd (AECL) and Dr. G. Alan Hepburn (AECL) for their support and guidance on this project.

10. References

[1] IEC 62241:2004, ISO/IEC Standard – Nuclear power plants – Main control room – Alarm functions and presentation.

[2] IEC 61513:2001, ISO/IEC Standard – Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems.

[3] IEC 62138:2004, ISO/IEC Standard – Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions.