CANDU® Digital Control Computer Upgrade Options

M. S. de Jong, J. de Grosbois and T. Qian
Atomic Energy of Canada Limited
Instrumentation and Control Branch
Chalk River Laboratories
Chalk River, Ontario
K0J 1J0

Abstract

This paper reviews the evolution of Digital Control Computers (DCC) in CANDU power plants to the present day. Much of this evolution has been to meet changing control or display requirements as well as the replacement of obsolete, or old and less reliable technology with better equipment that is now available. The current work at AECL and Canadian utilities to investigate DCC upgrade options, alternatives, and strategies are examined. The dependence of a particular upgrade strategy on the overall plant refurbishment plans are also discussed. Presently, the upgrade options range from replacement of individual obsolete system components, to replacement of the entire DCC hardware without changing the software, to complete replacement of the DCCs with a functionally equivalent system using new control computer equipment and software. Key issues, constraints and objectives associated with these DCC upgrade options are highlighted.

1. INTRODUCTION

CANDU plants have been pioneers in the use of computer control systems for nuclear power plants. Digital Control Computers (DCCs) have been used in all CANDU plants built since the construction of Pickering A in the early 1970s. Initially, IBM 1800 series computers were used in Pickering A. Since then, computers based on the VARIAN V7*x* series architecture have been used in all CANDU plants except Darlington, which uses DCCs based on DEC PDP-11 minicomputers. Although some design and implementation details differ between stations, all plant DCCs have a similar system hardware and software architecture, and a basic common system functionality and behaviour.

The original configuration of the VARIAN-based DCCs is shown in Figure 1.

[1] CANDU® is a registered trademark of AECL.

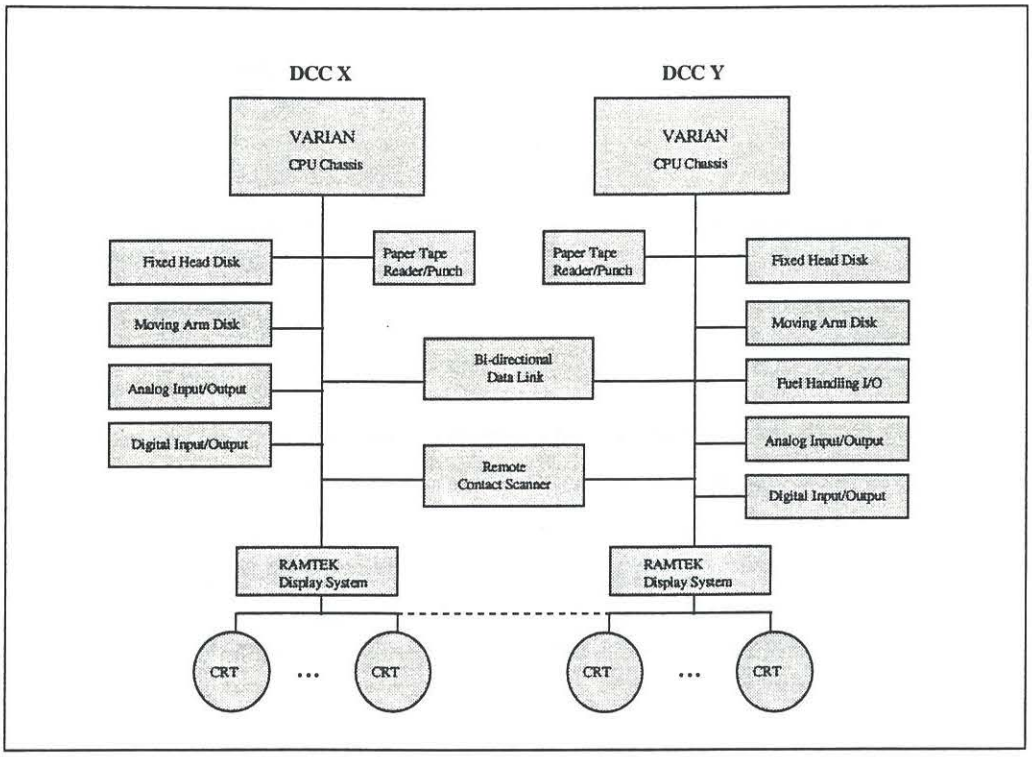

Figure 1: Original DCC System Configuration

Each plant uses two computers (DCCX and DCCY) in a dual-redundant configuration. Each DCC has the same basic complement of peripherals: a paper-tape reader/punch, a fixed-head disk for fast mass storage, a moving-arm disk for removable bulk storage, a range of analog and digital input-output modules and a sophisticated RAMTEK display system with multiple CRT displays. A single fast contact scanner is accessed by both DCCs. In addition, DCCX has additional inputs for flux mapping and channel temperature monitoring, and DCCY has additional inputs and outputs for fuel handling.

The software on these computers consists of a series of separate control programs that run as separate processor tasks, scheduled and co-ordinated to run on regular fixed periods by a system executive. The system executive performs ongoing internal diagnostics that provide hardware and software self-checks and it also monitors and manages all interrupts and general input/output driver routines to service peripheral devices. There are several different control programs that perform the fundamental algorithms for control of the main systems of the nuclear plant, and also display-annunciation programs that provide the operator interface.

The diagnostic programs run to ensure that the other control and display programs are functioning properly. If a malfunction is detected, the diagnostic programs take appropriate action. These actions include re-trying the program or operation that failed, transferring control to the other DCC, shutting down or restarting the DCC, and notifying the operator of any actions taken. A special characteristic of the DCC system configuration is that most of the control and display programs run on both computers at the same time, but only one version of each program controls the outputs associated with that program. If a program controlling the outputs fails, then control of the outputs is transferred automatically to the corresponding program on the other DCC. Thus, the "master-slave" relationship between the two DCC computers can be effectively allocated on a program-by-program basis.

The main control programs that run on the DCCs are the following:

- Reactor Regulating System,

- Steam Generator Pressure Control,
- Unit Power Regulation,
- Steam Generator Level Control,
- Heat Transport Pressure and Inventory Control, and
- Moderator Temperature Control.

The display and annunciation programs provide the main operator interface to the computer system for monitoring and supervision. Operators can request that different reactor status displays be presented on the CRTs by data entry at the dedicated keypads for the CRTs.

The VARIAN computer architecture is a 16-bit minicomputer system that was developed in the early 1970's. The computer performance requirements are very demanding for this older design: each DCC has several thousand analog and digital inputs; some of the control programs must be run several times each second; and each DCC drives several CRT monitors and receives inputs from several keypads. To achieve the necessary performance, some special hardware systems (e.g., the RAMTEK display system) were used to reduce the CPU load, and all software was written in VARIAN assembly language to maximise the execution speed, and minimise the memory requirements.

Over the past twenty years, these computers and their associated programs have demonstrated the high reliability required for CANDU Nuclear Power Plant operation. DCC maintenance staff can also be credited with improving system performance and maintaining acceptable overall hardware failure rates with both corrective and preventative maintenance, despite ageing of DCC systems and their components.

2. WHY UPGRADE?

Despite the success of the original DCC design, a need has arisen to upgrade and refurbish these systems. This need arises from several sources:

- The reliability of some of the original components is not as good as what is now available. Specific improvements can be made that reduce maintenance and improve availability.
- The technology used in these computers is old and in some cases obsolete. Obtaining spares and/or replacement parts is becoming more difficult as time goes on.
- There is evidence of component ageing that is showing up as increased failure rates after many years of operation.
- There has been an evolution in the functional requirements and expectations of plant process control systems driven by a combination of operational experience, industry technology advances, changing regulatory requirements, and more stringent international standards.

Many of the original peripherals were based on electro-mechanical components which tended to break down more frequently than was expected. The paper-tape reader/punch, fixed-head disk, moving-arm disk and the early impact line printers are typical components in this category.

Often compounding any problems with the original equipment is that many of the original components are now obsolete and no longer available. The lifetime of the technology used in the DCC system varies dramatically. For example, many of the TTL-level integrated circuits (ICs) are still available but the disk hardware has been largely unavailable since the end of the 1970s. When equipment or components are obsolete, significant problems can occur in finding suitable qualified replacements when needed. In some cases, the system containing the obsolete components must be completely replaced or re-designed. CAE now offers board level replacements for the original input/output cards, which are a "form, fit, and function" replacement based on a redesign. Obsolete equipment in the DCCs now includes not only most of the original electro-mechanical devices, but also the original VARIAN computers, the core memory, and the RAMTEK display systems.

Ageing of electronic components is generally not a problem provided adequate maintenance is performed and a suitable operating environment is provided. Nevertheless, when the original DCC computer systems where designed and manufactured, appropriate hardware technology was not available which could be demonstrated to last for the required 30 to 40 year lifetime of a plant. Long-term in-service usage with many components and assemblies used in the DCC was limited at the time. Today there is some concern about the possible deterioration of cable

sheathing insulation materials (i.e., certain plastics) used in some plants. Mechanical vibration can also be a possible source of failures of ribbon cables or circuit boards. Leakage currents in some devices tend to increase with age, causing marginal performance or failures after some years. Components in this category include electrolytic capacitors and opto-isolators. Operating the DCCs at elevated temperatures has also been shown to result in more frequent component failures. Thermal expansion and contraction effects due to ambient temperature swings are thought to have caused recurring problems with integrated circuit seating in mounting sockets. Factors such as cooling fan failures, dust accumulation in core memory, dirty fan filters, and repeated power-up cycles have been cited to accelerate ageing and increase component failure rates.

Finally, the expectations of computer-based operator interfaces have changed enormously since the CANDU DCC operator interface was originally designed. This reflects both the increasing use of computerised operator interfaces throughout the industry and the better understanding of how to design these interfaces for safer and more effective use by plant personnel. There now exist international standards and guidelines for the design of operator interfaces, and both customers and regulators are requesting or requiring compliance with these standards. For example, the ongoing development of the CAMLS (CANDU Advanced Message List System) system by COG, and the ACCIS (Advanced Control Centre Information System) plant display system for CANDU 9, indicate the direction in which present and future operator interfaces are evolving. Meeting the demands for this increased functionality in the existing DCCs will push the design limits of the hardware and software.

3. INFRASTRUCTURE FOR UPGRADES

Accurate design basis documentation, good configuration management tools and processes, suitable hardware and software development tools, and an effective maintenance program are essential before considering any major upgrade. Plant operators must have complete knowledge of the present state of the equipment, its past maintenance history, and effective tools and test environments to verify and validate any system changes. Only in these circumstances can an effective upgrade strategy be planned.

At present, the hardware configuration is well known. However, it is important to have as complete a history of hardware failures and changes as possible. Over the long term, this history permits identification of particular items that may be failing more frequently, or require more maintenance than expected. The effectiveness of any changes to the design or to maintenance procedures to address these problems can also be determined over a period of time. A current COG work project is examining the maintenance, reliability and upgrade history of all Canadian CANDU plants that use the VARIAN-based DCCs to identify any specific cost-effective incremental upgrades, design enhancements, or maintenance procedures.

The DCC software presents a general challenge to plants considering upgrades that require software changes. The original software has demonstrated its reliability for over several hundred reactor-years of operation, with only a few deficiencies found and corrected in that time. However, most of the software was developed before the current software development standards were available, resulting in potentially incomplete documentation and test cases for verification and validation of the functionality of the software. Ideally, the software documentation and development environment should be updated to meet current guidelines and standards for reactor control software. This is a major undertaking for any plant. The design of the original software, programmed in assembler with the required optimizations for speed and memory, makes this task even more challenging. As a result, upgrade options that do not require any, or at least minimize, software changes are frequently preferred over alternatives that, while more attractive for other reasons, require significant software revisions to the existing DCC software. Nevertheless, over the long term, updated DCC system documentation and complete software validation test suites that meet current standards are essential to provide the broadest range of upgrade options.

4. UPGRADE STRATEGIES

The potential upgrade options or strategies to be considered for DCCs in existing CANDUs can be classified into four, somewhat overlapping, categories:

- individual component replacements or upgrades;
- subsystem upgrades with functionally equivalent replacements;
- upgrading subsystems and moving display functions to a Plant Display System; and
- complete DCC replacement with DCS equipment.

4.1. Individual Component Replacements

This level of upgrade can easily be regarded as just good maintenance. Essentially, components that are found to be failing at an unacceptable rate are replaced on a regular basis, or alternate components that are functionally the same, but more capable of withstanding the operating stresses are substituted. For example, many plants now replace all electrolytic capacitors in DC power supplies regularly every so many years, as these capacitors were observed to deteriorate with time and use. Similarly, resistors have been substituted in some circuits with higher power ratings where failures had been observed with lower power rated resistors.

Opto-isolators in digital input-output boards also appear to deteriorate after some years of use, with the leakage current increasing with increasing age. Newer component designs may not be as susceptible to these effects. Hardware design modifications such as these are fairly easy to implement since there is no fundamental change in the circuit functionality, and thorough testing of the changes is usually straightforward. After implementation, some re-calibration of the system may be necessary, but no software changes are required.

4.2. Subsystem Upgrades by Equivalent Functional Replacements and Add-Ons

Most of the upgrades to the present DCCs are in the category of DCC subsystem modifications that require little or no software changes. In most cases, these can be thought of as either "equivalent functional" replacements or "add-ons". Up to now, most of these types of changes have involved the replacement of the original electro-mechanical peripheral devices with more modern technology, having either equivalent or better functionality. There are several reasons for this:

- Many of the original electro-mechanical devices were amongst the least reliable components of the original DCCs, i.e., these devices needed the most maintenance.
- The logical and electrical interface is relatively simple, allowing the original system to be replaced by a newer system with the same interface.
- In some cases, the original equipment was in relatively widespread use on various other industrial systems, resulting in a sufficiently large commercial market for upgraded replacement systems.

It is also at this point that there exists some divergence in upgrade strategies. Often the replacement equipment has much better performance than the original equipment, e.g., faster access or larger capacity. However, these capabilities can only be exploited by modest changes in the DCC software, usually in the executive. Thus decisions must be made whether to upgrade the software to take advantage of the potential performance improvements, or to leave the software alone with the assurance that the new system will perform exactly the same as the original system.

The choice between these options is never completely clear, as it depends heavily on the confidence with which changes to the software can be made and tested, versus the benefits of any performance improvements. Plants that have good control of the software configuration, good test suites for software changes, and good hardware and software diagnostic tools are well positioned to take advantage of any performance improvements available through hardware upgrades with modest software changes.

For example, AECL has developed a paper-tape reader-punch replacement that uses a standard IBM-compatible personal computer, which has been installed in some Canadian plants, and in newer CANDU 6 plants abroad. In this case the electrical interface was simple to duplicate, and no DCC software changes were necessary.

A common upgrade in all older plants has been the replacement of the fixed-head disk with a battery-backed-up RAM disk unit from Imperial Technology. Here an electro-mechanical system is replaced by an all solid-state memory unit, providing greater reliability through the elimination of the moving parts. The

replacement system is also capable of higher throughput to the CPU with a redesign of the original fixed-head disk controller and some software modifications.

Another valuable upgrade is the use of the AECL-developed Parallel Data Link Controller cards which serve as a general purpose interface between a DCC and a standard IBM-compatible personal computer. While this modification requires DCC software changes to be effective, the addition of this card permits most of the features available on IBM PCs to be accessible to the DCCs. Some of the ways this capability has been used include

- replacement of the moving arm disk with the hard disk in the PC, and
- connection to an external network for remote storage and processing of DCC-acquired data (i.e., an "add-on" gateway interface).

In the first case, the less reliable and lower capacity moving arm disk is replaced by a modern standard PC hard disk for data storage or near real-time analysis with complex programs on the PC. In the second case, the PC serves as a gateway to a larger plant network for remote storage and archival of historical plant process data in an Historical Data System (HDS), for interactive processing of recent plant data by station staff. At the same time, this gateway provides isolation between the DCC and this network in the event of network disruptions.

The upgrades of this type described to this point have involved minimal or no software or hardware design changes, and utilise existing system interfaces. Others to be considered which are a little more complex and require meaningful system design modifications include:

- Replacement of core memory on the original VARIAN computers with modern solid-state memory

The motivation here is two-fold: concern about reliability problems, particularly parity errors, in the existing core memory; and lack of commercially available spare memory in the event of failure of existing memory. This substitution is difficult because of the large differences between the electrical interface to core memory and the interface to solid-state memory.

- Replacement of the RAMTEK display systems

There are several different alternatives being considered. AECL is developing a Pentium-based system that completely emulates the original RAMTEK display system, requiring no DCC software changes whatsoever. However, the computing power of this system will permit the enhancement of the available displays and character sets. Point Lepreau is examining an approach where DCC software is modified to send the data to be displayed to a VME-based Pentium system where the final display is generated, emulating the equivalent RAMTEK display. In this case, most of the display program functionality has been transferred to the VME system. Bruce B is currently examining several RAMTEK replacement system alternatives that have been proposed by various vendors.

- Replacement of the VARIAN CPU

Although the VARIAN CPU architecture is used in most DCC computers (except for the Pickering A and Darlington plants), only the plants completed before the mid-1980s have computers built by VARIAN. Later plants (Cernavoda; Wolsong 2, 3, and 4; and Qinshan) use computers manufactured by Second Source Computers Inc. (SSCI). The SSCI computers implement the VARIAN CPU instruction set, but use more modern components and introduce several design improvements over the original design. These improvements include solid-state memory with single-bit error correction and double bit error detection, better memory mapping and protection hardware, and greater address space.

AECL has modified the original executive software to take advantage of many of these features for the DCCs in the newer plants. While substitution of the SSCI CPU for the original VARIAN CPU is possible in older systems, substantial work would need to be done to verify the proper operation of all plant DCC software on the new computer system because of the changes to the executive software and differences between the execution time for identical sets of instructions on the two CPUs.

In general, these incremental upgrades have proven to be reasonably cost effective and provide a relatively proven short-term (i.e. 5 to 10 year) solution to DCC obsolescence issues.

Figure 2 illustrates the configuration of the DCCs with the various upgrades in this category, all of which have already been implemented at the various stations in some form. Note that an upgrade or replacement exists for all major subsystems and/or peripherals. It is important to note that for these types of upgrades, there is still considerable design engineering effort required, particularly for the VARIAN CPU and RAMTEK replacements, and that implementation during an extended plant outage may be necessary.

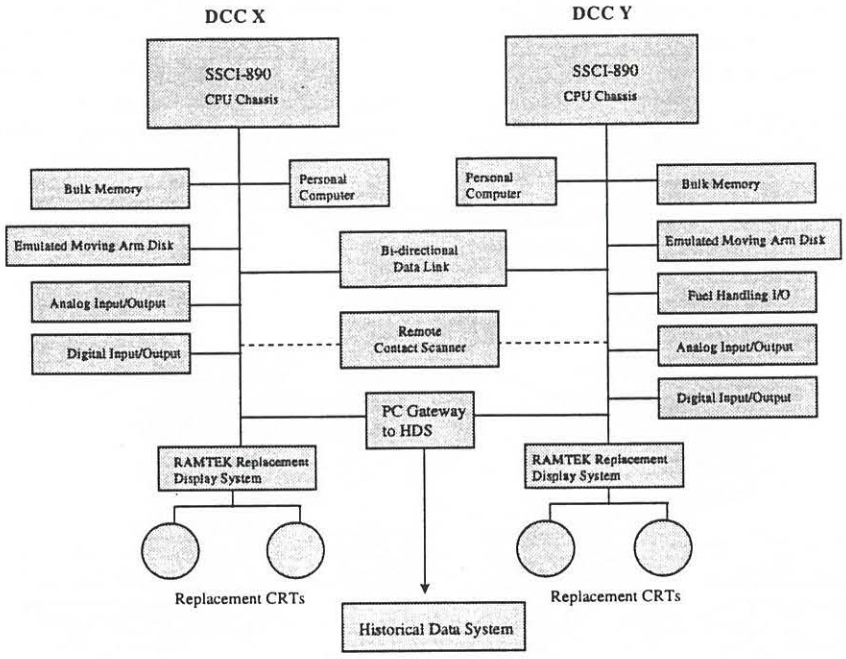

Figure 2: Functional Equivalent Subsystem Replacements and Add-Ons

4.3. Upgrade by Moving the DCC Display Functions to a Plant Display System

This approach involves the replacement of the RAMTEK display system with a plant display system (PDS). It requires significant changes to the design and function of specific DCC subsystems. It is an approach that typically requires changes to hardware interfaces and significant alterations to the system software, which may include both the system executive as well as peripheral or interface handlers/drivers. This involves a complete redesign of the display subsystem to take full advantage of newer hardware and software technology, and to provide improved functionality and features. Using the latest hardware and software technology allows improvements in performance, reliability, and maintainability. While system architectural changes are required, the approach attempts to localize their impact. This type of upgrade involves both interfacing the new subsystem with the existing hardware and software interfaces, and the re-allocation of many system functions or services from the older DCC to the plant display system, and in the process, both off-loading the VARIAN, and avoiding the design limitations of the older hardware.

Figure 3 illustrates the current conceptual architecture for the DCC and PDS being proposed for the Akkuyu Project. This approach would incorporate many of the "functionally equivalent" DCC subsystem replacements (i.e. peripheral upgrades) outlined in the previous section, as well as the complete removal of the display system functionality from the DCC. Display functionality to support the operator interface, including annunciation, mimic displays previously controlled by the DCC, would be moved to and under the control of the new Plant Display System (PDS). A clean interface for data transfer and coordination between the two systems would be provided.

Removing the operator display functionality from the DCC also provides an opportunity to improve overall system safety, reliability, and maintainability. This can be achieved by:

- Isolating the control software and interlock/safety control software functions (in a more stable DCC software environment) from incremental revisions, re-configurations, and enhancements necessary in the annunciation and display system.
- Improving the overall defense-in-depth of the control room systems architecture by reducing the inter-dependencies and localizing the impact of a failure of the display system, and minimizing its affect on the DCC.
- Providing increased display system functionality and configurability with a PDS product designed to accommodate these in-service changes and supported with a suitably robust maintenance and support toolset and environment.

This approach also allows system functions like the print logs and the contact scanner to be interfaced to the PDS layer of the architecture. Although not feasible in existing plants, digital and analog input signals which are used for monitoring purposes only, could also be supported on a Data Acquisition (DAS) node directly on the PDS LAN. Support for more

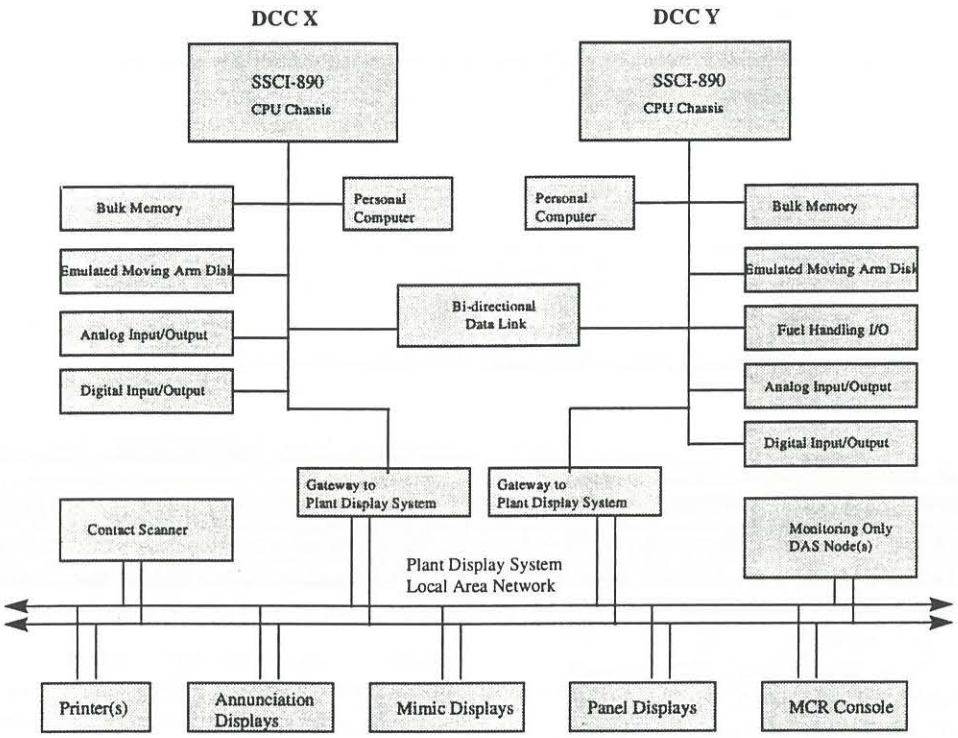

Figure 3: Migration to an Architecture with a Separate PDS

advanced displays, including flux mapping, channel temperature monitoring, fuel handling, and critical safety parameter monitoring would be implemented in the new PDS system. Finally, it should be noted that although commercial PDS products are available, this approach involves a considerable DCC software re-engineering effort, and implementation of design changes to the system would only be feasible during a major plant outage. It does however, make good use of the existing and proven DCC software. Although this approach does not completely eliminate longer term DCC maintenance and obsolescence issues, it does provide a relatively proven solution for existing stations, and for near-term future CANDUs.

4.4. Complete DCC replacement with DCS Equipment

The final option can be described as a complete retrofit replacement of the DCC control computer with suitable commercially available Distributed Control Systems (DCS) equipment. As in Section 4.3, this would include moving the operator display functionality to a separate Plant Display System, such as AECL's ACCIS (in development) or another viable commercial PDS product. In this approach, the general architecture and system behavior of the original DCC system can be closely "emulated", with some improvements where appropriate. The functionality of each of the main DCC control programs would be "migrated" to a separate dual redundant DCS X/Y "node-pair". Collectively, all of the "X" nodes behave as the original DCCX, all of the "Y" nodes behave as the DCCY. A similar approach is under consideration at the Point Lepreau Generating Station, whereby an incremental upgrade strategy is under preliminary investigation. The feasibility of a gradual transition to a new system on a program-by-program basis is being explored. In a typical DCS, each node (which is often referred to as a "remote terminal unit" (RTU) or "station"), communicates with the other nodes via a dual-redundant LAN.

It is important to note that this approach does involve considerable effort, and would require a complete re-implementation of all the control programs, and extensive testing. Hence, this approach would only be considered feasible during a long planned outage and economically justifiable for plants undergoing refurbishment for major life-extension. Figure 4 illustrates this approach.

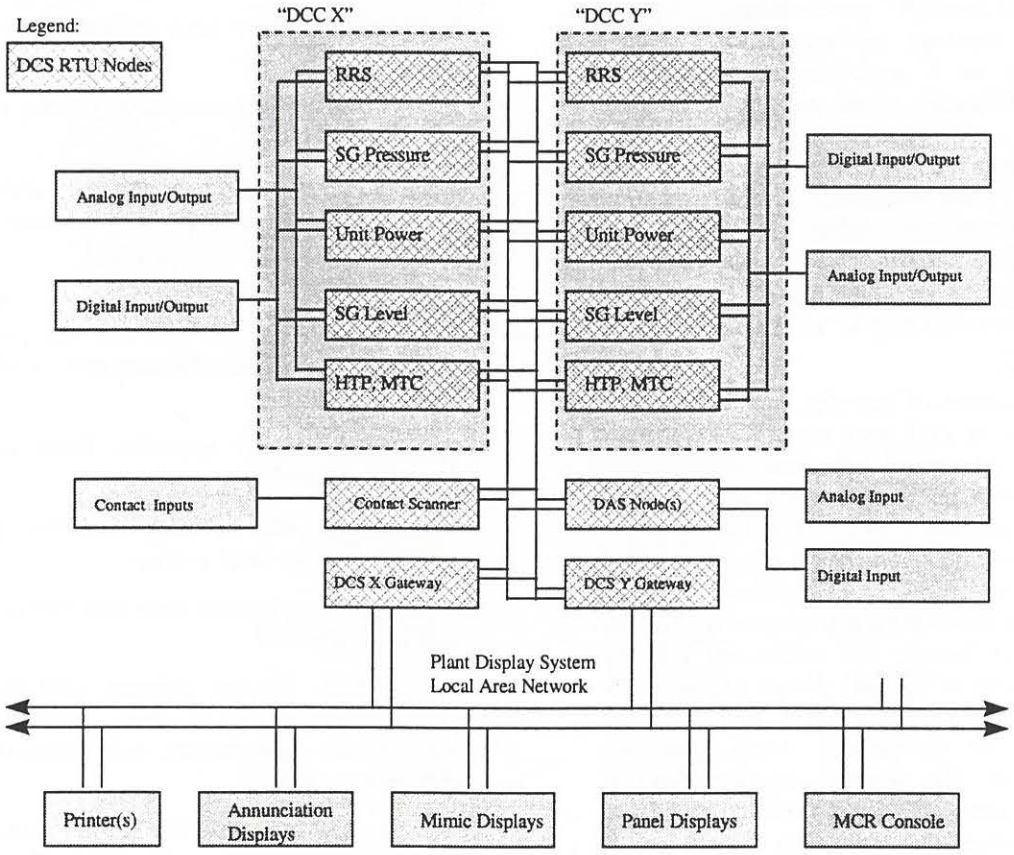

Figure 4: Migration to DCS-PDS Architecture

Note that the diagram also shows that the PDS gateway, the contact scanner, and data acquisition (DAS) nodes (used for "monitoring only" functions), could also be implemented with standard DCS equipment.

An advantage of this approach, is that DCS equipment is highly modular and configurable, and further system expansion or optimization would be possible in future. Leading DCS products are also provided with a graphical development and test environment that would improve overall system maintainability. For existing plants, it is possible the installed data acquisition hardware could be re-used, while in new plants, the input/output boards used would be the DCS vendor's standard product.

This approach offers a long term solution for existing stations which is compatible with the direction in future CANDUs towards the use of suitably qualified commercial distributed control system equipment.

5. USING A COMMERCIAL DCS

It is important to note that in considering the use of any "off-the-shelf" pre-developed computer system or software product in safety-related Category 2 or 3 applications, software and system qualification issues must be thoroughly addressed. A comprehensive qualification report is required to provide a reviewable and defensible documentation that the product can be made to meet the safety, reliability, and maintainability requirements for the intended context of use. A qualification should also establish the stability and "proven-ness" of the product.

The qualification of complex system products like a DCS or PDS may require the separate assessment of several subsystem components, and may result in significant cost and effort. If addressed properly, the process will identify and aid in the resolution of technical risks early in the system design cycle. Qualification places an emphasis on establishing a given product version and its usage history, and credits any inherent safety features or fail-safe design attributes. It should also identify possible failure-modes, limitations, or deficiencies which must be addressed in the intended configuration or context of use. Careful consideration of the product configuration issues, the overall system architecture, and any features or functions to be avoided or guarded against is required. The product qualification process does not replace other system engineering design cycle activities such as various verification and validation activities. It does provide a degree of confidence that the product quality is such that, for a specified version of the product in a specific context of use, and provided all qualification issues are adequately addressed in the design process, a level of integrity in the system design can be achieved that is equivalent to a product designed in compliance to the appropriate Category 2 or 3 standard. Qualification enables the use of suitable and proven products and reduces the need for costly, risky, and custom in-house designs of complex system products.

6. SUMMARY

It is clear from the previous discussion that there are several viable options to consider with respect to DCC upgrades. Some of the key factors that will determine both the technical and economic feasibility of alternative DCC upgrade options include:

- the age of the station,
- upgrades that have been implemented to date,
- the expected decommissioning date for the station,
- when and how long any planned station outages provide an opportunity window to install and commission an upgrade,
- how much longer maintenance of the existing DCC equipment due to parts availability and expected failure rates will be feasible,
- the capital cost of upgrades, funds and resource availability,
- the technical and licensing risk and the ability to manage these issues,
- the current maintenance costs and technical staff resources, and
- the benefits of the upgrade including improvements in system safety, reliability, performance, functionality, maintainability, and OM&A costs.

Each station will have a different set of decision parameters which may result in different approaches. For stations with a longer expected life, the economics of a more long term solution become much more attractive. The use of a suitably qualified and proven commercial "off-the-shelf" DCS product is a viable option in this case.

7. REFERENCE PAPERS

Melancon, P., Hubert, J. *Gentilly 2 Digital Control Computer Maintenance Strategy*. Hydro Quebec. 3rd International Conference on CANDU Maintenance. Nov. 1995.

Hong-Woo, K. *Computer Maintenance Experience of Wonsong 1*. KEPCO. 2nd COG Computer Conf. Oct. 1995.

Walker, P., Wang, B.C., Fung, J. *Hardware Replacements and Software Tools For Digital Control Computers*. AECL. CNS Conference. June 1996.

Gour, N., Rivest, J.-M., *"Digital Control Computers' Cable Replacement at the Hydro-Quebec Gentilly 2 Nuclear Power Station"*. Hydro Quebec. CNS 2nd International Conference on CANDU Maintenance. Nov. 1992.

Harber, J.E., Kattan, M.K., and MacBeth, M.J. *Distributed Control System for CANDU 9*. AECL. CNS Conf. June 1996.

Storey, H. *Point Lepreau's LAN-Based Station Control Computer and Generic Monitoring System and Historical Plant Data Collection and Distribution System*. NBP. 1992.

DeVerno, M., de Grosbois, J., Bosnich, M., Xian, C., Hinton, J., Gilks, G. *Canadian CANDU Plant Historical Data Systems: A Review and Look to the Future*. AECL. CNS Conference Paper. June 9th, 1996.

Fieguth, W., Hinton, J., *Advanced Control Centre Information System (ACCIS)*. AECL. CNS Conference Paper. June 9th, 1996.

Tremaine, D.R., Ahluwalia, D.S., de Grosbois, J.F.P., Echlin, E.G. *Guide for the Qualification of Software Products*. COG-95-179. Oct. 1995.