invensys

Triconex

White Paper

Point Lepreau Refurbishment:

Project Programmable Digital Comparator (PDC) Replacement for SDS1 and SDS2 – Update 1

Authors: K.G. Fraser, N.M. Ichiyen and A.E. Condor (AECL)
P.D. Thompson (New Brunswick Power)

What's Inside:

Point Lepreau Refurbishment:

Project Programmable Digital Comparator (PDC) Replacement for SDS1 and SDS2 – Update 1

1. Abstract

NB Power is tentatively planning to conduct an 18-month maintenance outage of the Point Lepreau Generating Station (PLGS) beginning in April 2008. See [1] for a description of the overall refurbishment project. The scope of the outage was determined from the outcome of a two year study (Phase 1) involving a detailed condition assessment of the station. This study examined issues relating to ageing and obsolescence, along with a detailed review of Safety & Licensing issues associated with extended operation. In order to minimize schedule and regulatory risk for the Refurbishment project, pre-project work was initiated in early 2002, called Phase 2 ESA (Early Start Activities).

Phase 1 assessments concluded that replacement of the Programmable Digital Comparators (PDCs) for both shutdown systems was required to ensure operation of the plant for an additional 25-30 years. As part of the Phase 2 ESA program, critical tasks related to the PDC replacement were identified. This paper describes the progress of the Phase 2 ESA program and the planned future (Phase 2) work for the PDC replacement for Shutdown System Number One (SDS1) and Shutdown System Number Two (SDS2).

2. Introduction

At the 2003 CNS conference, the Point Lepreau Refurbishment Project Programmable Digital Comparison (PDC) Replacement for SDS1 and SDS2 paper [2] was presented that discussed the method used to select a replacement hardware platform (Tricon™ system), for the SDS1 PDCs. The paper also discussed the software development approach used for the SDS1 and SDS2 application software. This paper continues the discussion of the activities performed up to the end of 2004 and includes the qualification of the Tricon system, the design of development, testing facilities for both shutdown systems and future work to be performed on the PDCs.

3. The Programmable Digital Comparators

Two completely independent shutdown systems, SDS1 and SDS2 are currently in use in CANDU (CANada Deuterium Uranium) reactors.

Each system contains three independent safety channels arranged in a two-out-of-three voting system. Channelized instrumentation is used to monitor a number of plant neutronic and process variables. If variables in any two channels of a single system are outside the predetermined envelopes, a shutdown is initiated.

At the Point Lepreau Generating Station, the logic for most of the process-related reactor trip coverage is implemented in computers. This allows optimization of trip functions for various operating conditions and reduces the burden of calibration, testing or maintenance activities that would have been mandatory with conventional analog and relay-based logic. A denser packaging of logic is now possible, with the corresponding space savings, while increasing the flexibility in implementing enhanced trip functionality. Computers allow implementation of self-checking and equipment monitoring functions that improve the availability and decrease the maintenance and testing load on the station staff.

To emphasize the straightforward computing functions contained within the computers commonly referred as Programmable Digital Comparators (PDC). The original PDC was a general purpose minicomputer, MP 100 from Data General. By the time AECL was used at the Point Lepreau Generating Station, the MP 100 was well established in process control applications, particularly in the pulp and paper industry.

The configuration introduced in the CANDU 6 reactors was two independent PDCs per channel, for a total of six PDCs per shutdown system. Each CANDU shutdown system consists of three independent channels.

In newer plants (such as Wolsong 2, 3, 4, Qinshan 1, 2 and Cernavoda 2), the original PDC equipment was no longer available from the manufacturer. Discussions with the manufacturer revealed that some integrated circuits (ICs) used in the PDCs had ceased production. This meant that the manufacturer was not able to obtain the parts needed to produce the PDCs. As the manufacturer no longer had a suitable product line, new hardware suppliers had to be selected.

The assessment showed that the best option is the Tricon product from Triconex and that a single PDC per channel configuration was feasible. Since the Tricon product also had a slight advantage in the tool selection assessment, it was decided that for Point Lepreau Refurbishment, Triconex is the preferred supplier for the SDS1 PDCs.

For SDS1, the selected computer hardware was from Asea Brown Boveri (ABB) and the product line was called Procontrol P13. For SDS2, the computer hardware was supplied by PEP Modular Computers (now called Kontron) and uses an industry standard VME-based architecture.

4. Point Lepreau PDCs Platform Selection

Condition assessments were carried out during 2000-2001, to assess plant equipment and systems to be replaced as part of the refurbishment. The assessment concluded that replacement of the PDCs for both shutdown systems was required to ensure continued operation of the plant for an additional 25-30 years. The recommendation from Phase 1 for SDS2 was to use the same hardware and software development methodologies used for Qinshan 1, 2 and Wolsong 2, 3, 4. The hardware platform considered resistant to obsolescence and along with the hardware would be maintained for throughout the life of the station.

For SDS1, the recommendation from Phase 1 was to use a different hardware platform from that used for Qinshan 1, 2 and Wolsong 2, 3, 4. It was considered unlikely that the hardware would be maintained for the remainder of the station life. The hardware platform must support a graphical function block software language approach similar to that used for Wolsong 2, 3, 4 for SDS1. Provided that the performance requirements could be met, a single PDC per channel configuration was preferred. NB Power approved these recommendations for SDS1 and SDS2 as Configuration Change Assessments (CCAs).

5. Phase 2 ESA Results

The scope for Phase 2 ESA was to define the hardware and software approach for replacing the SDS1 PDCs, review the software standards and prepare procedures applicable for the SDS1 and SDS2 PDC software development approach.

SDS1 HARDWARE SELECTION

Requirements were established and based on a number of sources:

- Point Lepreau project contractual documents
- Point Lepreau preliminary technical specification
- Technical specifications from previous PDC projects such as Qinshan
- Relevant international standards, such as IEC standards
- Assessment document, integrated approach tool selection and evaluation
- Engineering judgment and other requirements deemed important for Point Lepreau replacement SDS1 PDCs

The hardware platforms consistent with the software development tools from the software tool assessment were assessed against the following requirements.

The assessment showed [2] that the best option is the Invensys Tricon built on Triconex® technology and that a single PDC per channel configuration was feasible. Since the Tricon product also had a slight advantage in the tool selection assessment, it was decided that for Point Lepreau Refurbishment, Invensys was the preferred supplier for the SDS1 PDCs.

SDS1 PLATFORM QUALIFICATION

Tricon, not proven for use in CANDU shutdown system applications, with the platform including a substantial amount of previously-developed software, an extensive qualification assessment for the platform was implemented. This process was developed to meet the requirements of the IEC standard 61513 on the use of I&C in safety-related systems in nuclear power plants. The process also requires several additional IEC standards, 61226, 60880, 62138, 61508, 60987 and 60780, to be used to develop the qualification requirements.

The qualification procedure identifies numerous methods required in developing requirements for the qualification and dependent on the safety class of the system. PDCs are the highest class (Class 1) and are subject to the most stringent requirements of the procedure. The various methods used along with the results are presented in the following subsections.

The process consisted of developing the qualification plan, which identifies each method to be used and the qualification requirements in checklist form. Data was gathered by examining Triconex documentation and by visiting the Triconex facility to interview staff and examine evidence. About two weeks were spent at the Triconex facility during three visits. The first visit was technical in nature and lasted 5 days. The other two visits were each three days long and dealt with quality assurance issues. A final report was prepared listing the results and recommendations. The Tricon qualification assessment covered the following areas:

- Product quality assurance process assessment
- Hardware specification review
- Third-party certifications of the Tricon product
- Operating history
- Reference site assessment
- Failure modes assessment
- Goodness of design
- Maintenance assessment
- Anecdotal evidence
- Application software prototype
- Code verification on the software prototype
- Function block testing

The Audit Team concluded that Triconex had put in place and are properly managing a quality system capable of making products meeting AECL's quality standards and design requirements for the SDS1 PDCs.

Each topic is discussed in further detail in the following subsections.

PRODUCT QUALITY ASSURANCE PROCESS ASSESSMENT

The assessment consisted of two audits by QA and technical staff. The first audit was led by the PLR project QA manager and one additional staff. Triconex was audited against the requirements of the CSA standards N286.1-00, "Procurement Quality Assurance for Nuclear Power Plants," and N286.2- 00, "Design Quality Assurance for Nuclear Power Plants." This was a standard audit of Invensys' corporate QA policies with the result that Invensys was placed on AECL's Approved Supplier List.

The purpose of the second, technical QA audit was to determine whether:

- The Tricon product meets the technical quality objectives for safety, reliability, maintainability and reviewability for the SDS1 PDC platform
- The intent of the applicable standards, in particular IEC 61513, 61508-2, 60880, 62138, 60987 and 60780, are satisfied

The second audit scrutinized the following aspects of the Tricon product lifecycle to ensure that Triconex has adequate processes in place to meet the foregoing quality objectives and the processes are implemented correctly by Triconex' staff.

- Safety lifecycle management that included the overall safety of the lifecycle and planning
- Overall system engineering process that included the system requirements specification, software and hardware integration and verification and system validation
- The software engineering process, that included the software lifecycle, the software requirements specification, software design and implementation, software modification and verification and configuration management
- The hardware engineering process that included the hardware lifecycle, requirements specification, design, implementation, modification and verification

The audit was led by the PLR project QA manager, one additional QA staff and two technical staff. Triconex' staff interview consisted mainly of the former lead verification engineer for the Tricon product and was extremely knowledgeable about most aspects of the product lifecycle.

The Audit Team concluded that Triconex had put in place and properly managed a quality system capable of making products meet AECL's quality standards and design requirements for the SDS1 PDCs.

HARDWARE SPECIFICATION REVIEW FOR SUITABILITY IN THE PLR SDS1 APPLICATION

The hardware was assessed as suitable prior to the qualification during the hardware selection process [2]. Furthermore, detailed information was gathered during the qualification and specific recommendations were made for the production phase. In particular, the analog input module required for the PLR project was still in the design phase at the time of the qualification. One recommendation was to review the final production specifications of the module when they became available.

Information for the hardware review was collected from detailed design documents available during the qualification and from interviews with Triconex staff.

THIRD-PARTY CERTIFICATIONS OF THE TRICON PRODUCT
The certification assessment involved reviewing third-party certifications for the Tricon product. The two major certifications are the TÜV1 and the US Nuclear Regulatory Commission.

The US Nuclear Regulatory Commission has approved the Triconex system as suitable for safetyrelated systems in nuclear power plants.

TÜV is a well-known certification group based in Europe with a solid reputation worldwide for certification of safety systems. TÜV has certified the Tricon as suitable for SIL-3 applications according to IEC 61508. The TÜV certification made a number of recommendations and usage restrictions that were documented in the Triconex Safety Considerations Guide, which contains recommendations for using the Tricon in safety applications. These recommendations were also considered for their applicability to the PLR PDCs.

In addition, the US Nuclear Regulatory Commission has approved the Triconex system as suitable for safety-related systems in nuclear power plants. This certification is necessary in order to use the Tricon in all safety-related nuclear power plant application in the United States.

Tricon's certifications were used as the basis for developing the qualification requirements. Considerable more effort would have been required to qualify the product if the certification was not passed.

OPERATING HISTORY
The operating history assessment involved analyzing the amount and type of operating history, history of errors detected and the history of the changes made to the software product(s). The assessment considers all Tricon system sales, estimated duty cycle and similarity to the PDC application. The guidelines consider the Tricon system to be of high complexity with no minimum operating history levels dictated by the guideline for high complexity systems. The minimum level for medium complexity systems is 5000 years, but each high complexity system must be evaluated individually. It should be noted that the high complexity is due in part to the extensive built-in diagnostics. The built-in diagnostics are a basic part of achieving the IEC 61508 SIL-3 certification that the Tricon system has achieved. The operating history of the system is based on the total usage history of 140 million hours (now 200 million hours) with no unsafe failures.

This system was evaluated in light of the same triple modular redundant (TMR) architecture that has been in use since version 5 in 1989. Having the same TMR architecture means that the interfaces among the I/O modules, I/O processors and the main processors remain the same. Any updates to modules must be integrated into a system that has interfaces already defined in the TMR architecture.

For this reason, some credit was taken for older Tricon versions. Versions from 9.6 and above use the same processor and I/O modules, with the differences between versions are very minimal, usually a minor change to one module's firmware. Credit for these versions is taken at 100%.

Version 9.5 systems are credited at 75% of operating years and are identical to 9.6 and above systems except for the Main Processor (MP) module. The software used on the Tricon 9.6 MP module (the MP 3008) was ported from the Tricon 9.5 MP module (the MP 3006/3007). The majority of the MP 3006/3007 code was re-used as-is. The main differences were from diagnostics and communications, which were different due to the changed architecture of the MP module.

Older system versions from 1986 to 1999 were conservatively credited at 30% of operating years. This was due to the architecture and interfaces of the system remaining unchanged over the life of the product.

The final result was more than 12,000 years of operating history and was considered acceptable, given the safety record during that time and with certifications by TÜV and the Nuclear Regulatory Commission.

REFERENCE SITE ASSESSMENT (Tricon end-users feedback on performance in the field)
A questionnaire was sent to Tricon end-users to obtain feedback on the performance of the Tricon in the field. Only one response was received from a nuclear utility using the Tricon in a turbine control system and they were generally happy with the product and had nothing negative to report.

FAILURE MODES ASSESSMENT

A detailed assessment of the failures and failure modes was performed using proprietary and nonproprietary information from Triconex. The assessment was performed in three different aspects: evaluation of Triconex' Failure Modes and Effects Analysis report. The evaluation of the answers from the Failure Modes questionnaire was obtained during the technical visit and evaluation of the database of customer alert bulletins published by Triconex.

Single fault failures are generally isolated to one of the controller's three channels; the remaining two channels maintain full control and operate normally as a 1oo2 system instead of a 2oo3. No single fault can cripple the system and generally faulty modules can be replaced on-line without interrupting the system. The TMR architecture of the Tricon PLC provides additional reliability to prevent an immediate SDS1 channel (such as D, E, F) failure which would degrade the entire SDS1 trip computer system from a 2oo3 configuration to a 1oo2 configuration. The failure modes and known failures that could prevent a Tricon PLC system from performing its safety function are detected by the built-in system diagnostics, periodic testing, or application-specific design.

This activity included an assessment of the Tricon's built-in diagnostics capabilities. Each system component detects and reports operational faults including such items as memory failures, internal communications failures (such as between modules), processor halt, redundant processor failures, single and multiple leg failures, internal fuse failures and power supply failures.

Invensys performed a reliability and availability analysis on the Tricon PLC in accordance with the EPRI TR- 107330 guidelines. The study was based on several modules including those modules used in the PLR SDS1 PDC application. The built-in diagnostics were reviewed with the Tricon Failure Modes and Effects report. The diagnostics provide assurance that the system can identify faults and provide the necessary fault indication. There is however some faults that are not detected and must be considered by the PLR SDS1 design team. These are generally minor issues that require additional testing. For example, the power supplies must be tested periodically to ensure they have not degraded.

GOODNESS OF DESIGN

The goodness of design was assessed as part of the technical QA activities and involved inspecting product design examples, such as design documentation and source code. It also involved interviewing senior product development staff to gain a more detailed understanding of the product design attributes and assessing and gaining confidence in the Tricon's quality and integrity. Factors considered included verifiability, understandability, robustness, predictability, modifiability, modularity, structuredness and consistency.

MAINTENANCE ASSESSMENT

The maintenance process assessment involved an assessment of the vendor's ability to upgrade and support the product over the long-term. The assessment showed that the product requires minimal maintenance effort at site and that no day-to-day maintenance is required. The system has built-in diagnostics and system status variables that are available to the application for monitoring.

The Tricon also supports online firmware upgrades and online replacement of faulty modules using active spares and hot swap technology. Upgrades can be carried out with minimal interruption to the process. The qualification plan and report dictate how upgrades are qualified. Invensys provides 24 hours a day, 7 days a week telephone technical support by trained staff, on-site support (with an additional fee), emails, conference call and CustomerNet. The Vendor also has well defined QA processes to support the maintenance of the Tricon system.

ANECDOTAL EVIDENCE (Research of available information, including the Internet)

This activity largely consisted of a search for relevant materials concerning the Tricon on the Internet. Few articles were found and were mostly positive. The information discovered was general and nonspecific but gave a general sense of the perception of the product. One article discussed the experiences of Texas Instruments using the Tricon at their manufacturing plants. Triconex has won a reader's choice award from the website automation (techies.com) for seven straight years.

APPLICATION SOFTWARE PROTOTYPE

An application software prototype was implemented to assess the Tricon system's suitability for use as the SDS1 PDCs. The prototype development process included the following activities:

1. Implement "slice" software requirements specification (SRS) and software design description (SDD) of a three-trip-parameter prototype that follows the applicable project procedures.

2. Perform a requirements review on the SRS, a design review on the SDD and design verification on the SDD, that follows the applicable procedures.

The "slice" prototype was successfully implemented. From the application software viewpoint, the Tricon system was suitable for use on the SDS1 programmable digital comparators for the Point Lepreau Refurbishment project.

The Integrated Approach (IA) process [2] used to develop the application software was also suitable for the specification, design and verification of the SDS1 application software, as applied on the Tricon System. The IA was previously the subject of a design review at AECL and has received CNSC approval.

CODE VERIFICATION ON THE SOFTWARE PROTOTYPE

The function block diagrams (FBD) are translated into executable code in several steps. First, the FBD are converted into Pascal-like Structured Text (ST), then encoding machine (EM) code and then into the executable code. Code verification was performed on the application software prototype to confirm that the FBDs were correctly translated into EM code. No logic errors were discovered during the code generation process that was applied to the prototype. This activity was spot-checked on the TÜV certification.

The conclusion of the qualification process was that the Tricon system is suitable for use in safety critical computer applications such as the PLR SDS1 system.

FUNCTION BLOCK TESTING

The Tricon function block language blocks were individually tested in a black box to ensure functionality according to the Tricon documentation and the specifications in the IEC 1131-3 standard. The test results were positive.

The results of the testing were recorded in a TriStation language reference manual document. The language reference manual provides a precise mathematical description for each block. The use of the primitive blocks in the SDS1 PDC application software is restricted to the ranges tested and documented in the language reference manual.

RESULTS OF THE QUALIFICATION

The qualification objectives focused on identifying the products that were assumed, known acceptable or unacceptable behaviors, functions, or roles in the system that arose from the project application context. Each issue was taken into consideration and assessed in the overall qualification. The evidence gathered and assessed during the qualification process established an adequate degree of confidence in the product's integrity and ability to meet both the system and qualification requirements with respect to safety, reliability and maintainability.

6. Software Engineering Tools and Facilities

TOOLS AND FACILITIES

Software development and testing activities are aided by the use of Development and Validation (DAV) test rigs. Each shutdown system is assigned a test rig. The test rig consists of three main components: the target PDC hardware to run the application software, a data acquisition system (DAS) and a personal computer for programming and testing.

The PDC component of the test rig is used during the software development for debugging and informal testing. It is also used by the software developer to confirm the performance timing requirements of the system (overall response time). The test rig is used by the verifiers and validators for testing. The PC is equipped with software to interpret test scripts which read and write the PDC's I/O using the DAS.

The test rig for SDS1 is shown in Figure 1 (see next page). The cabinet on the left contains two large black Tricon chassis that make up the PDC for SDS1. The PDC is connected by Ethernet cable to a PC and is used for software development and programming the PDC. The programming tool supplied by Triconex includes the graphical programming environment and emulator for development testing. The cabinet on the right contains a small DAS rack at the top and a PC at the bottom. The DAS is a rack from the Micro2016 system made by RTP that is connected to the I/O blocks of the PDC. The PC is used to interface with the DAS and run formal verification test scripts. Tcl/Tk test scripts are used to communicate with a DDE server, which controls the DAS I/O.

The test rig for SDS2 is shown in Figure 2 (below, right). The rack at the top of the cabinet is the DAS and the rack below is the target PDC hardware. A PC is used to interface with the data acquisition system (DAS). The DAS is a compact PCI system made by Kontron that is connected to the I/O blocks of the PDC. The PC is used to interface with the DAS and to run test scripts. Development testing is performed using Tcl/Tk test scripts that interface directly with the DAS I/O, with an additional I/O monitoring tool created with LabView. Formal verification testing will also be performed using this rig.

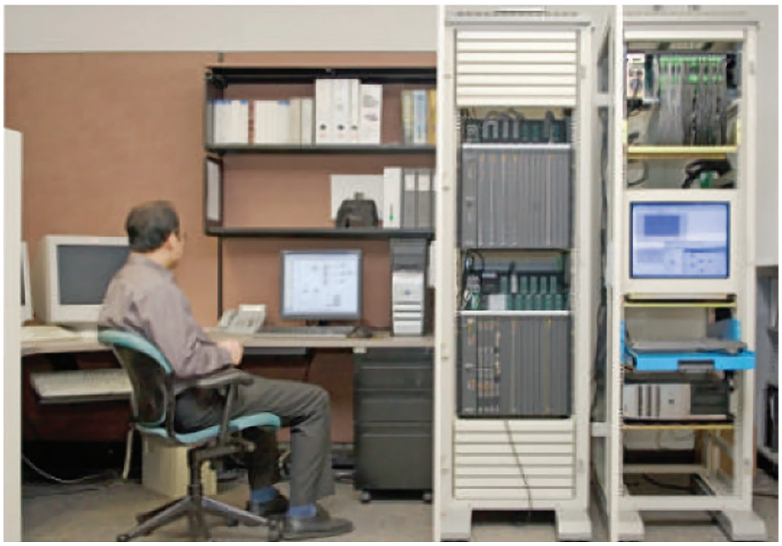

Figure 1. SDS1 Development and Validation Test Rig

Figure 2. SDS2 Development and Validation Test Rig

TOOLS AND FACILITIES QUALIFICATION

All the software engineering tools and facilities (T/F) to be used in SDS1 and SDS2 PDC software production for the PLR Project must be selected or developed to meet the usage requirements appropriate for their specific application areas. Each T/F must be qualified following a qualification approach based on the potential impact of the failure of the T/F and the existence of any mitigating factors. For example, the potential impact of a compiler error could have the incorrect code executed on the PDCs. This may be mitigated by the fact the code is thoroughly tested.

The qualification approach (such as acceptance testing, analysis and review) depends on the failure impact of the tool or facility. T/Fs with minimal impact and widespread industry use (such as Microsoft Word or Notepad) can be qualified by filling out a simple form containing basic information such as the T/F version and purpose. T/Fs with higher failure impacts require a more rigorous form of qualification.

A qualification plan and report is used to document the qualification of the tools. Additional tools may be qualified according to the plan and the records for each are filed in a common location. This approach is consistent with the requirements of IEC 60880.

The majority of the tools and facilities used for the SDS1 and SDS2 software engineering have been qualified for use. Some tools that will be used for formal testing are still under development and will be qualified once they are complete.

7. CNSC Interaction

To ensure that regulatory acceptance of the approach for the replacement of the PDCs are in place early in the program, a letter was sent to the CNSC (Canadian Nuclear Safety Commission). This letter identified the key elements in the design process for the PDCs – in particular the software development process. Subsequently, a number of key documents that define the intended design processes were sent, so that the CNSC could advise the utility if they had fundamental objections to the design approach.

The set of key documents included:

- The SDS1 software development approach assessment document
- Critical software development procedures for SDS1
- SDS1 and SDS2 quality project plan
- SDS2 assessment document on review of software standards and procedures
- Software procedures
- System overview design requirements
- Platform qualification procedures and reports

A number of comments were received; responses sent back and were accepted by CNSC. In May 2004 CNSC confirmed the methodology is acceptable. The documents submitted were reviewed and revised to incorporate the CNSC comments and the revised documents were accepted by CNSC. In March 2005, the comments received on the last pre-production document, the SDS1 Platform Qualification Report, were resolved to CNSC's satisfaction. This completed CNSC acceptance of all pre-production documents.

CNSC has accepted all software development procedures, therefore, it is not necessary for CNSC to review in detail all design documentation produced. Rather, the intent for the production phase of the work is to submit to CNSC the verification and validation documents and provide objective evidence that the accepted process is being followed.

8. Future Work

Once Phase 2 of the project is approved by the utility, tenders will be issued for the procurement of the hardware and the software design will start. The software production and verification/validation will be performed on "Development and Validation (DAV)" rigs at AECL. These are SDS-specific, such as one rig for each of SDS1 and SDS2 that includes the target PDC hardware, one PDC channel. In addition, the DAV rigs will contain hardware to apply the test cases for unit and subsystem testing and for validation and reliability qualification.

The major milestones to complete the project are:

- Start software design
- Issue tenders for procurement
- Procure and install DAV hardware
- Software verification
- Completion of coding
- Software testing
- Delivery of production PDCs to AECL
- Validation and reliability testing
- Delivery to site

9. References

[1] R.M. White, et. al., "Point Lepreau Refurbishment - Update 5," paper presented at the 26th Annual conference of the Canadian Nuclear Society, held in Toronto in June 2005.

[2] N.M. Ichiyen, et. al., "Point Lepreau Refurbishment Project Programmable Digital Comparison (PDC) Replacement for SDS1 and SDS2," paper presented at the 24th Annual conference of the Canadian Nuclear Society, held in Toronto in June 2003.