THE APPLICATION OF COMPUTERS IN 600 MWe CANDU SHUTDOWN SYSTEMS

R.S. GILBERT and H.A. MARTIN*

Atomic Energy of Canada Limited, Engineering Company
Mississauga, Ontario

*Martin, McCubbin & Associates Ltd.
Toronto, Ontario

ABSTRACT

The use of microcomputers or Programmable Digital Comparators (PDCs) in domestic CANDU 600 MWe plants is the first major application of digital logic in CANDU shutdown systems. These units have been installed to provide reliable and flexible conditioning logic for six process trip parameters in each of the two shutdown systems which these CANDU plants employ.

The PDCs systems use commercial off-the-shelf hardware which has been modified and qualified to meet the environmental requirements for a nuclear power plant application. Since the PDCs have been designed to provide accurate reliable and fault tolerant conditioning logic, they are expected to contribute significantly to improved operating margins and shutdown system availability.

INTRODUCTION

The 600 MWe plants, like other recent CANDU designs, have two independent and redundant shutdown systems. Both of these systems have triplicated channelized instrumentation which uses general coincidence two-out-of-three trip logic. The unique feature of the domestic 600 MWe designs, is that the shutdown systems employ conventional analog instrumentation and microcomputer based trip logic.

For licensing reasons, two microcomputers have been installed in each safety system channel, and these computers handle the trip decisions for six of the nine shutdown system parameters. These computers are designed to function principally as intelligent alarm or comparator units and have consequently been called Programmable Digital Comparators (PDC). The trip parameters used in the first shutdown system (SDS-1) and the six parameters processed by the PDCs are summarized in Table 1.

TABLE 1: SHUTDOWN SYSTEM 1 TRIP PARAMETERS

Parameter	Implementation
Rate Log Power High	Analog
Neutron Power High	Analog
Reactor Building Pressure High	Analog
Primary Flow Low	PDC1
Pressurizer Level Low	PDC1
Boiler Level Low	PDC1
Primary Pressure High	PDC2
Primary Pressure Low	PDC2
Feedline Pressure Low	PDC2

The parameters and implementations used in the second shutdown systems (SDS-2) are identical to the first system except that the primary flow parameter is replaced by a core differential pressure low trip parameter.

DESIGN FLEXIBILITY AND RELIABILITY

When the design of the 600 MWe shutdown systems was almost complete, domestic licensing requirements became more stringent and prescriptive. A major new licensing criterion was applied to the shutdown systems which required that each system have two diverse parameters to provide trip coverage for every design basis accident. This new requirement resulted in the addition of several parameters to the design. In addition, further safety analysis also indicated that some of the shutdown system parameters required trip setpoints which were a function of reactor power and of which main circulating pumps were operating. The precise form of these setpoint functions was uncertain and expected to be subject to the results of future analysis and licensing reviews.

Three possible ways to implement these new trip requirements were evaluated. The traditional approach of using commercial analog instrumentation, was rejected because it was too inflexible and could not readily handle complex setpoint functions. Custom designed analog circuits were also considered but again, this approach could not provide sufficient flexibility. It was decided that a microcomputer based design could handle simple or complex setpoint functions, and further trip parameter changes if these proved necessary. Also a digital approach was judged to be the most reliable and accurate method to provide a power signal for conditioning setpoints. One particular advantage of a microcomputer based design, is that it can easily detect failed or abnormal inputs. If a failed input is recognized, it can also alarm to ensure such a fault is not overlooked and it can take corrective action to ensure a single input failure will not disable trip parameters. The digital approach also has the advantage that it can readily calculate the power value for conditioning setpoints from a weighted average of neutron flux signals. The PDC design incorporates these features and is expected to increase the system availability because it detects and alarms out-of-range or inconsistent process parameter signals if they occur.

Since the PDCs represent a significant change from the traditional design of shutdown systems and since there was no previous operating experience with such a design, it was decided that the system would be more easily licensed if trip parameters were implemented using two PDCs in each safety channel. The six process trips which the PDCs handle were divided so that the two parameters which protect against the same accident are in different PDCs or are implemented by traditional analog logic and a PDC. This approach ensures that the failure of one PDC will not disable all process trips in one channel.

SIMPLE SOFTWARE

The PDC has a very simple software structure which uses no interrupts. The software is contained in about 3K words of programmable read only memory (PROM) and it uses about 100 words of random access memory (RAM). The program is written in assembly language and consists of a single loop of six software modules which are sequentially executed. A single pass of the program loop is completed every 35 ms. Each module is dedicated to a specific function or trip parameter. The first module computes the reactor power for conditioning trip setpoints. The next three modules then process trip parameters. The fifth module provides tests and checks which ensure that the computer is functioning properly. This module also generates any ouputs (e.g. relay contact closures) which have been determined by the previous four modules. The last module initializes the PDC for the next program cycle.

The software is designed so that it alternates between two types of program passes. The first of these is called a "real" pass. In this mode the PDC uses actual field signal data as it executes each module. At the end of this pass, the PDC will provide an update for an external watchdog and set trip or alarm outputs, depending upon the status of the field inputs which were examined. The second type of pass is called the "test" pass. During this pass, the PDC modules use input data which is read from PROM instead of real field signals. At the end of this pass, the PDC checks to ensure all of its results agree with a set of expected results which are also stored in PROM. If a discrepancy is detected between these two sets of data, the computer fails safely by allowing an external hardware watchdog to time out and cause a channel trip. By using this alternate path technique and by defining several "test" pass data sets, it is possible to check the ability of the computer to make correct trip decisions for all trip parameters and ensure the computer is functioning properly.

In addition to the "test" pass, the computer does a "thread" check which verifies that all software modules are executed in the correct sequence. The PDC also checksums all of the PROM memory at least every 350 ms to guarantee the integrity of the software logic and setpoints which are stored in the PROM memory.

As mentioned earlier, the PDC software will detect and alarm out-of-range signals which might be indicative of component failures. In fact most of the PDC software logic is associated with the rationality and spread checking of input signals. Since the PDC does recognize abnormal signal values, it takes corrective action by using default values, which ensure trip coverage is not degraded. The fault tolerant nature of the PDC logic is a major advantage of this design and it provides a significant benefit by ensuring the

availability of the power conditioning of trip parameters.

HARDWARE AND INTEGRATION

Each digital comparator in both shutdown systems, consists of a Data General MP100 microNova computer plus a Data General Data Acquisition (DG/DAC) subsystem and power supply. The MP100 contains the central processor (CPU), the random access memory (RAM) and the PROM. The DG/DAC subsystem contains all of the process inputs and outputs used by the PDC. Table 2 summarizes the inputs and outputs for a typical PDC.

TABLE 2: SUMMARY OF I/O FOR PDC-1

Voltage	I/O Type	Description
0-5V	Analog Inputs (AI)	7 Process Trip Signals
		1 Ion Chamber Linear Power Signal
		1 Ion Chamber Log Power Signal
		3 Incore Flux Detector Signals
		2 Power Calibration Inputs
		1 DG/DAC Test Input
0-5V	Analog Outputs (AO)	1 Average Power
		1 Log Power
		2 Process Trip Setpoints
		1 DG/DAC Test Output
48V	Digital Inputs (DI)	3 Circulating Pump Conditioning
		1 Watchdog Test
		1 DG/DAC Test Input
48V	Digital Outputs (DO)	13 Form A Relay
		24 Solid State
		1 DG/DAC Test Output

Since the PDCs were installed very late in the design, every effort was made to fit them into the existing conventional hardware configuration disturbing as little as possible of the existing circuitry, cable routing, etc. At the same time certain functional requirements made additional circuitry necessary. This integration problem was solved in the following ways:

- Analog inputs from process variables were already 4-20 mA current loops, so a dropping resistor was conveniently mounted in the transmitter power supply cabinet to convert these current signals to voltages for the AIs. Any new analog signals required were made to conform to the voltage range produced by this dropping resistor (approx. 0-5V).

- Several contact inputs were added to provide logic for setpoint switching. These were from new handswitches on the main control panel and only minimal additional wiring was required.

- The trip contacts (PDC DOs) were integrated into the existing configuration by simply replacing, on a one-for-one basis, the trip contact from the alarm units previously used to energize the trip relay, with a digital output contact from the PDC. In the case of multiple loops (eg. 2 boiler levels) only one contact (DO) was used. In these cases there was minimal disturbance to the trip chain logic.

- Because the setpoints for the process variables in the PDC's were determined as a function of power, new meter displays (identical to those already on the main control room panel) were required to display the setpoints and the power signals generating them. This caused little disturbance to the circuitry as such, but caused the existing panel arrangement to be totally unsuitable since good design dictated that meters displaying setpoint be strategically located beside the related variable. Since these circuits were all new, the displays were standardized as a 0-5 volt output.

Each PDCs principle inputs are the process trip measurements and its major outputs are the trip contacts associated with each parameter. Since the PDC acts like an intelligent comparator, the rest of the shutdown logic is a traditional design and instrumentation on the main control room panel is conventional. Therefore from the operators viewpoint, there is no special interface which would indicate that digital comparators are used in the logic. The only unique indications associated with the PDCs in the main control room are three alarm windows to annunciate abnormal input signals and watchdog trips.

Just as the PDC software tests its own functional capability, the DG/DAC hardware is tested by wiring one AO directly to one AI and one DO to one DI. The AO and DO outputs are changed periodically by the PDC software and they allow the computer to verify that it can control and read the inputs and outputs of the subsystem.

If a discrepancy is detected between outputs specified by the software and the inputs it reads back, the PDC generates an alarm.

Another feature which ensures that both the input and output subsystem and the CPU functions properly, is provided by an external hardware watchdog. This watchdog is mounted in a small indicating panel beside each PDC. This panel contains a light emitting diode display which is illuminated to indicate trips or abnormal conditions detected by the comparator. The watchdog itself must be updated every 100 ms or it will fail safe and trip the channel. It has a very simple design and it is updated when the PDC alters the state of a special DO at the end of each "real" software pass.

HARDWARE QUALIFICATION

In the 600 MW reactor safety system, all components were required to be seismically qualified to the level applicable for the particular site. In the case of the PDC's, since this was a new device operating in an industrial environment, it was felt that some measure of confidence should be gained as to its electrical noise immunity and its ability to operate at elevated temperatures for period representative of a loss of Class IV Power incident. The magnitude of the seismic excitation levels for the PDC's was determined by using a seismic analysis for SDS instrumentation cabinets which predicted the magnitude of the sinusoidal input to the device over the frequency range 1-33HZ for the PDC location in the cabinet. The amount of excitation to which the SDS cabinet is subjected is based on the Floor Response Spectra (FRS) of the Design Basis Earthquake (DBE for each particular 600 MWe site).

This analysis allowed a very straight forward bi-directional sinusoidal table excitation to be applied to the PDC's over the seismic frequency range of 1-33HZ.

The computer was tested on a shaker table which provided horizontal and vertical motion. The resonant frequencies of the panel and FRS, together with the panel's damping factor, dictated an acceleration building to a maximum of 2.2g over the range 7-16HZ, and tapering off at the high and low frequency ends to about 0.25g.

Commercial grade microcomputer systems are normally not constructed with seismic qualification in mind. None the less, by supporting larger masses and by stiffening the chassis, a successful modification of each PDC was accomplished. Some of the modifications required were:

- The CPU had its card cage stiffened by welding its inner card cage to the outer shell.

- The circuit board for the CPU's power supply had all heavy board mounted components glued to the board. The power supply was also held in place by support wedges and a card retainer.

- The DG/DAC power supply required the most extensive modifications because it was the most massive component in the system. To qualify the power supply, it was mounted on a special heavy duty bracket which allowed the supply to be supported without resting on or contacting the DG/DAC chassis.

- All cards in the DG/DAG also had card retainers fitted, to immobilize them during a seismic event.

The seismic qualification of the PDC was interesting from two points of view. It showed that without too much difficulty, and applying a little common sense (mechanically speaking), a commercial-grade microcomputer could be made robust enough to pass a shake test of the magnitude required for most locations. It also demonstrated the extraordinary punishment such a ruggedized device can structurally withstand and continue operating without a single failure.

TRANSIENT INTERFERENCE

The purpose of the transient interference test was to demonstrate that the PDC's located in the control equipment room or in the secondary control area (SCA) would be immune to conducted transient interference (caused by switching nearby) in their input/output circuits and AC power lines.

By immune, it is meant that the PDC will not: (1) behave in a manner that would render a shutdown system unsafe, and (2) behave in such a manner as to cause spurious shutdowns of that channel and hence of the station if a second channel is under test at the time of a spurious trip.

The first condition is mandatory while the second condition is highly desirable and would only be waived if the occurrence of this type of miss-operation could be shown to be of extremely low frequency.

The IEEE standard 472-1974 "Guide for Surge Withstand Capability Tests" and Ontario Hydro specification C-5403-78 "Specification for Transient Interference Immunity Tests on Electrical Equipment" have been used as the guides for these tests.

Specifically, the Ontario Hydro Specification at Level D (500 V) has been used as the test standard. Level D was chosen as the appropriate voltage level since SDS1 and SDS2 signals all run in isolated channelized cable trays and conduits and the equipment itself is in an environment where minimum high voltage switching takes place.

The Ontario Hydro test consists of injecting noise on a selected input, output, or power line, in both the common mode and differential mode at each of the six frequencies (130 kHz, 220 kHz, 360 kHz, 600 kHz, 1 MHz, 1.6 MHz) at the Level D voltage (500V) with test software exercising the system.

Some modifications were necessary to ensure system immunity. The changes required the shielding of cables and some I/O board modifications where injected noise was causing logic problems on the board itself (notably the Digital Output relay board and Analog Output boards). When all such solutions were implemented, the PDC would run continuously while being subjected to all frequencies of transient noise at Level D.

ELEVATED TEMPERATURE

The concern over the performance of the PDCs under conditions of a loss of Class IV Power resulting in a loss of air conditioning prompted an investigation of the ability of the PDCs to operate under elevated temperature conditions for periods of time representative of this situation.

To perform this test, the complete PDC including the CPU, I/O chassis, and its power supply, was placed in a temperature-controlled oven. The test was run such that temperature was raised from 30°C in 3 steps as follows: 2 hours at 40°C, 2 hours at 50°C and 1 hour at 55°C.

The testing showed that the PDC will operate completely satisfactorily at the temperatures it experienced. There is every confidence that the system could run for extended periods at these temperatures.

CONCLUSION

The PDCs are a significant step in the use of digital computers in CANDU shutdown systems. The use of digital logic has proven to be very flexible in accommodating late design changes and the PDC development has demonstrated that commercial computer hardware can be adapted for nuclear power plant applications. These computers are the first major step in the use of computer technology, rather than tradition relay logic in CANDU safety systems. It is expected that the further application of digital technology will enhance the operability and availability of safety systems in the future.