Control and safety computers in CANDU power stations

In Canada, Stage 3 of development calls for a fully computerized shutdown system

by R.S. Gilbert

The nuclear power industry has always been very conservative in adopting digital technology in its control systems. In most cases plant designers have not seen the need, or they have been reluctant, to incorporate digital control systems in nuclear power plants.

Mr Gilbert is Manager, Electronic Systems Branch, Atomic Energy of Canada Ltd., Sheridan Park Research Community, Mississauga, Ontario.

References used for this article were "Evolution of Computer-Based Surveillance, Control and Man-Machine Communication Systems in Nuclear Power Stations", by H.M. Wilkinson, December 1979; "Benefits from the Use of Computers in CANDU Shutdown Systems", presented by N.M. Ichiyen at the IAEA Specialists Meeting on the Use of Digital Computing Devices in Systems Important to Safety, Saclay, France, November 1984; and "The Use of Digital Computers in CANDU Shutdown Systems", by R.S. Gilbert and C.W. Komorowski, prepared for the same Saclay meeting.

Unlike the nuclear power industry, the process control industry (for example, oil refineries) embraced computer technology because it offered significant advantages in the control of large process systems. Early in the 1970s typical plant control systems were designed around a large central computer. This central computer (or main frame) received sensor information from the plant and then performed all the decisions required to directly control or optimize the operation of a plant. Even in these installations, however, manual backup systems were commonly provided to control the startup or shutdown of processes and to ensure continued operation, if the central computer failed, or stopped functioning.

The designers of the CANDU power plants recognized the advantages offered by computer control and have utilized control computers in the operation of these plants for more than a decade and a half. The functions

Computer-controlled functions in plant designs

	Douglas Point	Pickering 'A'	Bruce 'A'	Pickering 'B'	CANDU 600	Bruce 'B'	Darlington
Electrical energy output (megawatts)	1 X 200 (200 MW)	4 X 540 (2160 MW)	4 X 750 (3000 MW)	4 X 540 (2160 MW)	1 X 680 (680 MW)	4 X 750 (3000 MW)	4 X 850 (3400 MW)
In-service dates (first/last unit)	1962	1971/73	1977/79	1982/83	1982/83	1983/87	1987/90
Digital inputs	80	400	512	448	1104	576	656
Analog inputs	550	1152	1408	1408	1728	1840	2080
Digital outputs	46	272	408	256	712	504	448
Analog outputs	17	42	32	42	64	36	72
Display CRT (per unit)		2 CRTs	10 CRTs (B/W)	9 CRTs (Colour)	13 CRTs (Colour)	10 CRTs (Colour)	18 CRTs (Colour)
Printers	3 typewriters	2	2	2	2	2	2
Major real-time software routines	4	10	18	14	17	18	19

A typical CANDU plant control system is very large. A CANDU 600 has about 1700 analog inputs, 1100 digital inputs, 64 analog outputs and 700 digital outputs. The system also has a contact input scanner which is used to initiate annunciation messages. This scanner monitors the status of 2000 digital signals, 300 times every second. If any one of these inputs changes state, the scanner automatically passes this information to the controlling computer. The photo shows the Gentilly-2 nuclear plant in Quebec, a 645-MWe reactor that began commercial operation in 1983. (Source: AECL)

Computer-controlled functions in several generations of plant designs							
Monitoring instrumentation							
Function	Douglas Pt.	Pickering 'A'	Bruce 'A'	Pickering 'B'	CANDU 600	Bruce 'B'	Darlington
Point alarm scanning	▨	▨	▨	▨	▨	▨	▨
Channel temperature monitoring	▨	▨	▨	▨	▨	▨	▨
Xenon monitoring or prediction		▨	▨	▨	▨	▨	▨
Reactor regulating system	▨	▨	▨	▨	▨	▨	▨
Unit power regulation		▨	▨	▨	▨	▨	▨
Boiler pressure control			▨	▨	▨	▨	▨
Moderator temperature control			▨	▨	▨	▨	▨
Reactor stepback			▨		▨	▨	▨
Flux monitoring & mapping			▨	▨	▨	▨	▨
Turbine monitoring		▨	▨	▨	▨	▨	▨
Turbine run-up		▨	▨	▨	▨	▨	▨
Fuelling machine control		▨	▨	▨	▨	▨	▨
Sequence of events monitoring		▨	▨	▨	▨	▨	▨
Primary heat transport control					▨		▨
Boiler level control					▨	▨	▨
De-aerator control						▨	
CRT messages (alpha-numeric)			▨	▨	▨	▨	▨
CRT graphics			▨		▨	▨	▨
Historical data storage			▨		▨	▨	▨
Safety system monitor			▨			▨	▨
Safety system trip					▨		▨

performed by these computers have evolved and been expanded with each successive design. Very early in the development of the CANDU control systems the objective was to eliminate manual backup systems by creating a system which was reliable, fault tolerant, and fail-safe. Since these systems were the first of their kind, Atomic Energy of Canada and Canadian industry obtained some of the first experience in the design, qualification, and installation of large, direct digital control systems.

The conservative nuclear industry certainly has changed. Recent conferences indicate that digital systems are now becoming more prevalent in all reactor systems. In fact, CANDU stations, as well as others, are now using computer-based logic for safety as well as control functions. In CANDU plants these new safety-related applications incorporate the experience that has been gained using computers for overall plant control. This movement to use computers in special safety systems has been based on the expectation of reducing costs, plus improving the production and safety reliability of the system.

At the present time, a comprehensive system that uses computers for all shutdown functions is being designed. It is anticipated that it will fulfil specific expectations and continue the good operating results experienced to date with similar computer applications. It is also expected that the CANDU plants will continue to expand use of computers in all aspects of plant control, and that previous experience will be fully utilized in future designs based upon remote data acquisition systems and data highway technologies.

CANDU prototype plants

The first CANDU plant that used computers for control was a prototype plant called Douglas Point. It had a single Control Data 636 computer which was used to provide alarm scanning, temperature monitoring, and power regulation.

The accompanying table shows the computer-controlled functions implemented in several generations of plant designs. All of the commercial CANDU plants after Douglas Point implemented control functions in two microcomputers. These computers operate in a master/hot standby configuration called DCCX and DCCY, respectively. In this configuration both computers receive all sensor information and they execute identical plant control programs.

Normally the control signals from only the master computer are connected to control the plant process. Should a fault be detected by hardware or software self checks, control is automatically transferred to the hot standby computer (DCCY). This is achieved by disconnecting the master's control signals and connecting the standby's control outputs to the processes. Individual control functions or all control functions may be transferred depending upon the type of failure detected.

The master/hot standby design has been used to date in all CANDU commercial power plants. The system has demonstrated an availability of 99.8% over an operating life of more than 50 system years.

As previously noted, current CANDU plants, as well as others, are now using computers in their special safety systems. The CANDU plants' special safety systems are totally separate and independent of the plant control system described in the accompanying table. Until relatively recently, computers were not used in these systems.

However, the advantages and benefits that were demonstrated when computers were used for control have proven to be just as relevant to the special safety systems. Consequently, the newer plant designs have started to incorporate computers in the special safety systems. Shutdown System One (SDS1) and Shutdown System Two (SDS2) are two that have received the most extensive use of computers. The Emergency Coolant Injection System (ECI) is the third special safety system where computers have been applied.

Shutdown system basics

A shutdown system consists of process sensors, reactivity devices (e.g., mechanical "gravity-drop" absorber rods) and intervening instrumentation and logic. If the plant is sensed to be operating in a potentially unsafe state (e.g., power too high, coolant flow too low) the reactivity devices are inserted to terminate the chain reaction very quickly. For reliability, the sensors and logic are triplicated.

Since the mid 1970s, CANDU reactors have employed two independent and equally capable shutdown systems. Each of these systems is composed of three independent and redundant channels of instrumentation. The outputs from these three channels are combined in a two-out-of-three voting scheme, which is then used to initiate a reactor shutdown.

Some major requirements that impact the design of these systems are:

- The system status, plus the trip or shutdown measurement and their setpoints, must be continuously displayed in the central control room.
- The system must be completely testable from the central control room. These tests should demonstrate system operation from the primary sensor to the shutdown mechanism.
- The logic must be capable of operating under adverse conditions (e.g., high temperature, or during an earthquake).
- The system must be designed to meet an unavailability target of 0.001. Thus the system is designed and routinely tested to ensure it will operate 999 out of every 1000 attempts.
- Two different measurements must be provided in each channel of both shutdown systems to detect each design basis accident.

The computerization of shutdown systems has developed in three stages:

- Monitoring of important shutdown system variables
- Computerization of selected shutdown system trip functions
- Full shutdown system computerization involving trip logic, operator interfaces, testing, and monitoring.

The first two of these stages were realized in the late 1970s and early 1980s. The third stage is currently being completed and a fully computerized shutdown system will be deployed in 1986.

The major benefits offered by these digital systems include:

- Lower overall costs
- Greater logic flexibility
- Improved testing procedures
- Improved man-machine interface
- Better availability (lower unavailability).

The easiest way to understand how computers are being utilized in CANDU safety systems is to examine specific applications. The following sections in this article describe examples of how such systems are used.

Shutdown system monitoring: Stage 1

There are two (4 X 750 megawatt) CANDU stations situated at the Bruce nuclear power generation site in Ontario, Canada. A monitor computer system has been designed for both these plants. These systems have recently entered service. For the Bruce 'B' station, the monitor system was installed before the plant started up while the system for the Bruce 'A' plant is being retrofitted into operating units.

The purpose of this monitor computer is to provide the operator with cathode ray tube (CRT) displays that incorporate information from all safety system channels. The initial reason for considering the installation of the system was to provide margin-to-trip alarms and displays for the shutdown system flux measurements. However, as the design progressed, functions were added to further improve the presentation of information to the operator. These additional features included:

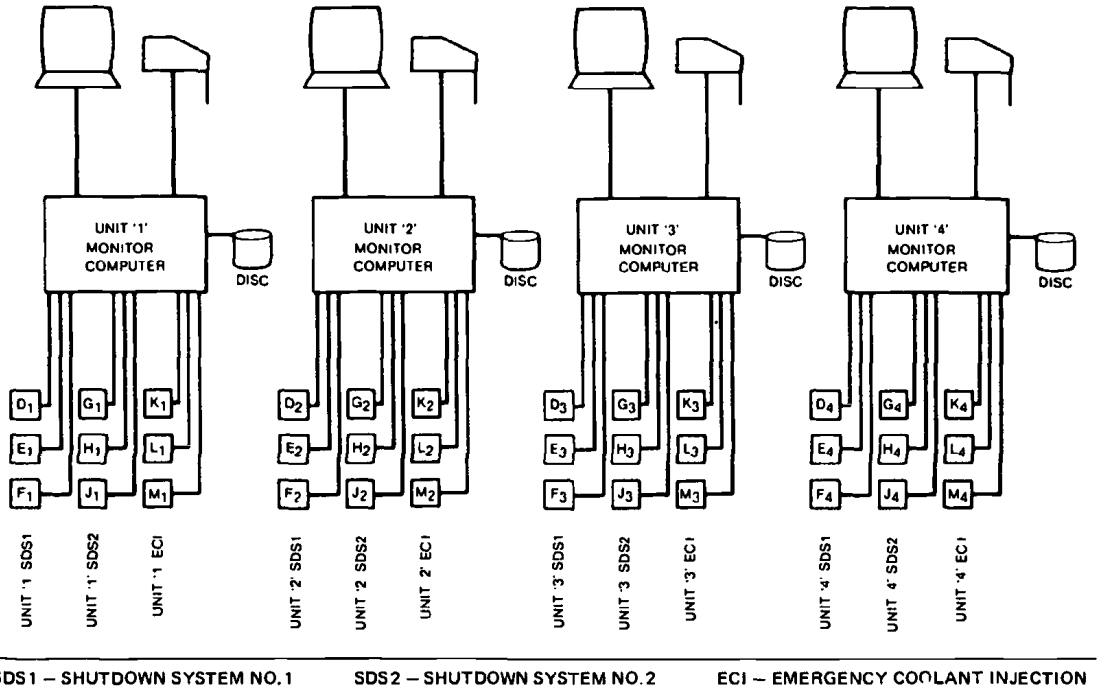
- Displays of process measurement values and setpoints
- Historical data storage and trend displays
- Recording of the value-at-trip during testing
- Special alarms to indicate system impairments.

Trip initiation: Stage 2

Shutdown systems in the 600-MW reactors are similar to those in other CANDU plants, with one exception. Some of the CANDU-600 trip functions required special conditioning logic and microcomputers have been used to implement this logic. These computers are called programmable digital comparators (PDCs) because they replaced the function of analog comparators and their associated conditioning. These PDCs have been in service since July 1982.

In contrast to the monitoring computer system that performs only a non-critical supervisory function, the PDCs perform the actual trip function for some of trip variables. In view of the critical nature of the PDCs,

BRUCE 'A' MONITOR COMPUTER CONFIGURATION



SDS1 – SHUTDOWN SYSTEM NO. 1 SDS2 – SHUTDOWN SYSTEM NO. 2 ECI – EMERGENCY COOLANT INJECTION

The figure shows the complete monitoring system for one station. The central monitor is a Data General MP-200 Micronova. This computer is completely isolated from any channelized shutdown system equipment because it receives data over fibre optic links from remote multiplexers. Each multiplexer is a Data General MP-100 Micronova. These multiplexers collect data from each of the channels in SDS1 and SDS2 and the ECI System. The portions of these three safety systems which initiate system operation use conventional analog instrumentation and relay logic. (Source: AECL)

a number of special design measures were adopted to ensure their reliability:

- Special software routines perform numerous checks on the computer memory, stored programs, stored data, input/output components, and computer instructions. These routines run continuously on-line during normal operation.
- A watchdog timer is provided to make each PDC fail-safe (i.e., trip the channel) in case of detected computer faults or outright computer failure.
- The software is kept very simple, and it is structured as a single loop with no interrupts. On alternate program passes, the trip software uses stored test data rather than field data to check its own operation.
- Each program pass includes a "check" to ensure that all parts of the software are executed in the correct order.
- Programs are stored in Programmable Read Only Memory (PROM).
- A number of mechanical and electrical modifications were made to seismically qualify the PDCs and to ensure that they were immune to electrically injected noise.

The programmable digital comparators are Data General MP100 Micronovas with 4K* of PROM. There are no peripherals other than the process input/output equipment that interfaces to these PDCs. The PDCs are designed in a minimum hardware configuration to enhance their reliability.

A fully computerized shutdown system: Stage 3

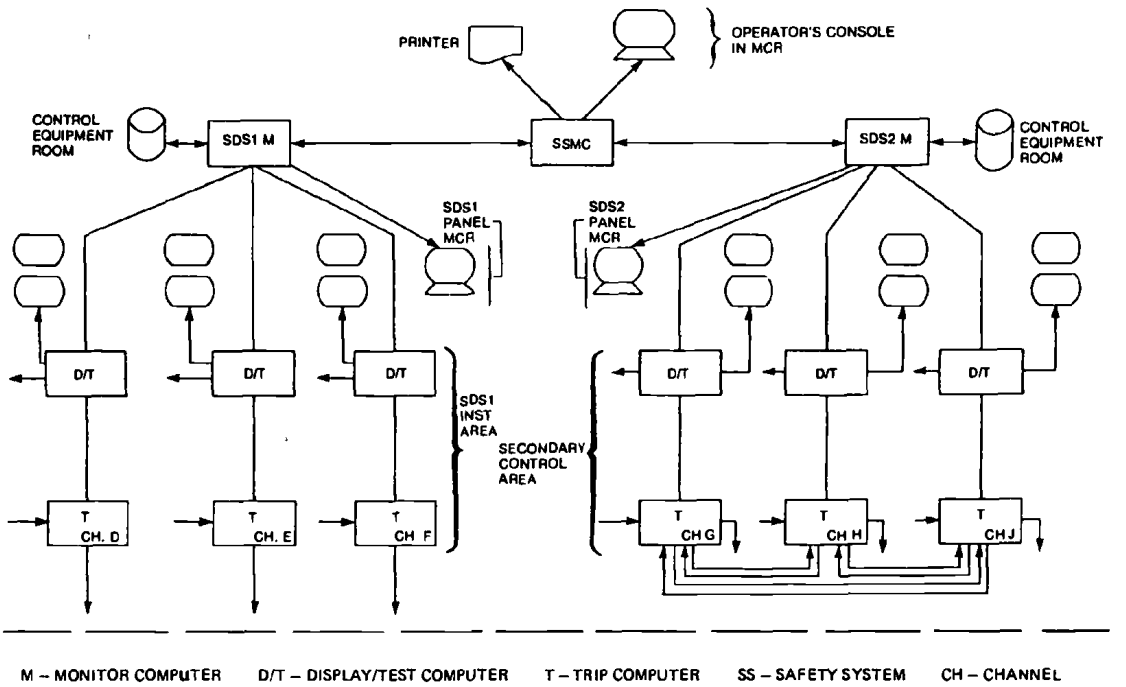
The Darlington 'A' plant is a multi-unit station patterned after the Bruce 'B' station mentioned earlier. This plant is currently under construction and the first unit will enter service in 1987. One unique feature of this station is that the shutdown systems (SDS1 and SDS2) use computers for all SDS functions in an integrated manner. (See the box on page 12 for description of computer hardware.)

Separate monitor computers are being used for each shutdown system. These two computers provide functions similar to the monitor computers described for the Bruce station. Each monitor operates independently and each receives data from three display/test computers about every two seconds. In the Darlington system these monitors also provide:

- An operator interface for the control of routine test sequences

* Kilobyte, a unit of core-memory size = 1024 bytes.

CONFIGURATION OF FULLY COMPUTERIZED SHUTDOWN SYSTEMS



The figure shows how the computers are arranged in the shutdown systems for one unit at the Darlington Station. Shutdown Systems One and Two (SDS1 and SDS2) use a total of 15 computers. These computers are isolated from one another because any data communication between computers occurs over fibre optic links. These data links are designed to operate asynchronously at up to 19.2K bits per second. Each link normally transmits about 500 bytes every second.

The computer at the top of this figure is called the Safety System Monitor Computer (SSMC). It is included in the design so that information from the SDS1 and SDS2 monitors can be presented to the operator at a central location. This processor controls the peripherals at an operator's desk which is located in the centre of the main control room (MCR). (Source: AECL)

- An operator interface for the recalibration of the neutron flux detectors
- A backup display facility for the channelized displays.

The operator interacts with these monitors in two ways. The operator can obtain information from either monitor by making requests through the Safety System Monitor Computer at his control desk. In addition, the operator can select functions through special keyboards at the two main control room panel areas dedicated to SDS1 and SDS2. Beside each of these keyboards are general purpose display (GPD) CRTs that present the display selected. The GPD CRT will normally be used for prompting the operator through test sequences and flux-recalibration procedures.

Channelized display/test computers

In each channel of both shutdown systems there is a display/test (D/T) computer. This processor receives data from an associated trip computer. This data is converted and used to provide bar graph displays of trip parameter measurements on channelized CRTs. This information is also transmitted to the appropriate monitor computer. These D/T processors not only provide the channelized displays but they also act as a buffer for the channelized test controls and other channelized inputs or outputs that must be isolated from the monitor computer or the main control room.

Trip computers

The trip computers process all of the parameters required from the two shutdown systems. They are similar to the CANDU-600 PDCs and they provide these functions:

- Sample field inputs
- Make all trip decisions
- Dynamically compensate flux-detector readings
- Receive and apply flux-detector recalibration factors
- Transmit data to the D/T computer.

Future trends

The successful application of computers in the operation control and, more recently, safety systems has continued to demonstrate the benefits of artificial intelligence in CANDU plants. The rapid pace of developments in the computer industry also has opened new opportunities for innovation. At this time, it would appear there are three areas where changes can be anticipated.

First, distributed data acquisition and/or control will be used to reduce plant wiring costs and construction schedules. This trend is exemplified by the current CANDU-300 design, which is incorporating a control system using data highways and remote multiplexers.

The second area where change will occur is in the enhancement of the man-machine interfaces in the control room. New display technologies and additional computing power have become available that will reduce costs and improve the quality of the man-machine interfaces.

The third area where innovations will occur are in the spinoffs or unique requirements associated with individual projects. There are specific situations where the hardware and software experience or systems used in the CANDU plants can be adapted for use in other applications. Examples of these include the use of computers in emergency response facilities or small-scale power projects.

Computer hardware for the CANDU shutdown system

The computers in the design for a fully computerized shutdown system are standard off-the-shelf products. All except for the Shutdown System Two (SDS2) trip computers are General Automation 250 series central processing units (CPUs) connected to General Automation input/output (I/O) hardware. The SDS2 trip computers are DEC LSI 11/23 processors connected to Computer Products I/O. All computers have 16-bit central processors. The Shutdown System One (SDS1) and SDS2 monitors have 64K words of memory and a 10.2M byte disc.

The display/test (D/T) computers and the Safety System Monitor Computer (SSMC) have 32K words of random access memory (RAM) and 16K words of read only memory (ROM). Typical inputs and outputs and associated hardware are listed in the accompanying table. These computers and the trip computers are stand-alone devices and execute their ROM resident programs in a continuous loop.

Display hardware

The video display generators (VDGs) that provide the CRT displays are RAMTEK model 6210 display generators. The generator is capable of colour graphic and alpha-numeric displays with a maximum resolution of 640 X 480 pixels.

Environmentally and seismically qualified CRTs are connected to the display/test VDGs. The monitor computers have colour displays that are not seismically qualified. The monitor VDGs have additional hardware providing a vector plotting facility for trend displays.

Field connections

All computers in the system are connected to the field signals via a specially designed termination module. This module can be used with several different makes of computer hardware and it has been designed to provide passive noise suppression and filtering for all of the inputs and outputs for each computer. In addition, this module contains fibre optic transducers, state indication for digital inputs and outputs, and a watchdog for each processor.

Communications and data link interlocks

All regular communications in this system are processed by DMA controllers in each computer. The information is passed asynchronously in all cases and most of the time in one direction only. The design does allow an operator to pass data from the monitor computers to a D/T computer and a trip computer. However, this feature is interlocked so that the downward transmission of data can only occur in one channel in each SDS at a time. The interlocks controlling this type of data transfer are external to the computers themselves and are part of the fibre optic transducer circuits in each termination module.

The ability to send data to an individual channel is used by the operator to control the testing of the channelized instrumentation and to recalibrate the flux-detector readings in a trip computer.

Typical Hardware Characteristics: Fully Computerized Shutdown System

Computer item	Safety system monitor	SDS monitoring	Display test	Trip
RAM	32KW	64KW	32KW	16KW
ROM	16KW	–	16KW	16KW
Serial links	3	5	4	1
Disc	–	1	–	–
Keyboard	1	1	–	–
VDGs	1	1	2	–
CRTs colour	1	1	–	–
Mono	–	–	2	–
Digital in	16	64	64	32
Digital out	32	32	128	48
Analog in	–	–	16	48
Analog out	–	4	4	4

RAM: Random access memory VDG: Video display generator
ROM: Read only memory CRT: Cathode ray tube

Software

All application software in this system is specially designed. Most programs, including the trip software, are written in FORTRAN. A vendor supplied operating system is used in the monitor computers.

The SSMC, D/T, and trip processors have very simple software architectures and typically execute one pass through a main program loop every 30 to 100 milliseconds.

As has been the practice on previous projects, each computer will contain several self-checking features. These are most extensive in the trip computers and they are designed to ensure that the central processing unit, memory, and input/output hardware function properly. If a computer detects a serious self-check fault or fails to execute its programs within a pre-defined time period, the watchdog for that computer automatically places the computer outputs in a safe state.