AECL - 9948

RELIABLE, FAULT TOLERANT CONTROL SYSTEMS FOR NUCLEAR GENERATING STATIONS.

T.O. McNeil
R.A. Olmstead
S. Schafer

AECL CANDU
Sheridan Park Research Community
Mississauga, Ontario L5K 1B2
Tel (416) 823-9040

Presented at the ISA Instrument Society of America
TORONTO SECTION INC.
33rd Annual Power Instruments Symposium
21-23 May 1990, Toronto

RELIABLE, FAULT TOLERANT CONTROL SYSTEMS FOR NUCLEAR GENERATING STATIONS.

T.O. McNeil
R.A. Olmstead
S. Schafer

May 17, 1990

Two operational features of CANDU Nuclear Power Stations provide for high plant availability. First, the plant re-fuels on-line, thereby eliminating the need for periodic and lengthy refuelling "outages". Second, the all plants are controlled by real-time computer systems. Later plants are also protected using real-time computer systems.

In the past twenty years, the control systems now operating in 21 plants have achieved an availability of 99.8%, making significant contributions to high CANDU plant capacity factors.

This paper describes some of the features that ensure the high degree of system fault tolerance and hence high plant availability. The emphasis will be placed on the fault tolerant features of the computer systems included in the latest reactor design - the CANDU 3 (450MWe).

CANDU Safety Principles

Before describing these systems, we need to present the CANDU Safety Principles, since they guide the architecture of the control and protection systems.

Process systems associated with safety are defined as those systems which perform or support the following safety functions:

a. shut down the reactor
b. cool the fuel
c. prevent the release of radioactive material
d. monitor and control the plant to maintain the above functions

All systems (process and control) in CANDU plants are assigned to one of two GROUPS. Each group is capable of performing safety functions. The Group 1 systems are the systems used for normal plant operation. The Group 2 systems are the backup safety systems which are provided to mitigate the effects of failures of the Group 1 systems, including failures which may be caused by postulated events such as earthquake, flood, fire, and tornado.

The two groups use diverse means of performing the safety functions. The diversity and separation of the two groups provides against common-cause failures due to postulated events, maintenance errors or design errors.

Control Computer System Configuration (Group 1)

Previous CANDU plants used dual redundant computer systems to control the plant. One computer system controls the plant while the other runs in a HOT STANDBY mode. In the event the controlling computer fails, the outputs from the HOT STANDBY machine, which sees the identical inputs, are connected to the plant. There is almost no communication between the two computers to minimize the possibility of cross link failures.

The CANDU 3, the most recent design, uses a distributed control system (DCS) which combines modern proven programmable controller and data highway technology with a proven dual-redundant computer configuration. The DCS, an integrated plant-wide system, performs control and data acquisition functions for the Group 1 plant systems. The PDS, a Plant Display System, is linked to the DCS to provide plant monitoring, operator interfacing, and data storage/retrieval functions.

The scope of the DCS includes all signal scanning and control functions for the following systems:

- reactor regulation
- moderator and auxiliaries
- heat transport and auxiliaries (including pressure and pressurizer level control)
- shield cooling
- boiler level (feedwater) control
- turbine - generator power regulation
- conventional plant process systems
- service water systems
- heavy water management
- irradiated fuel bay cooling

The signal scanning function includes all Group 1 alarm scanning and data acquisition for the Plant Display System. The signal processing function includes interlocking, sequential control and feedback control of valves, pumps, heaters, reactivity mechanisms, etc, as well as higher level group control and plant automation.

Control Computer System Architecture

The DCS is a geographically distributed digital system consisting of a number of stations linked by data highways (refer to figure 1). Programmable control processors, distributed among the stations, perform logical (binary) and numerical (analog) signal processing functions.

The instrumentation in Group 1 in all CANDU's is grouped into three channels. (A,B,C). Duplicated sensors are assigned to channels A and B. Triplicated sensors are assigned to channels A,B,C. The DCS is divided in three separate control channels (A,B,C) to support these three channels. Each DCS channel consists of a number of stations linked by two separate highways (A1/A2,B1/B2,C1/C2) (refer to figure 2). An additional highway is used to link some stations to a special PDS interface, to provide a high resolution contact scanning function for event sequence recording.

Two diagnostic stations are linked to the highways, DS1 for A1,B1,C1, and DS2 for A2,B2,C2. These stations provide on-line facilities for fault annunciation and identification to the module level, for displaying signal values from any station, for inputting test data, for displaying and adjusting control system tuning parameters, and for reading the contents of any application program memory (EPROM) in any control processor, bus coupler or highway address transmitter.

CANDU Computer based Shutdown System

The role of the shutdown systems is to shut down the plant if one or more process variables exceeds preset "trip" limits. Before 1982, these "trip" signals were generated using analog comparators and relay logic. In 1982, trip signals generated by real-time digital computers were installed at Point Lepreau and Gentilly II power stations. At these stations, the computer based trips replaced most of the trips implemented using analog comparators and relay logic. Computers offered the ability to design more complex logic with fewer components (and hence higher reliability) and supported on-line continuous self-testing.

Early in 1982, Ontario Hydro and AECL initiated a development program to evaluate a completely computerized shutdown system. The functions of this system included, in addition to tripping the reactor in the event of off normal plant operation, CRT displays of safety parameters, (eliminating conventional panel meters completely), computer assisted testing of the system, and continuous on-line monitoring of safety system operation to detect component failures.

After successful completion of the development program, feasibility of a fully computerized shutdown system was proven. The design of the safety systems at Darlington proceeded based upon the results of the development program. These systems are now installed and operating at Darlington.

Shutdown System Architecture

In all CANDU plants there are two diverse shutdown systems, Shut Down System 1 (SDS1), and Shut Down System 2 (SDS2). Each of these Shutdown systems consists of three channels of instrumentation. (SDS1 channels D,E,F /SDS2 channels G,H,J). These channels support triplicated trip functions. A plant trip occurs when two of three channels of a given trip function indicate that a trip parameter has exceeded a trip threshold.

Figure 3 shows the hierarchical configuration for the computers in SDS1 and SDS2. The bottom layer consists of 6 independent computers which support the trip functions in each of the six shutdown channels (D,E,F and G,H,J). The bottom layer or 'trip' layer performs the following functions:

- reads and checks safety system parameters
- performs the trip determination algorithm and issues trip signals
- performs self-checks
- drives channel alarm windows on the main control room panels
- sends plant parameters and trip computer status information to the Display/Test computers via fibre optic links.
- receives calibration data for in-core self-powered flux detectors from the Display/Test computers via fibre optic links.

The layer above the trip computers is the Display/Test computers. There is one Display/Test computer per channel. These computers perform the following functions:

- drives two panel mounted CRT's providing the operator values of the process and neutronic trip parameters and their setpoints.
- issues test signals to field devices on command from the Monitor Computers.

The next layer contains the Monitor Computers. There is one Monitor Computer per shutdown system. Each Monitor Computer performs the following functions:

- drives a panel mounted CRT with keyboard that allows the operator to initiate system test procedures and to input calibration information.
- drives a second CRT at the operator's desk for displaying shutdown system information on demand.
- performs consistency checks on the data (e.g. cross channel comparisons of similar parameters.)
- prints alarms
- prints test results for permanent records
- transmits alarms and test results to another Shutdown System Monitor Computer for long term storage.

The top layer (4th), the Shutdown System Monitor Computer, accepts data (alarms and test results) via serial links from all 8 shutdown systems at the Darlington plant (4 reactors, 2 shutdown systems each). This computer performs historical data storage, with the ability to recall information off-line.

Control System Retrofits

AECL, is assisting a number of Canadian and U.S. Utilities with control system retrofits

for nuclear and fossil power plants.

For example, retrofiting feedwater control loops in Boiling Water Reactors (BWR's) and Pressurized Water Reactors (PWR's) with digital computers, solves the current equipment obsolescence problem and promises better startup and transient control, reducing some of the trips now experienced on startup. These retrofits provide a number of advantages in addition to better control and spare parts availability:

- increased reliability over single channel analog systems
- decreased control room operator workload during post trip boiler level transients
- flexibility to introduce changes in the future
- reduction of calibration work load

Computer System Design Goals

The following design goals have evolved over the twenty years since the first CANDU commercial power station (Pickering 'A") went into service in 1971. They are:

- Superior control of startups & transients
- Highly reliable plant protection systems
- Correct system operation in the presence of faults
- Quick detection and correction of failures
- Operator aids to mitigate human failures
- Quality design and lower construction costs

How do these systems described above meet the design goals outlined in the introduction of this paper ? Let's look at each goal.

Superior Control of Startups and Transients

CANDU plants use an integrated plant controller which controls all major loops in the plant from reactor, heat transport loop, feedwater/steam flow and unit power regulation. The plant can be taken from zero power, hot critical to full power automatically. For example, transfer from auxiliary feedwater to main feedwater occurs without manual intervention. The controller uses multivariable control. The gains of the controller are variable depending upon current operation status. This approach has proven very successful .

For example, a controller with feedforward terms, variable gains, and suppression of integration 'windup' effects provides superior transient response. Figure 4 illustrates the improved transient response when the CANDU feedwater control algorithms are retrofitted to a BWR reactor compared to the response achieved from the original analog controller supplied with the original plant.

Highly Reliable Plant Protection Systems

A recent analysis of Significant Event Reports (SER's), revealed that human error was a component of 40% - 60% of all SER's. Also, 50% of these occurred during testing and maintenance. The shutdown systems must be tested periodically during plant operation. In plants using conventional instrumentation, this meant the operators need to take one channel "off-line" and manually inject "test trip" signals to assure that the system would operate if it was needed. There is a great deal of instrumentation in the 6 shutdown system channels, and the possibility of operator error causing a plant trip is significant.

The new computer based systems have a large number of features which aid the operator in testing and monitoring the health of the shutdown systems. First, all computers perform self-checks and alarm abnormalities. Second, the operator is presented clear colour graphic screens which present parameter values in a concise way and allow the operator to quickly make channel to channel comparisons. Third, the operator is assisted in performing periodic testing. That is, the system injects trip signals non-intrusively, and either confirms that the trip logic has functioned correctly or that there is a fault.

Diversity of equipment in the two shutdown systems is a licensing requirement in Canada to mitigate design failures. For example, the SDS1 Trip Computers and SDS2 Trip computers are manufactured by two different companies. In addition the SDS1 Trip computers are programmed in FORTRAN and assembler language. The SDS2 Trip Computers are programmed in PASCAL and a different assembler language.

Correct Operation in the Presence of Faults

The plant controller must not make false corrections to the plant based upon erroneous signals from failed instrumentation. CANDU plants use extensive signal validation on all inputs. Parameters with multiple sensors are validated by the controller through the use of "spread checking" . In addition to spread checking, selected outputs from the computer are "wrapped around" as inputs to allow checking of proper operation. All inputs are checked for rationality and consistency. Computer faults are alarmed, and in the case of the plant control computers, the "hot standby" computer takes over if the main control computer fails. If both control computers fail, a "watchdog circuit" ensures that all outputs are driven to the safe state.

Quick Detection and Correction of Faults

Finding failed equipment and replacing it, is the key to high plant availability. The computer systems are the major aids to maintenance because they perform self-testing, and assist the operator in periodic testing and annunciate instrumentation failures. The control computers support off-line diagnostic programs for use by the maintenance staff in checking computer I/O circuits, sensors, and actuators.

Operator Aids to Mitigate Human Failures

CANDU plants' man-machine interface have a number of key features which aid the operator in understanding plant status and taking the correct action. For example, discrepancy lights indicate when the main control handswitch is inconsistent with the position of the corresponding field device.Also an off normal handswitch panel light indicates when the handswitch position does not reflect a predefined normal configuration. Extensive use of colour-coded alarm CRT messages, with the minimum of alarm windows, alarm conditioning, alarm prioritization, and alarm grouping provides the operator with top level information immediately, and allows him to quickly retrieve more details as required.

Automation of most manual tasks allows the operator to work at a "plant supervisory" level giving him more time to analyze situations. In any postulated event, the operator need not take action for at least fifteen (15) minutes.

As mentioned earlier, the non-intrusive testing and automated testing performed by the shutdown system computers mitigate human errors.

Future CANDU plants will include computer systems that will automate some of the "cognitive" tasks of the operator in addition to the manual tasks now automated. Plant vital signs indication, electronic procedures, dynamic equipment status displays, and pattern recognition functions will all be features of future CANDU designs.

The most important human factors improvement for the CANDU 3 plant is the elimination of conventional, fixed format control panels from the control room. Information will be displayed and control actions initiated through CRT/keyboard consoles. Information and procedural guidance will be presented to the operator in combinations that will suit the context of the situation he is dealing with. He will no longer have to gather information from geographically separate panels.

Quality Design and Lower Construction Costs

The CANDU 3 designers are using a number of design aids to improve the quality of their work.

For example, the design of the software for these computers follows a software development plan which ensures the software conforms to established technical and functional requirements. The plan generally follows the Canadian Standard for Software Quality Assurance CSA Q396 and has been influenced by the International Electrotechnical Commission's standard IEC 880. The plan covers topics such as: Surveillance of Activities, Project Management, Sub-contractor control, Standards, Practices and Conventions, Software Development & Testing & Validation, Technical Design Review, Software Documentation, Software Configuration Management, and Test Control. The plan also requires the use of a detailed Programmer's Handbook. This handbook sets out coding standards, and a Test Overview Document defining the test program.

AECL is presently investigating the use of more formal software design methodologies to ensure high quality in safety critical software.

Distributed Control presents another opportunity to increase quality, and reduce construction costs. Given that many of the "connections" between sensors, controllers, and actuators, is now defined by software in distributed control architectures, the design process is amenable to automation. Savings at the site are achieved through the use of distributed control. since much of the wiring and cabling is reduced by the data highways. Approximately 6 months of site work is saved along with approximately $1 million savings in equipment costs.

Summary

The computer systems used in the control and protection of CANDU plants have demonstrated the advantages of using computers in control and safety applications. In summary these benefits are:

- provide superior startup and transient control
- correct system operation in the presence of faults
- quick detection of failures
- defense against human failures
- enhance the ability to produce higher quality designs
- lower design and construction costs

Figure 1 CANDU Control System Geographic Distribution

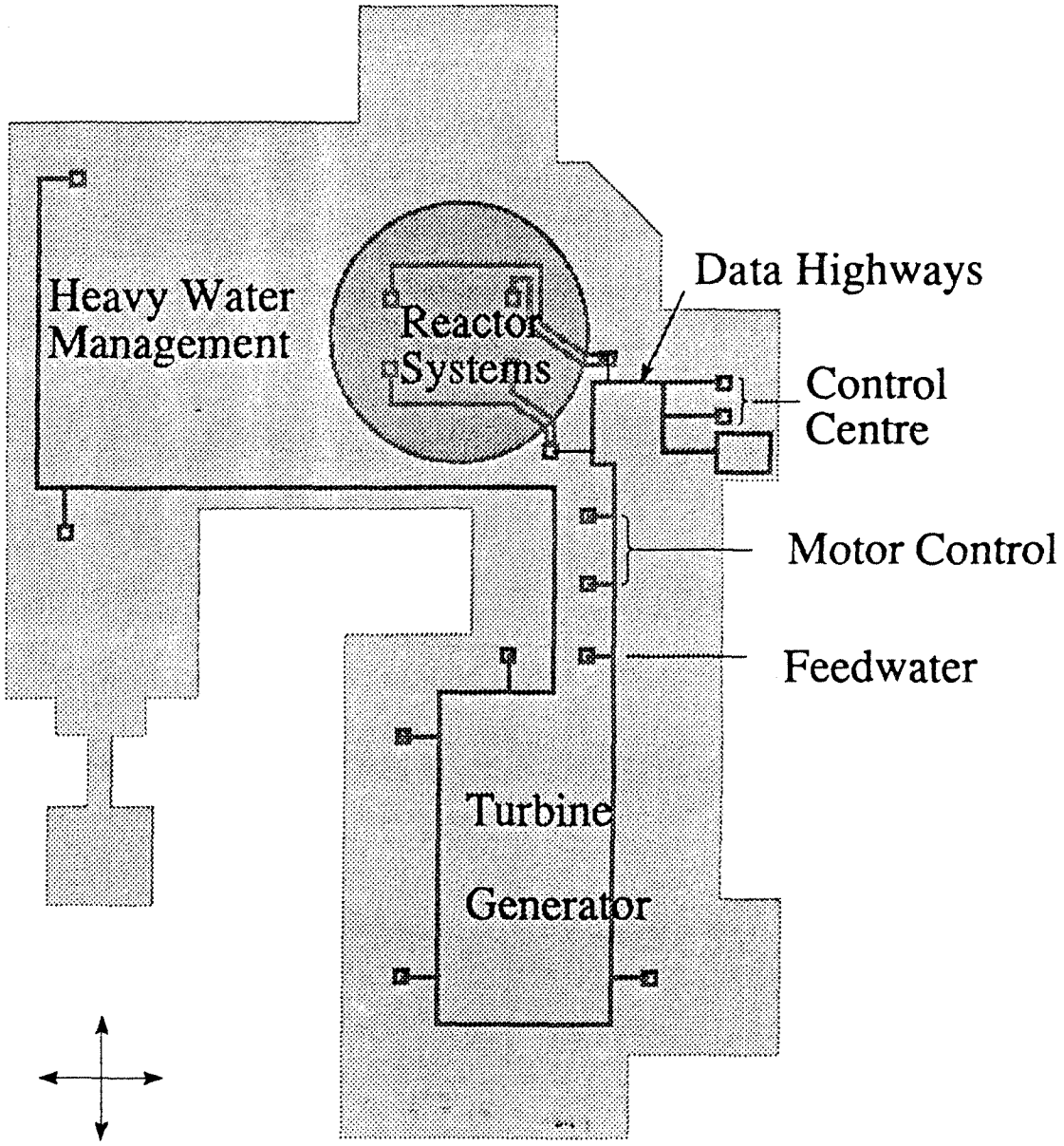


Figure 2 CANDU Distributed Control System Architecture

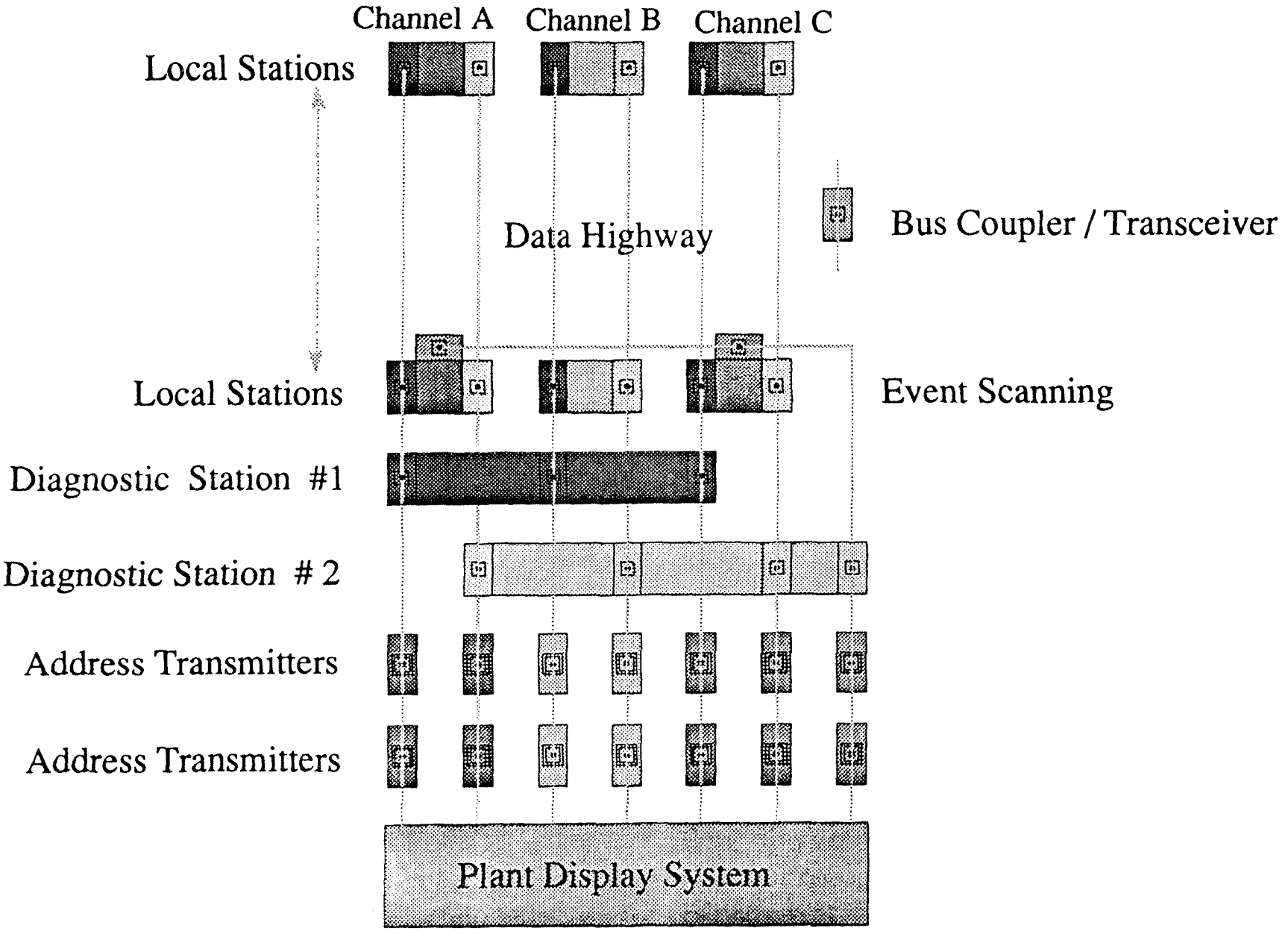


Figure 3 Configuration of Fully Computerized Shutdown Systems

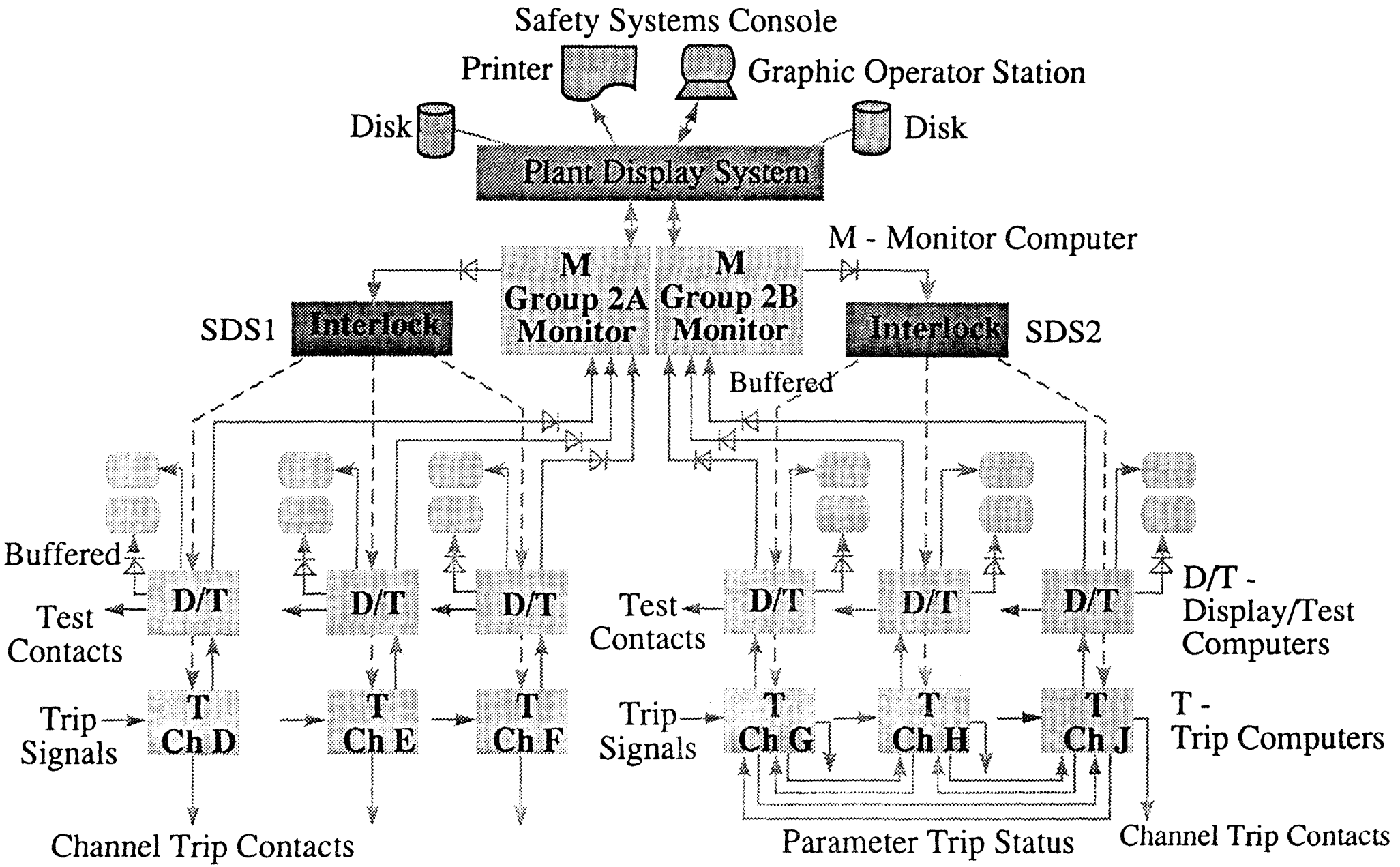
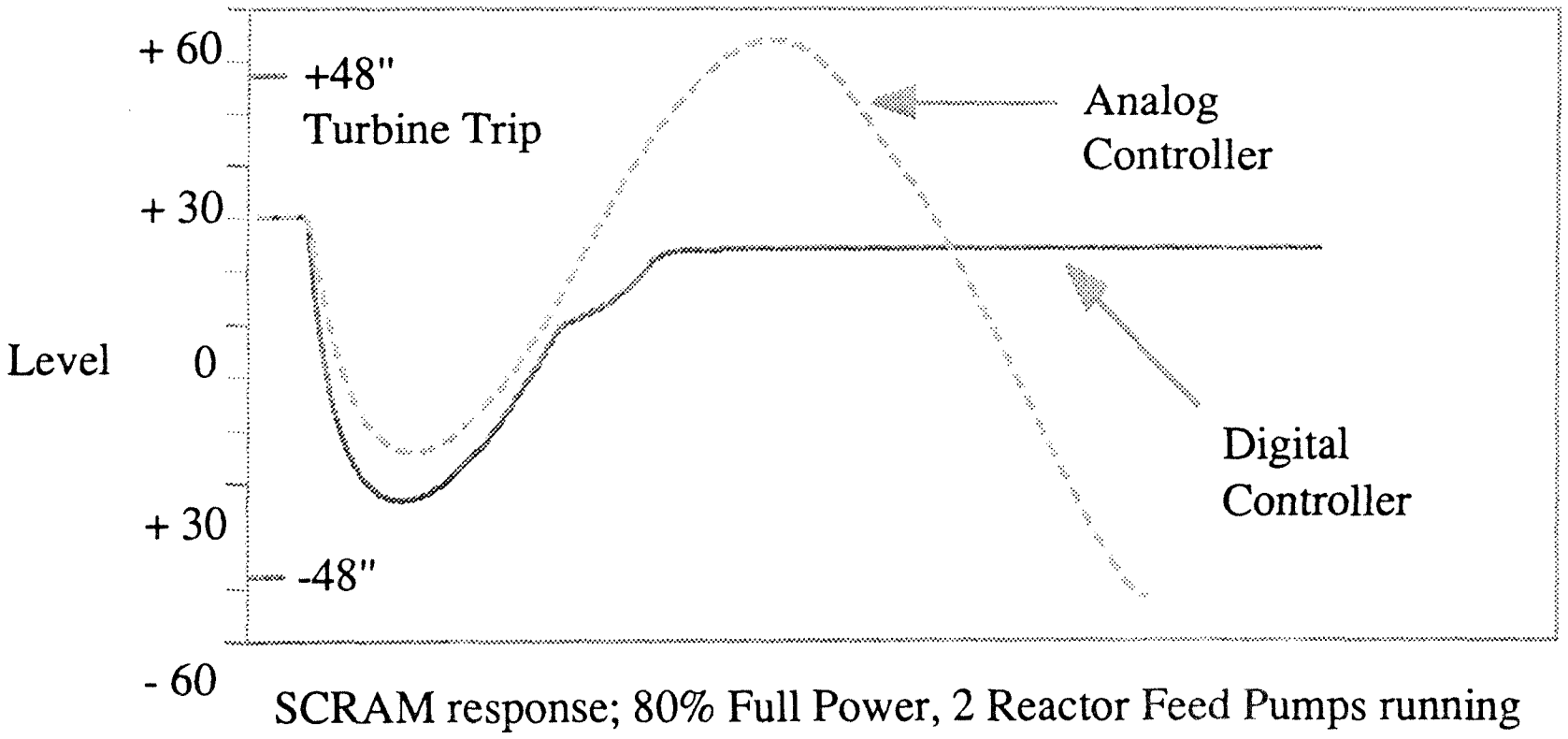


Figure 4 Digital Control vs Analog Control Transient Response



SCRAM response; 80% Full Power, 2 Reactor Feed Pumps running