Computerized Shutdown Systems

- CANDU reactors are designed with ***two shutdown systems*** to provide a combined unavailability target of 10^{-6} years/year.

- These special shutdown systems are **physically** and ***functionally*** separate from the process control systems and from each other.

- Each reactor shutdown system is designed to be fully capable of ***independently shutting down the reactor*** when called upon to do so.

- The special shutdown systems are designed, built and maintained to a very ***high quality assurance*** standard.

- These systems are designed to ***fail-safe*** so that safety action will always be provided, perhaps unnecessarily, in the event of system or device failures (i.e. such as loss of power).

- ***Shutdown System Number One*** **(SDS1)** utiiizes neutron absorbing rods (i.e. stainless steel coated cadmium rods) which are poised above the reactor core (i.e. ***vertical*** core access) and ***drop by gravity*** upon a request for shutdown (i.e. ***de-energize*** the clutches holding the rods above the core).

- ***Shutdown System Number Two*** **(SDS2)** injects a liquid chemical neutron absorber into the core through horizontally mounted injection nozzles (i.e. ***horizontal*** core access) upon a request for shutdown (i.e. fail-open control valves are driven open by venting to allow the poison injection to proceed).

- Note the ***diverse*** and ***independent*** reactor shutdown mechanisms.

- For ***reliability*** purposes and to ensure that no ***single failure*** prevents a necessary reactor trip, each system consists of ***three*** identical instrumentation and logic trip ***channels*** (i.e. triplicated).

- The system safety action is initiated if ***two of the three*** channels detect a condition requiring reactor shutdown. This is referred to as ***2 out 3*** consensus logic.

- A ***single channel*** tripping will not trip the reactor but has placed only its channel output devices in the ***safe state*** and initiated the corresponding ***alarms***. Now either of the remaining channels can initiate safety action when that channel also senses and responds to the trip parameter condition.

To date, there are ***four evolutionary phases*** of CANDU shutdown system trip logic design to present times from the traditional ***analog*** approach to the ***fully computerized*** system. It is important to note that the shutdown system itself (i.e. the physical system design) remained a consistent design over the years, but the control logic implementation strategy gradually become more and more computerized.

Typical Trip System Parameters

- It is worth considering typical shutdown system trip parameters for illustrative purposes. In each case the ***trip parameter*** and ***trip level*** is selected by safety analysis to ensure that the licensed fuel temperature limits are not exceeded. The parameters will trip with an ***adequate margin*** to the analyzed safety limit to ensure continual safe performance.

Neutronics

Neutron Flux Level High *- reactor power level is too high*

Neutron Rate Log *(Rate of Change of Logarithmic Power High) - rate of change in power is too fast*

Process

Steam Generator Level Low *- impending loss of principle heat sink*

Feedwater Line Pressure Low *- impending loss of principle heat sink*

Pressurizer Level Low *- unexpected low heat transport inventory*

Heat Transport Pressure High *- energy mismatch, reactor power too high*

Heat Transport Pressure Low *- impending heat transfer problems, boiling & cavitation*

Heat Transport System Gross Flow Low *- impending heat transfer problems*

Reactor Building Pressure High *- possible hot fluid leak in containment or loss of vacuum*

Moderator Level Low *- possible overrating of those channels still moderated*

Moderator Temperature High *- lower subcooling margin for moderator*

Manual

Manual Channelized Trip Pushbuttons (with common or individual capability)

Traditional Shutdown System Trip Logic - original design

- A shutdown system consists of process and neutronic ***sensors***, ***reactivity devices***, ***comparator logic instrumentation***, ***man-machine interfacing*** (MMI) devices as well as ***cabling*** and ***interfacing relays***.

- If any of the trip parameters are sensed to be operating ***beyond the acceptably safe margin*** to the analyzed unsafe state (i.e. power level too high, coolant flow too low, etc), then that parameter in that channel is recognized as being tripped and so the channel is ***de-energized*** in an attempt to trip the system (and thereby the reactor).

- As mentioned before, ***2 out of 3*** majority voting must occur before the system is tripped.

- Once ***two channels*** are tripped or de-energized, the final reactivity device control circuits are de-energized and safety action is initiated (e.g. shut down rods drop into core or liquid poison is injected) to shutdown the reactor.

- Even if one shutdown system does trip the reactor, the alternate Special Safety System remains poised to also trip the reactor, if called upon to do so, independent of the actions of the other shutdown system.

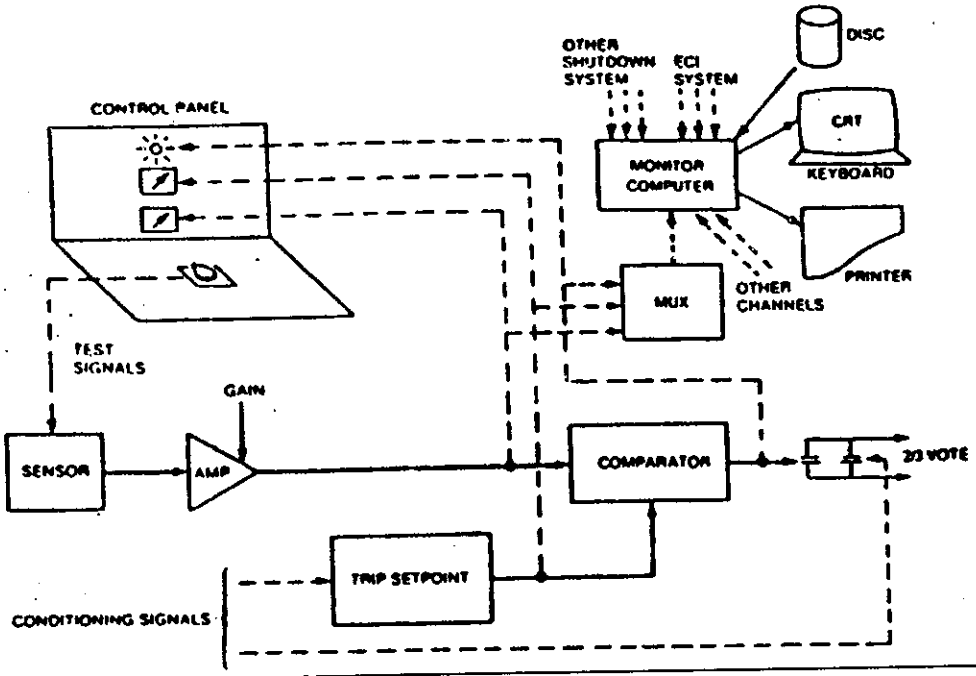


Figure #1 – Traditional Analog Shutdown System

Traditional Shutdown System Trip Logic - Operator Interfacing

- All ***trip signals***, ***trip setpoints*** and ***trip status information*** are ***continuously displayed*** in the main control room via conventional instrumentation devices.

- Manual controls allow the operators to ***periodically test*** the shutdown system channel devices from sensor to final reactivity device.

- Note that an ***entire channel can be tripped*** during a test condition but that the reactor would still be operated at power since ***a second channel has not tripped***.

- The ***unavailability target*** for each special shutdown system of 10^{-3} yrs/yr (i.e. 8.76 hours per year) must be verified by an on-going shift-based ***testing program*** to ***demonstrate the availability*** of the system to function if called upon to do so.

The trip logic in this design is implemented by ***relay logic*** while operator displays are small ***panel mounted meters and lights*** while operator controls are pushbuttons or handswitches. Data monitoring and logging was quite limited for this design and usually consisted of multipen trend recorders. This was an obvious area for human-system interfacing improvements.

Traditional Shutdown System Trip Logic with Monitoring Computers - first evolution

- The shutdown system ***trip circuitry*** and ***man-machine interfaces*** remained fundamentally unchanged from the traditional design - so that ***signal comparisons***, ***decision making***, ***trip initiation*** and ***man-machine interfacing*** remained as originally designed and proven functional.

- However, a new ***monitoring computer*** system was connected to the trip channels by rigorously ***buffered*** unidirectional interfaces.

- These ***one-way*** buffered interfaces were designed and tested to ensure that no faults in the computer system could possibly be ***propagated*** back into the trip circuit to ***degrade*** or ***disable*** the trip circuit functions.

- Once the safety system data was available within a computer system, then unlimited ***data manipulations***, ***statistical checks*** and ***comparisons*** could be made along with flexible and informative display capabilities.

- The monitoring computer system improvement consisted of a ***remote multiplexor***, located in each shutdown system channel, which obtains the channel parametric data.

Traditional Shutdown System Trip Logic with Monitoring Computers...continued

- This data can then be ***displayed*** on convenient bar chart or analog trend displays on a selected CRT in the main control room.

- The computer can also give the operator an early warning if a variable is detected too close to a setpoint (i.e. impose an operating margin threshold) , or for failed signals or signal discrepancies among similar signals.

- This manner of providing information to the operator can be much more ***user friendly*** while making it easier for the operator to be aware of ***small changes*** or to be alerted early of an ***impending upset*** condition.

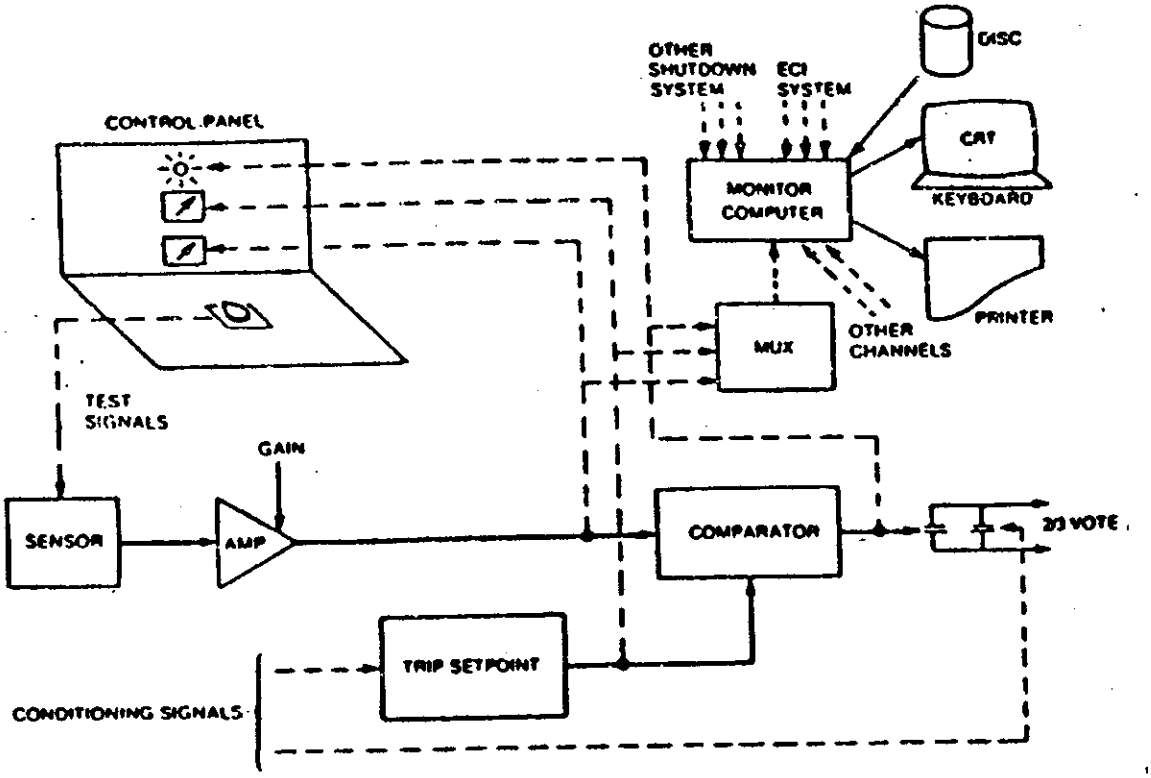


Figure #2 – Traditional Analog Shutdown System with a Computerized Monitoring Interface

Programmable Digital Comparators (PDC's) - second evolution

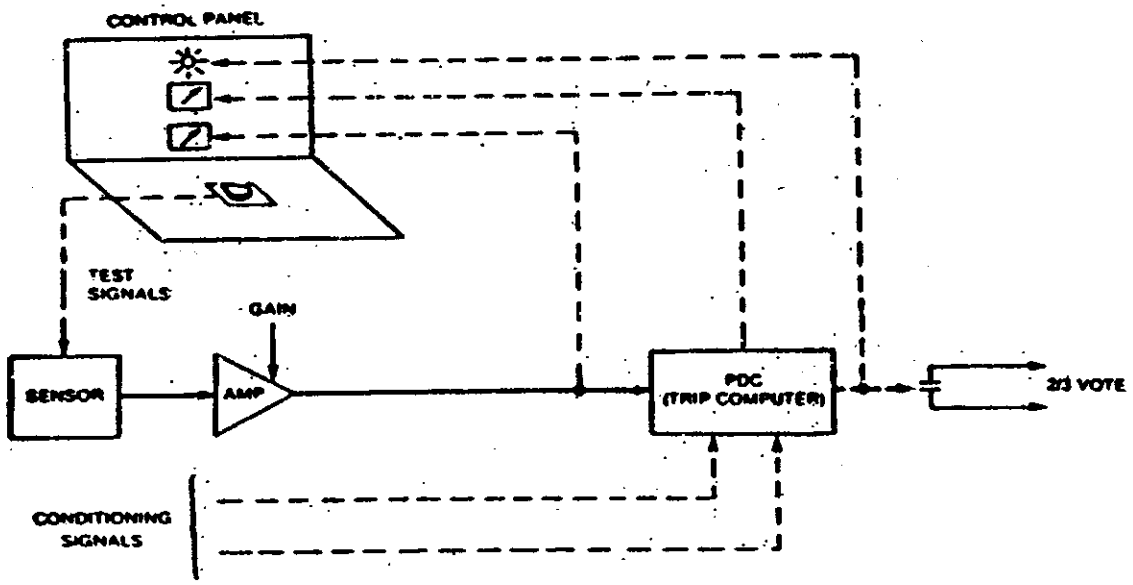
- The next step taken in the evolution of the trip channel implementation was to digitize the process ***trip comparison*** and ***logic circuitry*** by using digital ***microcomputers*** or programmable digital comparators (**PDC's**) in place of the analog devices.

- The shutdown system instrumentation still consists of the analog process and neutronic ***sensors*** and ***man-machine interfacing*** devices as well as ***cabling*** and ***interfacing relays*** which remained fundamentally unchanged from the traditional design. The ***neutronic trips*** were still implemented by the traditional analog circuits.

- But the ***process signal comparisons***, ***decision making***, and ***trip initiation*** were now moved to a ***programmable logic base***.

- Note that this method of design change is ***quite conservative*** so that the condition of the final configuration is ***always known***. As well, an additional diversity was provided in that the ***neutronic trips*** were provided by ***analog logic*** while the ***process trips*** were initiated by ***digital logic*** - a gradual design progress was accomplished.

- The PDC's are provided with a ***simple hardware timer***-like device called a ***watchdog*** timer. The watchdog monitors the ***performance of the PDC*** to ensure that expected operations are performed within an ***expected time interval*** to avoid such traps as an infinite loop execution or a stalled sequence.



Trip computer (600 MW design)

TCG

Figure #3 – Programmable Digital Comparator (PDC) Process Digital Shutdown System

Programmable Digital Comparators (PDC's) .....continued

- If the conditions for the ***watchdog timer are not satisfied***, that trip channel is ***de-energized*** independent of the trip parameter conditions (i.e the PDC has failed-safe)

- The logic in the PDC's could now be programmed to implement ***conditioning logic***, ***signal spread checks***, ***rationality checks*** and ***calculate power dependent trip setpoints***.

- In addition to outputting the trip channel signals, the PDC drives analog and digital outputs which ***drive conventional indicating devices*** on the main control room panels.

- Correct operation of the PDC analog and digital outputs can be ***dynamically verified*** by wiring the ***outputs*** (analog & digital) back to ***special inputs*** (analog & digital).

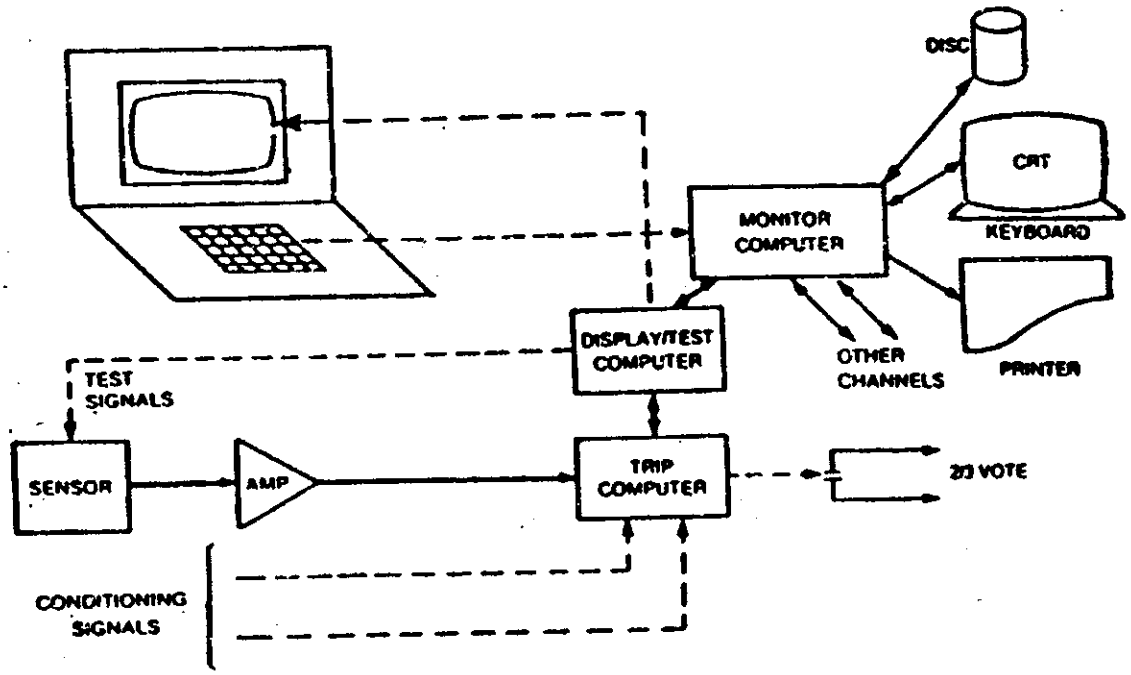
- Periodic programs can then be executed to ***test drive the outputs*** and ***read back*** the corresponding field value developed by the output system. If significant discrepancies are recognized on the read-back, then an appropriate alarm can be annunciated to prompt operator or maintainer intervention.

Fully Computerized Shutdown System - third evolution

- The fully computerized shutdown system is a combination and extension of the PDC trip computers and the Monitoring computers strategies. The four special safety system functions (i.e. ***trip logic***, ***testing***, ***monitoring*** & ***display***) are implemented in a fully computerized design.

- The shutdown system parameter sensing instrumentation still consists of the analog process and neutronic sensors, but ***all*** of the ***comparison*** and ***trip logic***, ***testing*** and ***monitoring*** functions along with the ***man-machine interfacing*** is now ***computer based.***

- The two shutdown systems (SDS1 and SDS2) have a ***similar computer configuration*** but each system is designed by a ***separate team of designers*** as one measure to ensure functional independence and each design team ***specifies equipment from a different manufacturer***.



Fully computerized shutdown system

Figure #4 – Fully Computerized Shutdown System for Process and Neutronic Trip Parameters

Fully Computerized Shutdown System....continued

- Fifteen computers (15) , organized into a ***three level hierarchy***, are used in the total computerized shutdown system design for each reactor. The three hierarchy level functions are ***trip***, ***display/test*** and ***monitoring***

- There are channelized ***trip*** and ***display/test computers*** for each safety system channel.

- There are ***seven*** (7) SDS1 related computers.There are ***three SDS1 trip*** computers (i.e. Channels D,E & F) ***and three SDS1 Display/Test*** (i.e. D/T) computers. A ***SDS1 monitoring*** computer is also provided to track and assess the trip parameters for this system by interfacing with the D/T computers so that seven computers are dedicated for SDS1.

- Similarly, there are ***seven*** (7) SDS2 related computers.There are ***three SDS2 trip*** computers (i.e. Channels G,H & J) and ***three SDS2 Display/Test*** (i.e. D/T) computers. A ***SDS2 monitoring*** computer is also provided to track and assess the trip parameters for this system by interfacing with the D/T computers so that seven computers are also dedicated for SDS2.

- Finally, a unit ***monitoring*** computer (common to SDS1 & SDS2) is provided to coordinate the system performance and testing data as well as administrative information from both the SDS1 and SDS2 monitoring computers.

- The data links to the unit monitoring computer are ***uni-directional*** from the individual safety system monitoring computer and are interlocked to allow data transmission from ***only one safety system at a time***.

- This results in 7 SDS1, 7 SDS2 and 1 unit computer for a total of 15 safety system computers.

- This configuration provides a central interface between the operator and the special safety systems while preserving the ***required separation*** between different safety systems and among different channels of the same system by using uni-directional fibre-optic links and hardware interlocks. External hardware interlocks on both inputs and outputs ensures that ***only one channel can be tested*** or calibrated at a time.

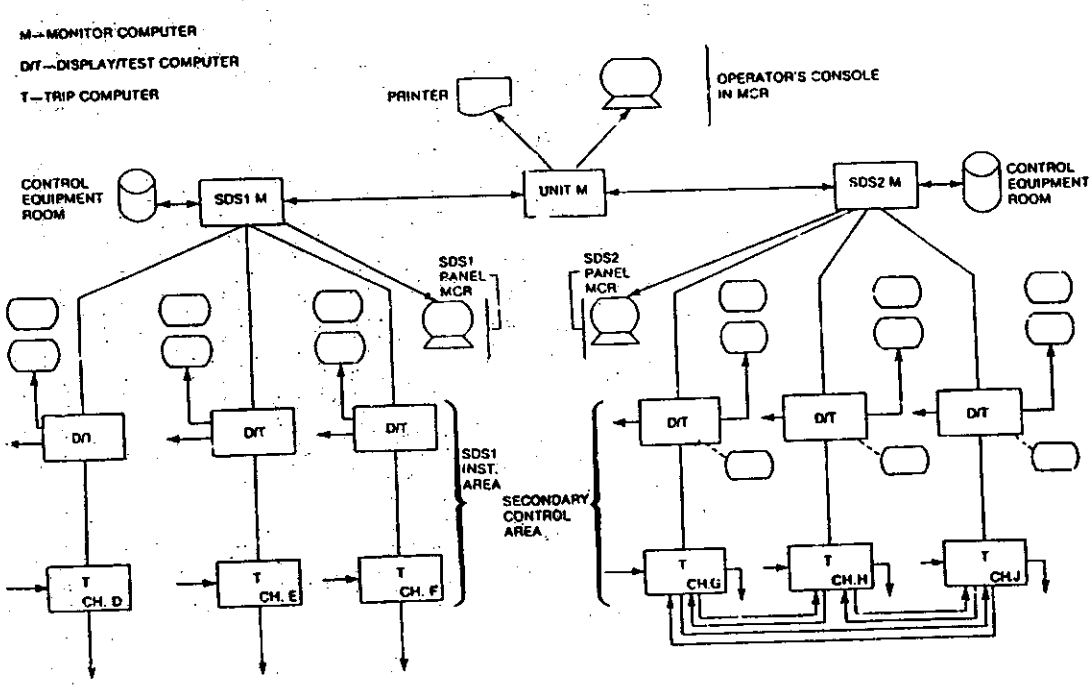


Figure #5 – Configuration of Trip, Display/Test and Monitoring Computers for SDS1 & SDS2