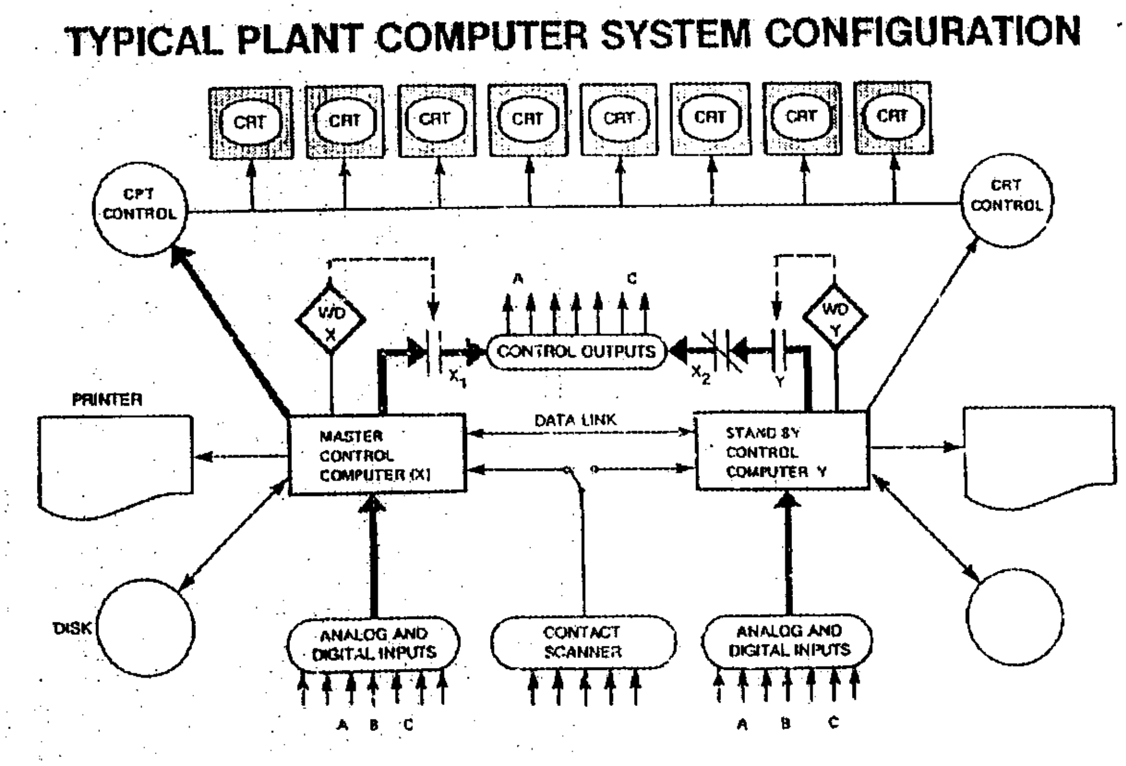
TYPICAL PLANT COMPUTER SYSTEM CONFIGURATION
CRT
CRT
CRT
CRT
CRT
CRT
CRT
CRT
CPT CONTROL
CRT CONTROL
W/D X
WD Y
A
C
CONTROL OUTPUTS
$X_1$
$X_2$
Y
PRINTER
DATA LINK
MASTER CONTROL COMPUTER (X)
STAND BY CONTROL COMPUTER Y
DISK
ANALOG AND DIGITAL INPUTS
CONTACT SCANNER
ANALOG AND DIGITAL INPUTS
A B C
A B C

**Figure #1 - A Dual Redundant Control Computer Configuration**

## Wiring the Controlling Computer to the Field Device

- By wiring the ***'Master in-control'*** logic via normally-open (N.O.) contacts in series with the ***'not in control'*** normally-closed (N.C.) contacts allows only the designated Master Computer to access the field.

- For example allow that DCC-X signal outputs are routed through a ***N.O.*** DCC-X controlled relay (say contact xc1 of relay #1) contact and then through a ***N.C***. DCC-Y controlled relay (say yc1 of relay #2) contact before being wired ***to the field device***.

- In this way, with DCC-X in-control, relay #1 will be energized causing contact xc1to ***close*** and relay #2 will be de-energized causing contact yc1 to also be ***closed*** so that both contacts in the circuit to ***connect DCC-X to the field*** are closed.

- Similarly, allow that DCC-Y outputs are routed through a ***N.O.*** DCC-Y controlled relay (say contact yc2 of relay #3) contact and then through a ***N.C.*** DCC-X controlled relay (say contact xc2 of relay #4) contact before being wired ***to the field device***.

- In this way, with ***DCC-X in-control***, relay #4 will be energized causing contact xc2 to ***open*** and relay #3 will be de-energized causing contact yc2 to also be ***open*** so that both contacts in the circuit to connect DCC-Y to the field are opened . ***DCC-Y is not connected*** to the field since DCC-X is in-control.

- On detection of a ***disabling*** program or computer ***fault***, that computer is no longer able to satisfy the logic conditions for being ***'in-control'*** and so is unable to energize its output signal selection control relays.

## Determination of the Controlling Computer

- At the same time, the *former standby* computer is able to now fulfill the *'in-control'* logic requirements and so is able to *energize* its output control relays.

- The change in state of these output control relays then *switches* the control of the field devices from the former master computer to the previous standby machine completing the automatic transfer from say DCC-X to DCC-Y.

- Each computer is fully capable of *individually* running the plant independently and the operator can select the desired 'master' computer by handswitch control.

- The two machines are connected by a *data-link* which can transmit non-essential information for annunciation and display purposes.

- Both computers provide CRT based *operating displays* and log sequential operational information resulting from normal operations or an event.

- Computerized *alarm information* is displayed on the central annunciation CRT's.

- Stylized *system displays* and *graphical updates* (analog trends, bar charts, point data, etc) are provided on the system panel and the console CRT's.

## Computer Program Checks

- Either computer can drive any of the CRT displays and the two annunciation CRT's - usually the 'Master' computer is selected to drive these CRT's but the standby computer can be selected to ***cross-check*** indications that are being obtained.

- It is important to indicate (at all times) ***which Computer*** information is being displayed as well as showing which computer is in control.

- The computer system checks for faults at the ***program level*** (i.e. are the conditions satisfied necessary to allow this program to run automatically?) and at the computer ***system level*** (i.e. are the correct power supplies available for the computer, are expected operations being performed, necessary interfaces available and are operations being performed within the expected time slice, etc).

- External countdown registers are used to schedule programs and to time their execution.

- A program will ***fail*** (i.e. not satisfy the requirements for continued operation) if it does not ***execute within a specified time interval*** or if a specified number or combination of its inputs are not deemed to be ***rational***.

- At the system level, a machine fails if it does not update a ***watch-dog timer*** within a specified time interval, if a fault is detected in the ***input/output subsystem*** or if a ***memory parity fault*** is detected.

- On a system fault, all ***digital outputs*** for that computer are ***opened***, the ***analog outputs*** are set to the ***fail-safe*** condition (usually zero signal), and control is automatically ***transferred*** to the standby machine.

**Control Computer Availability**

- Each computer continuously performs extensive ***self-check*** tests on its peripheral hardware (i.e. analog inputs or outputs, etc) and on its internal computer components (i.e. CPU, ALU, memory, etc).

- Minor faults are annunciated to the operator or maintenance staff (as appropriate) for repair purposes while major faults will initiate the ***transfer of control*** logic so that the ***'in-control'*** status is relinquished to the standby computer.

- The design approach is to avoid the loss of ***monitoring***, ***control*** or ***annunciation*** due to the occurrence of one ***single failure***.

- In keeping with this philosophy, most sensors are ***duplicated*** or ***triplicated*** as is appropriate for the application.

- For ***duplicated*** measurements, the average value is used if the two signals are in good agreement, otherwise the most conservative value to ensure the safest decision (i.e. say the highest pressure) is selected for control sensing.

- Where ***triplicated*** signals are provided and they are all rational, then the ***median*** signal is selected for control sensing. Otherwise, the unacceptable parameter is ***rejected*** and annunciated as being irrational and the signal selection reverts to that of a duplicated system.

- ***Redundancy*** is also provided for the ***final devices*** so that control valves can be driven in parallel or configured in a master/standby manner.

- In addition, ***interchannel*** and ***computer to computer*** comparisons will check for differences in signals, thus facilitating early recognition and maintenance of signal degradations.

- This information ***monitoring*** and the ability to perform ***on-line maintenance*** contributes significantly to the high capacity factors achieved by CANDU plants.

## ANNUNCIATION and DISPLAY FUNCTIONS

- A wide variety of display functions are available to the operator. These include:
    - annunciation
    - graphical trends
    - bar charts
    - status displays
    - schematic displays
    - point data displays
    - summary data displays

- A standard ***keyboard interface*** to the computer driven CRT system has been developed for all of the operator information functions. This keyboard is the operator's prime means of communicating with the computer system.

- The CANDU main control room operations keyboard is divided into three groups:
    - numeric keys for data entry
    - function keys to initiate displays
    - keys for operator functions

- The labeled, special function select keys provide very rapid access to the various system data formats associated with each CRT.

- Typically the computer display ***response time*** to an operator request for a new data format is less than one second.

- Changes to data (that are allowed for the operator) stored in the computer such as control ***setpoints*** or ***alarm limits*** and changes for parameters appearing on a trend or bar chart; are done by the numeric key pad and control keys.

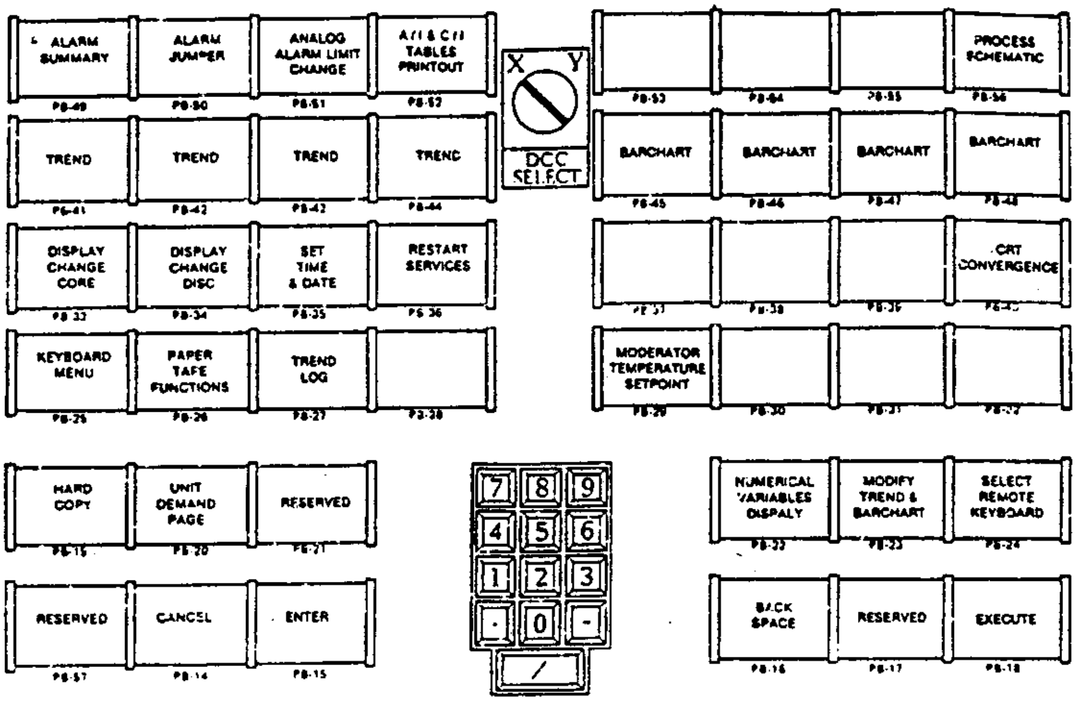

Figure 2. Typical Computer Control Keyboard Layout

## ANNUNCIATION CRT DISPLAYS

- Early traditional designs used ***hardwired alarm windows*** located above the control panels to annunciate faults.

- These alarm windows, although effective at attracting the operator's attention, provide limited information and are impractical when a lot of alarms are needed.

- In current designs, the hardwired windows alert the operator of the ***general occurrence*** of an important fault while further details are provided by the ***annunciation CRTs***.

- The annunciation data can now be manipulated as any batch data system to ***prioritize*** the display of alarms as well as to ***logically group*** the alarm messages, allow ***unique*** summaries to be prepared and to link the alarms to necessary follow-up operating or maintenance actions.

- During a plant upset (such as a reactor trip or stepback) minor alarms (i.e. low priority) are ***inhibited*** from being displayed on the CRT - only ***major*** (i.e. high priority) alarms are presented until the upset has cleared.

- This prevents the CRT from being '***flooded***' with messages during ***critical recovery periods*** while allowing the operator to respond to those alarms which are ***more important*** for station operations.

- However, all alarms with their ***time of occurrence*** and the ***unique alarm reference number*** are all saved to disc. At the operator's request, a ***summary*** of all existing alarms on a system or total plant basis can be displayed and this summary can be reviewed on the CRT or printed out for further review or documentation purposes.

## GRAPHICAL TREND DISPLAYS

- Graphical trends display the status and change of a parameter in a continuous analog manner with respect to a selected ***time frame*** and ***magnitude scaling***.

- ***Historic data*** may also be retrieved from disc storage to review a previous operating event. The operator specifies the ***time period*** of interest and the ***scale range*** for the display and a static display of the request is prepared.

- Different variables in the graphical trends are identified by ***colour*** to assist the operator's ***discrimination***.

- Parameters can be set up by default to have ***pre-selected*** ranges and time servicing or those attributes can be uniquely set.

- Similarly, the option of ***dummy variables*** is provided so that the operator can link any parameter to that dummy trend.

- Parameters can also be specified as part of the automatic ***historical logging*** process (so that previous performance can be assessed) or as a ***temporary parameter*** (i.e. not historical) so that viewing the trend is only possible if that parameter has been selected for display.

## BAR CHARTS

- Up to sixteen signals can be displayed on a ***bar chart***, each having an ***identification code***, ***scale values***, ***alarm limits***, ***current value*** and ***units***.

- This approach allows ***high density displays*** of multiple similar parameters from which any variance can very easily be seen.

## OTHER DISPLAYS

- A variety of special purpose displays are ***unique*** to particular systems and operating conditions. For some displays, the data processing capabilities of the computer system provide ***information not normally available*** with conventional instrumentation.

- For instance, a dynamic plot of the reactivity control system operating point relates the ***reactor power control error*** to the ***average liquid zone level*** on an X-Y display to show the ***action points*** for initiating the various control mechanism operations - this provides an easy to understand ***overall reactivity*** control mechanism ***coordination***.

- Similarly, a ***plant block*** schematic diagram with superimposed operating data provides an overall plant condition status indication with navigation icons to allow direct access to the associated subsystem displays.

- CRT plant displays can be assessed by operators in an ***on-going*** manner so that operational feedback can be used to modify existing displays or to create new ones to achieve an enhanced operations performance.

- Such a plant-wide summary display also provides an ***understandable navigation approach*** to allow the operator to quickly and conveniently select major system displays from one central coordinating display so as to maintain unit status continuity knowledge.

## CANDU DCC Assignment

1. Explain the term dual-redundant by referencing the Master/Standby DCC configuration as a practical example.

2. Make a simple sketch to show how interfacing relays can be used to ensure that only one computer (the one identified as the present Master computer) can be connected to the field output device while the standby computer is disconnected by this same logic.

3. Explain briefly how the provision of a data cross-check feature between two computers can help the operator to very quickly recognize a potential problem condition.

4. What is the function of a 'watch-dog' timer in a digital control application?

5. Why can the variation of a parameter in a triplicated measurement system be recognized and identified as a problem much more easily than is the case in a duplicated measurement system?

6. Why is it important to display the computer-in-control identification at all times for a redundant computer system?

7. What purpose would a two key sequence (i.e. enter key and execute key) serve when made as a requirement to complete a control data entry action? If this is a good idea for control data entries. why not make it a requirement for all operator data entires?

8. Provide an illustrative list of five (5) CRT display types that can be provided for operators and briefly describe their main features.

9. What information do you think is essential to be included in a CRT alarm message? Explain the four or five key information features that you would recommend as being essential to efficiently advise an operator of a potential problem situation. How should this information be presented to best help the operator understand the new situation?