AECL--10510

CA9200430

ATOMIC ENERGY
OF CANADA LIMITED

ÉNERGIE ATOMIQUE
DU CANADA LIMITÉE

MAPLE-X10 REACTOR DIGITAL CONTROL SYSTEM

SYSTÈME DE COMMANDE NUMÉRIQUE DU RÉACTEUR MAPLE-X10

M.T. DeVERNO and H.W. HINDS

Chalk River Laboratories

Laboratoires de Chalk River

Chalk River, Ontario K0J 1J0

October 1991 octobre

AECL Research

MAPLE-X10 REACTOR
DIGITAL CONTROL SYSTEM

by

M.T. DeVerno and H.V. Hinds*

Civil & Electrical Design Branch
*Instrumentation & Control Branch
Chalk River Laboratories
Chalk River, Ontario, Canada K0J 1J0
1991 October

AECL-10510

EACL Recherche

SYSTÈME DE COMMANDE NUMÉRIQUE DU RÉACTEUR MAPLE-X10

par

M.T. DeVerno et H.W. Hinds*

RÉSUMÉ

Le réacteur MAPLE-X10, en cours de construction aux Laboratoires de Chalk River d'Énergie atomique du Canada limitée, est un réacteur à eau ordinaire de type piscine, de 10 MW(t). Il servira à la production de radio-isotopes et au dopage du silicium par transmutation de neutrons. Le réacteur est commandé par un système de commande numérique (SCN) et protégé par deux systèmes de sûreté autonomes contre tout événement résultant d'un fonctionnement anormal. Le SCN est un système de commande intégré servant à régler la puissance du réacteur et à commander le fonctionnement des systèmes. L'objet premier du système de contrôle-commande est la sûreté; sa fonction est de réduire le nombre d'événements contraires à la sûreté résultant de défaillances du système et d'erreurs d'exploitation. La sûreté est assurée grâce aux moyens suivants: redondance, conception à sécurité intégrée, détection automatique des erreurs et utilisation de composants de grande fiabilité. Le SCN permet d'assurer le pilotage automatique du réacteur, depuis l'arrêt jusqu'à la pleine puissance, et l'arrêt automatique du réacteur si les limites de sûreté sont dépassées ou dans le cas d'une défaillance des capteurs critiques. L'utilisation de matériel couramment utilisé dans l'industrie et un contrôle d'assurance qualité rigoureux de ces derniers contribuent à maintenir l'équilibre coûts-avantages tout en garantissant une fiabilité supérieure.

Service d'études de génie civil et électrique
*Direction Instrumentation et Contrôle
Laboratoires de Chalk River
Chalk River (Ontario) Canada K0J 1J0
Octobre 1991

AECL-10510

AECL Research

MAPLE-X10 REACTOR
DIGITAL CONTROL SYSTEM

by

M.T. DeVerno and H.V. Hinds*

ABSTRACT

The MAPLE-X10 reactor, currently under construction at the Chalk River Laboratories of Atomic Energy of Canada Limited, is a 10 MW_t, pool-type, light-water reactor. It will be used for radioisotope production and silicon neutron transmutation doping. The reactor is controlled by a Digital Control System (DCS) and protected against abnormal process events by two independent safety systems. The DCS is an integrated control system used to regulate the reactor power and process systems. The safety philosophy for the control system is to minimize unsafe events arising from system failures and operational errors. This is achieved through redundancy, fail-safe design, automatic fault detection, and the selection of highly reliable components. The DCS provides both computer-controlled reactor regulation from the shutdown state to full power and automated reactor shutdown if safe limits are exceeded or critical sensors malfunction. The use of commercially available hardware with enhanced quality assurance makes the system cost effective while providing a high degree of reliability.

Civil & Electrical Design Branch
*Instrumentation & Control Branch
Chalk River Laboratories
Chalk River, Ontario, Canada KOJ 1JO
1991 October

AECL-10510

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1.0 INTRODUCTION

The MAPLE-X10 reactor, currently under construction at the Chalk River Laboratories (CRL) of Atomic Energy of Canada Limited (AECL), is a dedicated isotope production facility based on the MAPLE (Multipurpose Applied Physics Lattice Experimental) research reactor concept [1,2]. The MAPLE series of research reactors is being developed by AECL for the world market and the MAPLE-X10 reactor will serve as a demonstration of the generic MAPLE concept. This reactor will be used exclusively for the commercial production of radioisotopes and silicon neutron transmutation doping [3].

The reactor is controlled by a Digital Control System (DCS) and protected against abnormal process events by two independent safety systems. The DCS provides an integrated environment for reactor regulation, process control, and balance-of-plant control and monitoring. Automated computer-controlled regulation of reactor power from the shutdown state to full power is a key component of the DCS. The use of commercially available, dual, redundant computer hardware makes the system cost effective while providing a high degree of safety and reliability.

This report provides an overview of the MAPLE-X10 reactor and describes the DCS. The description of the DCS focuses not only on its technical attributes but also on the design principles and philosophy, design methodology, and quality assurance programs applied throughout its development life cycle.

2.0 BACKGROUND

The MAPLE-X10 reactor is a 10 MW_t, pool-type, light-water reactor. A graphic representation of the reactor structure is shown in Figure 1.

The reactor core is located above a grid plate and inlet plenum structure at the base of the pool. The core (approximately 0.4 m in diameter by 0.6 m in height) consists of driver-fuel assemblies and isotope production target assemblies arranged in a close-packed hexagonal array. Each fuel and target assembly is located within a vertical coolant flow tube, which is open at the top of the core and connected to the grid plate at the base of the core. The core is surrounded by an annular D_2O-filled reflector tank containing a number of vertical flow channels for isotope irradiation. A large diameter, upright hollow cylinder (chimney) is attached to the reflector tank at the top of the core and is open at the top to the pool. The chimney acts as an outlet coolant plenum.

The core is cooled by low-temperature and low pressure light-water. Water circulated by one of two full-capacity pumps enters the inlet plenum and flows upward through the grid plate and into the fuel channels. It exits from the fuel channels into the chimney and flows vertically towards two discharge nozzles located on opposite sides of the chimney. The primary coolant flow mixes with a downward flow of pool water in the chimney and the mixture is drawn through the discharge nozzles to the pump inlet. The discharge of the pump leads to the primary heat exchanger, where heat is transferred to process water. The discharge of the PCS pump directs most of the coolant to the inlet plenum with approximately 10% of the flow diverted to the bottom of the pool, bypassing the core. This bypass flow cools the bottom of the pool, rises around the outside of the reactor, and is then drawn into the top of the chimney. The downward flow of pool water suppresses the upward flow of the primary coolant and channels the coolant into the PCS outlet nozzles. This suppression of upward flow prevents activation products collected by the primary coolant as it flows through the core from rising towards the top of the pool, where it can present a radiation hazard. When the reactor is shut down, decay heat is removed by thermosyphoning through the primary coolant system or the pool.

Reactor regulation is provided through the control of three annular hafnium control absorber rods (CARs) located in the outer area of the core. These hafnium absorbers slide over three circular flow tubes and are connected by rigid rods to stepper motor drive assemblies positioned above the pool. The stepper motor drive assemblies are controlled by the DCS through stepper motor interfaces.

Reactor protection against abnormal operation and design basis events is provided by two independent safety systems. Safety System #1 (SS1) utilizes three annular shut-off rod (SOR) absorbers, similar in design to the CARs, to maintain a safe sub-critical state by dropping into the core under gravity upon detection of neutronic and process excursions outside of the normal operating envelope. Safety System #2 (SS2) independently monitors both neutronic and process parameters and shuts down the reactor when operation outside of the normal control envelope is detected. SS2 employs electromagnet disconnects on the CAR drives and a power disconnect to the CAR drive motors to ensure that any possibility of continued updrive of the CARs is prevented, and that the reactor remains in a sub-critical state.

2.1 Research and Development Program

The design of the DCS has been supported by two key research and development projects:

a. MXSIM dynamic simulation of the reactor and control systems, and

b. the development of the MAPLE-X10 Dynamic Test Bed (DTB).

The MXSIM computer code is a dynamic simulation of the MAPLE-X10 reactor core, reactivity mechanisms, process systems, and Instrumentation and Control (I&C) components. The I&C modelling includes both instrument dynamics and a model of the digital controller (i.e., timing and quantization effects). Although limited in its modelling of two-phase thermalhydraulic flow, the MXSIM code is applicable over the full range of normal operating to trip conditions, and has been used to test the reactor control system design, with emphasis on reactor regulation.

The DTB is a reactor simulation platform developed for dynamic testing of the DCS, and was designed with a simplified set of reactor dynamic models to achieve real-time operation. The DTB models the response of CAR hardware, reactor kinetics, and process systems to the DCS control outputs. The DTB includes hardware inputs and outputs corresponding one for one with the outputs and inputs of the DCS. A specialized DTB operator interface enables operator control over the DTB/DCS interface to simulate failures of equipment and process systems. Thus when the DCS and DTB are coupled together, the system provides full-scope dynamic testing of the control algorithms, verification of operational task analysis and procedures, evaluation of the man-machine interface, and operator training.

3.0 CONTROL CENTRE OVERVIEW

The layout of the ground floor of the MAPLE-X10 facility and a general layout of the control room are shown in Figures 2 and 3. The control centre includes the following system components and panels:

a. Digital Control System,
b. Safety System #1 Panels,
c. Safety System #2 Panels,
d. Main Operator Console,
e. Exhaust Air Filtration System (EAFS) Control Panel,
f. Heating, Ventilating, and Air Conditioning System (HVAC) Control Panel,
g. Closed Circuit Television (CCTV),
h. Radiation Monitoring System Panels,
i. Fire Protection System,
j. Security System,
k. Telephone, Public Address, and Intercom Systems, and the
l. Maintenance Panel.

The DCS and safety systems occupy prominent positions within the control room. The operator console contains: the control system CRT station and the operator panel, PL-02. This operator panel contains: the controls and indicator panels for resetting, poising, and monitoring the condition of the safety systems; mushroom buttons for initiating a manual reactor trip; and, a keyswitch to enable reactor regulation using the DCS. From the operator console, there is a clear field of view to all of the primary subsystem panels. The distances and viewing angles from the operator console permit monitoring of the panel instruments associated with both safety systems, the reactor regulating system, radiation monitoring, HVAC, and EAFS.

The maintenance panel contains handswitches that can be used to select the main PCS isolation valve positions and to override the DCS control of the PCS isolation valves and pumps for maintenance purposes while the reactor is shut down. Access to the maintenance panel is controlled through a keyed interlock with the DCS keyswitch on the operator panel. The keyswitch must be in the 'Lockout' position, ensuring the reactor is shut down, to allow the key to be removed to access the maintenance panel.

3.1 DCS Hardware & Software Overview

The DCS is a Moore Products Limited dual, redundant control computer and operator interface system with enhanced reliability and quality assurance [4,5,6]. The proven track record afforded by this industrial unit played a key role in its selection. The system architecture used within the DCS is presented in Figure 4 and consists of the following components:

a. two fault-tolerant Multi-Loop Controllers (MLCs),
b. a single non-redundant calculation module,
c. redundant watchdog timer modules,
d. redundant input/output (I/O) hardware,
e. a single Basic CRT Station (BCS), and
f. a Mycroterm maintenance terminal.

Each MLC is a fault-tolerant computer system with redundant memory systems and on-line self-diagnostic software [7,8]. The MLCs interface with the field devices through redundant input/output (I/O) hardware modules. Overall, the DCS includes approximately 200 computer I/O points, including relay contact, 4-20 mA, TTL level, and signal conditioned interfaces. The MLCs and I/O modules are monitored by hardware watchdog timer modules that control the switchover from operating MLC and I/O modules to the standby units upon detection of system failures [9]. A non-redundant calculation module is included in the DCS to expand the capabilities of the MLCs. The calculation module, equivalent to a MLC with no I/O connections, is used exclusively for the handling of non-critical functions where a single system failure will not impair the safe operation of the reactor.

The BCS is the man-machine interface [10]. It presents an extensive set of display screens and allows the operator to change setpoints and select control functions. The BCS also provides alarm annunciation, data recording, and historical data retrieval. The MLC, calculation module, and BCS are interconnected via a redundant data highway referred to as the high level link (HLL).

The Mycroterm is a rack-mounted maintenance terminal that is directly connected to the MLCs. It is used to investigate the MLC database and permits access to MLC programming constants not accessible through the BCS.

The software for the MLC and BCS is to a large extent pre-programmed and built into the firmware of the computers. The MLC has 30 basic programming functions, called algorithm blocks, which are 'configured' into a user program. This configuration can be accomplished through a menu selection process or through the use of a CADD-assisted configuration package. The use of a fixed set of algorithms restricts the functions that might be more easily accomplished by programming in a general-purpose language, but ensures that the system is robust and eliminates numerous potential errors. The BCS software is comprised of a set of 16 pre-programmed display formats and is also configured through menu-driven software. A list of MLC built-in algorithms and standard BCS display formats is provided in Table 1.

Overall, the MLC and BCS software has been extensively tested and has been proven during the last 10 years in over 10 million hours of use in industrial process control applications. These applications include both pharmaceutical and food processing industries where, as in the nuclear industry, high reliability is required.

4.0 INSTRUMENTATION AND CONTROL DESIGN PRINCIPLES

The general principles governing the design of the MAPLE-X10 Instrumentation and Control systems, and in particular the DCS, include:

a. separation and isolation of control and safety,
b. simplicity of design and function,
c. limited introduction of new technology,
d. software replacement of hardware,
e. operator interface mimics of basic control panels,
f. automated shutdown,
g. limited automation of reactor start-up,
h. computer system maintains the control envelope, and
i. simplified emergency procedures.

The separation of control and safety systems is one of the central principles of the CANDU* power reactor design and provides the foundation for the design of similar systems within the MAPLE-X10 reactor. All components of the control system are physically, electrically, and logically isolated from the safety systems or other plant systems not included within the control system. (Logical isolation means that failure of another reactor system should not drive the control system beyond its safe operating limits.)

Simplicity of design and function ensures that the DCS will be easy to operate and enhances the reliability and overall safety of the facility.

The limited introduction of new technology coupled with the software replacement of hardware is aimed at enhancing reliability and availability, while providing systems familiar to CRL reactor operations personnel. Maintaining a CRT interface that mimics basic control panel instruments such as three-term analogue controllers ensures an easy transition of CRL reactor operations staff to the new MAPLE-X10 facility. As the MAPLE-X10 reactor is dedicated to isotope production, it is intended that the reactor will be frequently shut down and started up (perhaps daily) for refuelling and isotope target changes. Therefore, the CRT screens must be easy to use and the operating procedures kept simple.

Safety is the overriding concern in the design of the control system. The most fundamental objective of the DCS is to maintain a safe control envelope under all conditions and to minimize unsafe events arising from system failures and operational errors. This is achieved through redundancy, fail-safe design, automated fault detection, and selection of highly reliable components. This amounts to a design based on defensive

---

*CANDU: CANada Deuterium Uranium. Registered trademark.

engineering principles. Redundant instrumentation, programming constraints, and interlocks are used to maintain reactor control and to initiate a controlled reactor shutdown whenever a process failure occurs that could lead to excursions outside of the control envelope.

Simplified emergency procedures also have a direct effect on the design of the DCS. The simplicity of the reactor design and purpose do not lead to conflicting operational considerations, and shutting down the reactor is the primary goal whenever there is a possibility that the safety of the reactor is compromised. Therefore, an automated reactor shutdown capability has been included within the DCS.

5.0 DCS FUNCTIONAL DESCRIPTION

5.1 Operational Design Philosophy

The general philosophy of the DCS is to control the reactor during normal operation as simply as possible, with automation of operator activities where possible. However, it is also necessary to maintain a sufficient degree of freedom to perform commissioning tests, maintenance procedures, and other special tasks. To achieve this, the DCS provides the operator with a manual control mode with limited control over the outputs of all control loops. This manual mode is controlled by the MLC, which ensures that all actions (automatic or manual) maintain a safe reactor state through the use of software constraints and interlocks. This MLC manual mode should not be confused with the maintenance panel functions, which bypass the computer and are intended for process system pump/valve maintenance operations in the absence of the MLC.

The control philosophy adopted is that the control system must prevent the reactor from being driven into a reactor trip (i.e., challenge the safety systems) or even into one of the alarm or interlock states described below. This imposes limits on acceptable operator commands even in manual mode within the MLC.

Alarms are configured within the MLC to inform the operator that a device has malfunctioned or that the process has entered an undesirable state. Alarms are not generated if the condition can be considered a normal operating state. Alarms can be enabled or disabled by process events and alarms may also be used to interlock with other parts of the control system, to initiate remedial actions to ensure safety or prevent damage to equipment. These alarms and interlocks provide safety features within the control system and are designed to reduce the number of reactor trips that might otherwise occur by causing remedial control system action, to ensure that the control envelope is not violated.

All analogue signals are checked for rationality to determine if the instrument loop is functional. Irrational signals are generally alarmed and may also initiate additional interlocks. Redundant sensors are used whenever sensor failure could compromise safety. In general, the most conservative of the redundant sensor readings is used in subsequent calculations and significant deviations between redundant signals generate alarms and may initiate interlocks.

5.2 Control Systems

The DCS is used for reactor regulation and control of all of the main process systems, including:

a. primary coolant system (PCS) pump/valve operations,
b. PCS coolant temperature control,
c. reflector cooling (RC) system operation and temperature control,
d. process water (PW) system total flow control,
e. purification systems for primary coolant, reactor and service pools, and
f. pool water make-up control.

The DCS also provides balance-of-plant monitoring, which extends to the electrical sub-systems, active/process sumps, transfer trench gate, flood detection, and monitoring of the state of the safety systems.

5.2.1 Reactor Regulation

The reactor regulating system (RRS) control loops are the most complicated within the DCS. These loops are enabled by the Lockout/Enabled keyswitch. The keyswitch must be in the 'Enabled' position to start up the reactor. If the keyswitch is in the 'Lockout' position, the RRS control immediately enters its controlled shutdown mode irrespective of what commands have been entered through the console. In addition to the keyswitch, which is a contact input to the MLC, there is an Operate/Shutdown softswitch on the BCS. If 'Enabled' via the keyswitch and the softswitch is in the 'Operate' position, then the operator can select a maximum power limit, enter a power setpoint, and the DCS will automatically control to the selected power, assuming that all internal checks confirm it is safe to increase power. If the softswitch is set to the 'Shutdown' position, then the flux control algorithm automatically enters the shutdown mode of operation and ensures a controlled shutdown to a safe reactor state.

Four limiting power levels ranging from 100 W to 10 MW are selectable through the BCS. This allows the operator to enter power setpoints as a percentage of full power. This method achieves a large dynamic power range and also integrates well with the proposed nuclear commissioning. Under normal operating conditions the 10 MW power limit is used.

Flux control is based on neutron flux sensors and a calculated thermal power derived from flow and temperature sensors. Redundant sensors and instruments are used for flux and thermal power measurement, including RRS fission counters, and PCS flows and temperatures. The RRS flux control loop can be operated in either automatic or manual control modes. Two submodes, thermal power mode and neutron power mode, are also available. These submodes allow the operator to select how the reactor power measurements are calibrated. In thermal power mode, a calibration coefficient is continuously updated based on a calculated thermal power. This calibration coefficient is used to adjust the neutron power measured by the flux instruments and control is based on this calibrated neutron power. In neutron power mode, the calibration coefficient is fixed.

Neutron flux is the primary means of sensing reactor power. The neutron flux signal is processed by the fission counter signal processing units to generate linear, logarithmic (log), and log rate (inverse period) signals, which are read as analogue inputs by the DCS. The linear flux and log flux signals are automatically calibrated as determined by the sub-mode selection (thermal power or neutron power modes). The calibrated linear and log flux signals are combined to provide a continuous representation of reactor power with a satisfactory accuracy through the full dynamic range of the neutron power instruments. To slow down the rate signal at high powers, the calibrated linear flux is modified by the log rate to generate a linear rate. The accurate log flux, log rate, and linear rate signals are blended by the flux control algorithm, with the resultant signal used for proportional-derivative (PD) control of the CAR velocities.

When the automatic flux control mode is selected, the operator enters a setpoint as a percentage of the maximum power limit and the DCS automatically manoeuvres to the desired power. The controllable range is from 10^{-8} of full power (FP) up to Full Power. When the manual mode is selected, power is controlled through automatic position control of each CAR. In manual mode, the operator enters a CAR position setpoint and the DCS automatically controls to the setpoint, thereby setting the reactor power level. However, the operation of this manual control scheme is bounded automatically to the maximum selected power limit. When in manual CAR control mode, the automatic flux control algorithm is given a 100% setpoint and the output of the automatic flux control algorithm will override the manual CAR control if necessary, to ensure that the control envelope is not violated.

Reactor shutdown can be initiated by the operator using the keyswitch (Lockout/Enabled) or the BCS (Operate/Shutdown softswitch). Shutdown can also be initiated automatically by the DCS when an abnormal process event is detected. These events range from failure of critical instruments to the detection of abnormal events. Once the reactor shutdown mode is initiated, it is 'locked in' until shutdown is verified and all abnormal initiating events have cleared. Shutdown causes all CARs to drive in until they reach the bottom, and combines a controlled shutdown to 0% FP with a minimum insertion speed of 40% of the maximum CAR drive speed.

5.2.2 Primary Coolant System

The DCS is used to operate the PCS pumps and valves and to control the PCS coolant temperature. Automatic and manual control modes are available for both pump/valve selection and temperature control. These modes are selected via the BCS.

When the pump/valve automatic mode is selected, the operator is only required to select PCS pump 1 or 2. Once the pump is selected, the DCS automatically configures the PCS valves and controls pump operation. In automatic mode the DCS turns on the selected pump when the 'Operate' softswitch is selected. When in shutdown mode, the DCS automatically turns off the pump two minutes after all CARs are fully inserted. This delay ensures that the ^{16}N has decayed sufficiently to present no hazard to the operator during refuelling and isotope target changes.

When the pump/valve manual mode is selected, the operator has direct control of the selection and operation of the pumps and valves under a number of programmed constraints. The operator can open or close the PCS pump isolation valves, but only if the pump is not running. The operator can also control the pump, but the pump cannot be turned on unless the isolation valves are correctly configured for the selected pump. Although reactor operation can be initiated without the PCS pump on, the reactor power level is constrained to be less than 1% FP if there is no forced cooling. Similarly, the pump cannot be turned off by the operator unless the power level is less than 1% FP.

The PCS core inlet temperature is controlled to a setpoint by a proportional-integral-derivative (PID) controller with auto/manual modes and bumpless transfer. The core inlet temperature is measured using redundant sensors and the maximum rational signal is used by the controller to position a valve on the process water side of the PCS heat exchanger. If both signals are irrational, then the controller uses the maximum scaled value. The controller includes non-linear compensation to provide better temperature control at low powers and to effectively linearize the system gain. A reverse-acting valve has been utilized as a fail-safe feature to ensure adequate cooling on loss of power to the control valve. In manual mode, the operator can directly control the valve through the BCS under MLC programming constraints.

5.2.3 Reflector Cooling System

The reflector cooling pump is controlled either Off or On using a softswitch on the BCS. Both the heat exchanger outlet temperature and reflector tank outlet temperature are monitored. The heat exchanger outlet temperature is controlled to a setpoint using a standard PID controller with auto/manual modes and bumpless transfer. This loop controls a reverse-acting valve on the process water side of the heat exchanger. The temperature controller is overridden and the process water valve is shut when the reflector flow is low to protect against freezing of the heavy water (process water temperature can fall below 4°C during winter). Under manual control, operators have direct control over the valve and the override is not effective.

5.2.4 Process Water System

The total process water flow through MAPLE-X10 is monitored and controlled using a standard PID loop to maintain a constant flow through the system. This control loop is necessary due to the design of the existing process water system at CRL. The PID controller has both automatic and manual control modes.

5.2.5 Purification Systems

Two systems are provided to maintain the water purity of the reactor pool and service pool. The purification system uses ion exchange and filtration to remove ionic and particulate contaminates, and the skimming system removes debris and films via filtration.

The purification system consists of two separate circuits: one for the reactor pool and the second for the service pool. The circuits are normally operated independently; however, interconnections have been provided so that each circuit can service the other pool if required. The reactor pool purification circuit takes flow from the primary coolant pump outlet, purifies the water, and returns it to the pump inlet. The PCS pump provides the driving force for this circuit. To provide purification while the pump is shutdown, the system also has its own pump. However, in this configuration, water is taken from the PCS pump inlet, purified, and directed to the PCS pump outlet to ensure circulation of pool water. The service pool purification circuit is a single circuit with its own pump, filters, ion exchange columns, and strainers. If either the reactor pool or service pool circuits are unavailable, the remaining circuit can be used to service the other pool. However, only one pool can be serviced at a time.

For the purification system the DCS controls the purification pumps, monitors flows, and monitors water quality via conductivity measurements. The DCS provides on/off control of the purification pumps using computer softswitches.

Similar skimming systems are provided for each pool. Water flows from weirs located on the side of the pool to a skimming system tank (partially full), through filters, and is pumped back to weirs located on the opposite side of the pool. The tank provides a reservoir to reduce fluctuations in pool level during flask operations in the service pool.

As with the purification pumps, the DCS provides on/off control of the skimming system pumps using computer softswitches. The DCS is used to monitor the level of the overflow tank and the skimming system flows. Interlocks are provided that turn off the skimming pumps if the overflow tank level is too low.

5.2.6 Pool Level and Inventory Control

When the skimming systems are operating, the pool level is held constant by the weir. Changes in inventory due to evaporation or other causes are reflected in changes to the levels in the overflow tank. The DCS is used to monitor both the overflow tank level and the reactor pool level, and provide control of the pool makeup water using an on/off controller with both auto/manual mode selection. In auto control mode, the makeup water valve is opened when the inventory is low and closed when the inventory is high. In manual mode, the operator may open and close the makeup water valve as desired.

The DCS also monitors the time that the makeup water valve is opened. The flow is on/off at a fixed flow rate and the DCS integrates the flow, to determine the total amount of makeup water used and generate an alarm if excessive makeup water is required.

5.2.7 Miscellaneous Systems

The DCS also monitors the following sub-systems:

a. electrical distribution,
b. failed-fuel detection,
c. pool trench gate,
d. operating status of other site reactors, and
e. safety system parameters.

The DCS monitoring of the electrical distribution system provides detection and alarming of major failures of important power supplies; e.g., the power supply to the PCS pumps, detection of ground faults on the Class III emergency power, and failure of the Class II power. Class II power is supplied by two uninterruptable power supplies (UPS). UPS-1 services Safety System #1 and the DCS, while UPS-2 services Safety System #2.

The DCS monitors the failed-fuel detection system and provides alarm annunciation.

The pool trench gate is used to seal the trench connecting the reactor pool and service pool. This gate ensures that the service pool will not drain in the event of a process piping failure. This gate is kept shut and sealed, except when fuel and isotope targets are transferred from one pool to the other. The DCS monitors the open/closed state of the trench gate and alarms when the gate has been open beyond a five-minute operator time period.

The MAPLE-X10 reactor shares some services with the Chalk River NRX reactor. Therefore, the DCS is also used to monitor the state (operating or shutdown) of the NRX reactor.

Safety system parameters are also monitored by the DCS in order to provide functional interlocks on start-up and shutdown, and for data archival. Electrical signal isolation is used to maintain system separation. The safety system logic does not rely on the DCS for the performance of any safety critical function.

5.3 Operator Man-Machine Interface

5.3.1 General Overview

The BCS console computer is the main vehicle for man-machine interaction with the DCS. The operator can observe and control all components of the DCS using this console. In most cases, there is no other control room display of the information on the DCS, the main exceptions being the RRS flux instruments, which have their own panel displays. In addition, both SS1 and SS2 provide independent measurement and display of all critical neutronic and process parameters.

Systems lying outside of the domain of the DCS and having their own control room panel displays include the Safety Systems, Radiation Monitoring, HVAC, Exhaust Air Filtration, Fire Detection and Control, Intercom, PA, and Security.

In the event of failure of the BCS, the operator can initiate a controlled shutdown of the reactor using the 'Lockout/Enable' key located on the control console panel, and can control the main process pumps and valves through the maintenance panel.

The MLC and BCS combination provides a standard industrial interface to all process control operations, thereby defining and resolving many of the human-factors issues related to CRT displays. The BCS internal software provides standard point display formats, which are arranged (configured) into single point displays, group displays, and overviews (see sub-section 5.3.2). The configuration of points includes linking to the MLC internal parameters via the HLL. Alarms, alarm priorities, and alarm acknowledgement are all functions of the BCS (see sub-section 5.3.3). The alarm itself can originate as part of the MLC programming or can be determined by parameters configured within the BCS points.

All measured variables and MLC outputs to the field appear on the BCS displays. Also shown are calculated values, internal logic states, and alarms. There are three minor variations to this general rule:

a. linear flux displays show the square of the unprocessed signal,

b. displays of flow show the square root of the unprocessed signal (except where flow transmitters supply a square root signal), and

c. some of the signals received from the RRS stepper motor interface are inverted prior to display.

The purpose of these modifications is to improve the human factors by providing true linear displays and maintaining the principle that discrete alarms are always associated with a low (0) state.

5.3.2 BCS Points, Groups, and Overviews

The basic building block of the BCS displays is the point display. An example of a point display representing an analogue PID controller is shown in Figure 5. The BCS is capable of 512 distinct point displays and although the current control system configuration includes only one BCS, additional units can be coupled to the HLL as required.

Each point is given both a tag number and point description. Tag numbers are a combination of the Basic Subject Index (BSI) numbering system used for MAPLE-X10 system identification and Instrument Society of America (ISA) instrument identifiers [11].

Point displays can be combined in groups of eight, which then represent a 'group' display as shown in Figure 6. The group is the most widely used display within the BCS for both control and monitoring. There is considerable flexibility in arranging groups, which have been arranged using the following criteria:

a. Reactor systems are assigned priorities in the sequence of neutronics (highest priority), primary cooling, secondary cooling, reflector system, purification and skimming systems, pool level and make-up, electrical system monitoring, and miscellaneous systems (lowest priority).

b. A cause and effect relationship is used to select the eight points in each group so that the cause of faults can be readily identified.

c. Groups are organized in a similar manner with control functions to the left-hand side of the display and information-only points to the right. Multi-discrete point displays always appear on the far right of a group. Also, the left to right sequence of points in a group is organized in the order of neutronics, flows, temperatures, pressures, levels, and miscellaneous.

d. The highest priority screens (1-2) are reserved as the main operating pages (i.e., high-power monitoring and low-power monitoring), which contain the main safety parameters associated with the immediate reactor state.

e. Common operating procedures are to be achieved with a minimum of screen changes.

Point groups can also be arranged into overviews. An overview is a condensed display of up to nine groups. No operator actions can be initiated from an overview; however, the display of process values, setpoints and alarm information make the overview a powerful tool for obtaining an general picture of the reactor state.

5.3.3 Alarm Annunciation

DCS alarms are annunciated to the operator through the BCS. All alarms cause an audible sound, which continues until the alarm is acknowledged. A printout of all changes to alarm status occurs as part of a permanent record. A priority is assigned to alarms based on the group number of the displayed point. Pressing the 'Priority' alarm button on the keyboard instantly accesses either the lowest numbered group with an unacknowledged alarm, or, if there are no unacknowledged alarms, the lowest numbered group with an acknowledged alarm.

5.3.4 CRT Display Hierarchy

The arrangement of groups and overviews for DCS is shown in Figure 7. This arrangement was derived from consultation with MAPLE-X10 reactor operations personnel and from the parallel development of preliminary task analyses (PTAs) of operator tasks with the design of the DCS. The BCS configuration takes advantage of the BCS alarm annunciation philosophy and the sequence of reactor start-up and monitoring (see sub-section 5.4).

The displays have been developed around the main reactor systems. The displays are arranged with the most important systems presented in the low-order groups, which automatically assigns them the highest alarm priority. Each system is assigned to a starting group number that is a factor of 10. The RRS is assigned a starting group number of 10, the PCS at 30, PW system at 40, and so on to the Safety System monitoring page, which is assigned the starting group number 80 (Note: the RRS takes more than 10 pages, which forces the PCS to start at group 30). The groups starting at 1 are reserved for on-power and reactor shutdown monitoring. Within each reactor system, system details are presented in descending order of operational priority through the assignment of consecutive group numbers. This assignment of groups numbers makes it easy to move to the highest priority information associated with a reactor system by the selection of the appropriate page by number (10, 20, ...), and then navigate through the system using the BCS 'next page' and 'previous page' keys. With only seven primary systems, groups are numbered 10, 30, 40, ... , 80, and operations staff can quickly become familiar with the group patterns.

5.4 Reactor Start-Up and Power Manoeuvring

The DCS provides a semi-automated reactor start-up with automated control of reactor power from 10^{-8} FP to Full Power. The following sequence represents the minimum reactor start-up procedure using the DCS:

a. Verify that both reactor safety systems are reset and poised and that there are no abnormal conditions that would maintain the DCS in a shutdown state.

b. With the shutdown/operate softswitch in the 'shutdown' position, select the maximum reactor power level.

c. Enable the control system using the lockout/enable keyswitch on panel PL-02.

d. Select the desired PCS pump and select PCS AUTO control.

e. Select the operate mode using the operate/shutdown softswitch.

f. Select the thermal compensation mode of reactor control.

g. Place the calibrated linear flux controller in AUTO.

h. Raise the calibrated linear flux setpoint to the desired value.

At this point, the DCS controls the power manoeuvre from the shutdown state to the desired power level.

The DCS performs internal checks to automatically verify step (a); however, the operator will not normally initiate a start-up sequence without verifying that no conditions exist where DCS interlocks would prevent a reactor start-up.

The steps described above represent the minimum operator actions to achieve a full-power state. The DCS monitors all critical reactor systems and will not allow start-up unless all conditions are acceptable. However, under normal circumstances the operator would perform a variety of additional functional checks prior to start-up. This 'checklist' is embedded into the BCS display hierarchy through the assignment of the display groups. This additional checklist ensures that the following systems are free of alarms and that the associated control loops are operational:

a. electrical sub-system,

b. pool inventory and make-up system,

c. purification and skimming systems, and

d. reflector cooling system.

Checking these systems is an operator task that would occur between steps (a) and (b) in the start-up sequence.

5.5 Automated Reactor Shutdown

The fundamental philosophy of the DCS is to maintain the control envelope and to shutdown the reactor under all conditions where this overriding principle may be violated. For this reason, the DCS includes a fully automated controlled shutdown from any reactor state. This controlled shutdown can be initiated manually through operator action or automatically by the DCS, based on the monitoring of key process parameters.

The DCS shutdown mode can be initiated manually by setting the Operate/Shutdown softswitch to 'Shutdown' or by turning the Lockout/Enable keyswitch to 'Lockout'. Since the keyswitch is read directly by the MLC as a contact input, it can be used to initiate a controlled shutdown on failure of the BCS.

The DCS automatically enters the shutdown mode of operation whenever any of the following conditions occur:

a. SS1 or SS2 trip the reactor,

b. any SS1 SOR is not poised (i.e., not fully raised),

c. any CAR separates from the CAR drive unit,

d. reactor power exceeds 110% FP or log rate exceeds 10%/s,

e. any one of the two flux instruments shows an irrational reading,

f. a significant deviation appears between the two flux instruments,

g. a PCS low flow condition is detected, or

h. a high reactor outlet temperature is detected.

Upon entering the reactor shutdown mode, the DCS drives the CARs to their down position at a controlled rate, and annunciates the shutdown on the BCS and on the operator console panel. Reactor start-up is inhibited until the condition leading to the automated shutdown is cleared.

5.6 Failure of the DCS

The DCS contains many fault-tolerant features to ensure enhanced reliability. Internal software and hardware checks are performed cyclically and the results are communicated to redundant watchdog timer modules. Should a DCS failure occur, one of two events will follow:

a. the watchdog will initiate a switchover to the second MLC, or

b. if the second MLC is unavailable then the watchdog will signal a dual MLC computer failure.

If a single MLC failure occurs, leading to a switchover to the second unit, then reactor operations can continue until maintenance can be performed. Therefore, the second MLC unit increases the availability of the reactor.

If a dual MLC failure occurs, the watchdog timer modules open redundant contacts. These contacts are normally open contacts held closed by the watchdogs, so that electrical supply failure to the DCS automatically initiates a dual MLC failure. These contacts are monitored by the stepper motor interface systems that drive the CAR motors using MLC control signals. When these contacts open, the stepper motor interface system automatically enters a step-back mode of operation and drives the CARs to their down position at a preset speed. The stepper motor interface hardware is powered from the same UPS, but from different circuits than the MLC.

6.0 DESIGN METHODOLOGY & QUALITY ASSURANCE PROGRAMS

The design programs implemented on the MAPLE-X10 project are a key element in the successful design and implementation of the DCS. The design process centres around a Quality Assurance (QA) program based on the Canadian Standards Association (CSA) N286.0-82, Quality Assurance Program Requirements for Nuclear Power Plants [12]. Project-specific QA documents have been produced to address the specific requirements of the MAPLE-X10 reactor and to comply with the intent of the N286 programs, which were originally specified to meet the requirements of large CANDU-type nuclear power reactors.

The project Quality Assurance Manual is a tier 1 document covering the QA requirements of the MAPLE-X10 project. It presents an overall project description and project organization, including the assignment of responsibilities and authorities of project staff and management for the successful completion and assurance of all phases of the project. These phases, each represented by tier 2 plans, consist of Design, Procurement, Construction, Commissioning, Operations, and Decommissioning.

The tier 2 plan most relevant to the design of the DCS is the Design Quality Assurance Plan. This plan sets the QA procedures and design methods used throughout the project. The Design QA Plan describes design management functions and responsibilities, and specific plans and procedures for document preparation, document transmittal, design review, and document control.

The Design QA Plan is augmented by a Software Quality Assurance Program Manual specific to the development of the DCS software. This tier 3 level document, which is based on CSA Software QA Program requirements [13,14], addresses the specific plans and procedures associated with the DCS, including the preparation of design requirements, the detailed design, and the verification and validation programs.

6.1 DCS Design Plan

A flowchart of the DCS design plan is shown in Figure 8.

The first stage of the design centres around the production of design requirements (DR's) for each reactor system. These requirements are produced in consultation with a number of MAPLE-X10 functional groups, including Reactor Operations, Safety and Reliability, Licensing, Physics, Thermalhydraulics, and Quality Assurance. Each DR is also subjected to a full project team review.

MAPLE-X10 Reactor Operations personnel are responsible for the operation of the facility when construction, commissioning, and licensing are complete. The MAPLE-X10 Operations Branch includes personnel with a variety of backgrounds and operating experience with the NRU (Nuclear Research Universal) and NRX (Nuclear Research eXperimental) reactors located at CRL. This cooperation between design and operations is a crucial element in the design process.

DR's are followed by the completion of design descriptions (DD's) for each reactor system. DD's represent a preliminary or conceptual design. The interaction at this design stage between Design, Operations, Safety and Reliability, Licensing, and other groups is very important. In parallel with the preparation of DD's, the Operations personnel prepare PTA's that eventually evolve into operating procedures. Review of DR's and DD's by Operations and of PTA's by Design is an integral component of the design plan to ensure the design can be successfully operated and maintained.

The DCS provides control and operator interaction with a number of reactor systems. A software technical specification describing the control logic, software structure, and operator interface requirements was produced to amalgamate the control requirements described in each reactor system DR and DD into a single document. This software technical specification was segmented into a set of four documents, including a written presentation of the control requirements, a complete description of all display points, a set of group displays, and a set of software logic diagrams. The software logic diagrams present a complete description of the logic flow and control algorithms to be configured within the DCS.

Review of the DCS software technical specification included both a complete project team review and a functional walkthrough of the logic diagrams. A similar review was conducted with personnel from Moore Instruments Limited, who are responsible for software configuration of the DCS.

The software configuration process is based on the translation of the DCS logic diagrams to logic represented by the interconnection of MLC algorithm blocks. The MLC algorithm block configuration is produced using a customized computer aided design and drafting (CADD) tool called Mycad. The Mycad diagrams are a complete representation of the MLC logic and BCS display. An automatic translator is used to generate the MLC program data base directly from the Mycad diagrams. The configuration process at Moore is segmented into three stages: preparation of Mycad diagrams, integrated software/hardware testing, and final acceptance testing. Review of the Mycad diagrams included a MAPLE-X10 team review and a functional walk-through of the logic. Testing of the integrated software and hardware system follows a detailed test plan prepared by the MAPLE-X10 project. This verification exercise is a comprehensive set of static tests designed to verify the software configuration against the requirements described in the software technical specifications. Following software testing, a final acceptance test will be completed to verify that the system meets all other requirements, including the fault-tolerant and redundancy aspects of the hardware systems.

Following the software design and implementation, the DCS will be subjected to dynamic testing at the Dynamic Analysis Facility at CRL. The principal aim of this test program is to determine the effectiveness (controllability and stability) of the DCS reactor regulation. A full-scope MAPLE-X10 Dynamic Test Bed (DTB) was prepared specifically for this test phase (see sub-section 2.1). Due to the full scope of the DTB and its ability to allow the DTB operator to override any DTB I/O point, the system is suitable for testing the DCS against simulated instrument failures, testing the suitability of the operating procedures centred around the DCS, and for operator training.

Subsequent to completion of dynamic tests and operator training with the DTB, the DCS will be installed at the MAPLE-X10 site and enter the Installation and Commissioning phases of the project. Detailed plans and procedures for these phases are currently in development.

7.0 CONCLUSIONS

The MAPLE-X10 DCS is an integrated control system used to regulate reactor power and process systems. It also provides control and monitoring over the balance-of-plant and can be used to monitor the reactor safety systems. The safety philosophy for the control system is to minimize unsafe events arising from system failures and operational errors. This is achieved through redundancy, fail-safe design, automatic fault detection, and the selection of highly reliable components. Two key operating features contribute to the uniqueness of the MAPLE-X10 DCS. The first is a fully computer-controlled reactor regulation from the shutdown state to full power. The second is its automatic shutdown capability. The control system constantly monitors all critical control parameters and automatically shuts down the reactor when safe limits are exceeded or sensors malfunction. In the unlikely event of a dual computer failure, the MLC watchdog circuitry triggers an emergency signal to each stepper motor interface, which overrides the DCS and inserts each CAR into the core.

Also unique to the MAPLE-X10 DCS is the use of a commercially available dual redundant computer system with enhanced quality assurance. This makes the system cost effective while providing a high degree of maintainability and safety with proven reliability. The DCS computer components include fault-tolerant MLC units and I/O hardware, a non-redundant calculation module (for use where increased reliability is not required), and a BCS operator interface. The MLC is supplied with a set of standard software algorithm blocks that are configured by the user. The BCS also has pre-programmed point displays that are configured into groups and overviews using a menu-driven program. To date, the MLC built-in software has accumulated over 10 million hours of use in conventional process control applications.

The MAPLE-X10 Quality Assurance programs and Design Plans have been developed to meet the stringent standards (CSA N286.0-82) of the Canadian nuclear power reactor industry. These programs control all aspects of both the hardware and software design of the DCS, and provide assurance that the DCS meets all functional and operational requirements.

8.0 REFERENCES

1. A.G. Lee, W.E. Bishop, and W. Heeds. Safety Features of the MAPLE-X10 Reactor Design. AECL Report, AECL-10262 (1990).

2. R.F. Lidstone, G.E. Gillespie, and A.G. Lee. Operating and Safety Features of the MAPLE Reactor. AECL Report, AECL-10322, 1991.

3. W. Heeds, The MAPLE-X Concept Dedicated to the Production of Radio-Isotopes. AECL Report, AECL-8837, 1985.

4. W.M. Goble, and T.W. Tucker. High Availability Controller for Safety Systems Within a Distributed Control Environment. Moore Products Co., Technical Paper 3906, presented at CONTROL EXPO Control Engineering Conference, 1987 May.

5. D.A. Johnson, W.M. Goble, and B.D. Stover. Software Reliability in Control System Instrumentation. Moore Products Co., Spring House, PA 19477.

6. D.E. Butler, W.M. Goble, and B.D. Stover. The New Challenge in Control System Reliability - Software. Moore Products Co., Technical Paper 3915, presented at ISA International Conference and Exhibit, Houston, Texas, 1988.

7. W.M. Goble. Redundancy or Not - Matching Process Controller Architectures to Your Process. Moore Products Co., Technical Paper 3916, presented at ISA Internal Conference and Exhibit, Houston, Texas, 1988.

8. MYCRO Distributed System: Multiloop Controller (MLC) User's Manual. Moore Products Co., Technical Manual TM-202.

9. MYCRO Multiloop Controller Redundancy Design for Fault Tolerance. Moore Products Co., Spring House, PA 19477.

10. MYCRO Basic CRT Station. Moore Products Co., Application Engineering Release AD 3901-B1, Issue 4, 1986 July.

11. Instrument Society of America. Standards and Recommended Practices for Instrumentation and Control. 10 Edition, 1990 Update.

12. Canadian Standards Association. Quality Assurance Program Requirements for Nuclear Power Plants. National Standard of Canada, CAN3-N286.0-82, 1982 September.

13. Canadian Standards Association. Quality Assurance Program for the Development of Software Used in Noncritical Applications. National Standard of Canada, CAN/CSA-Q396.2.1-89, 1989 January.

14. Canadian Standards Association. Quality Assurance Program for the Development of Software Used in Critical Applications. National Standard of Canada, CAN/CSA-Q396.1.1-89, 1989 January.

Table 1: MLC Built-In Algorithms and Standard BCS Display Formats

MLC BUILT-IN ALGORITHMS

#	DESCRIPTION	#	DESCRIPTION
1	PID Controller	16	Totalizer
2	PD Controller	17	Averaging
3	Batch Extension for PID	18	Calculator
4	PID Controller - Velocity	19	Programmer
5	PI Controller - Error Squared	20	Impulse
6	Integral Controller	21	Comparator
7	On-Off Controller	22	Auto-Manual with Bias
8	Dead Time Table	23	Peak-Picker
9	Adaptive Filter	24	Gate
10	Linear Characterizer	25	Fan In
11	Lead Lag	26	Fan Out
12	Signal Select	27	Sequencer
13	Timer	28	Track And Hold
14	Switch	29	Level/Weight Charger
15	Logic	30	Dual Alarm

STANDARD BCS DISPLAY FORMATS

TYPE	DESCRIPTION	TYPE	DESCRIPTION
A	Single Loop Controller	I	Calculator
B	Analogue Indicator	J	General Purpose Point
C	Single Loop Indicator	K	External Set Control
D	Manual Adjuster	L	Programmer
E	Discrete Indicator	M	Multi-Discrete Input
F	Discrete Output	N	Multi-Discrete Output
G	Motor Stop/Start	O	Sequencer
H	Discrete Output with Proof	P	Comment

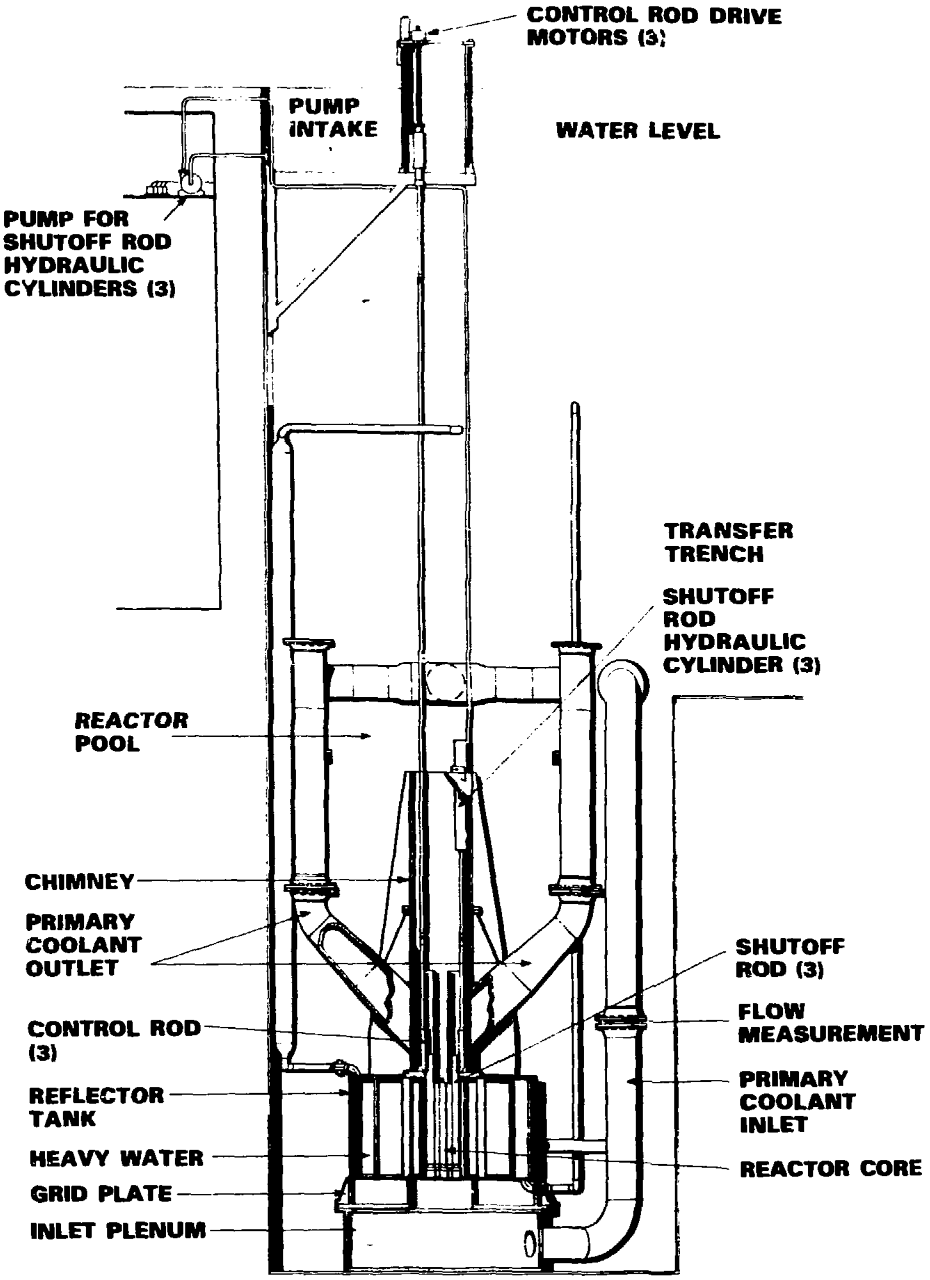


Figure 1. MAPLE-X10 Reactor Structure

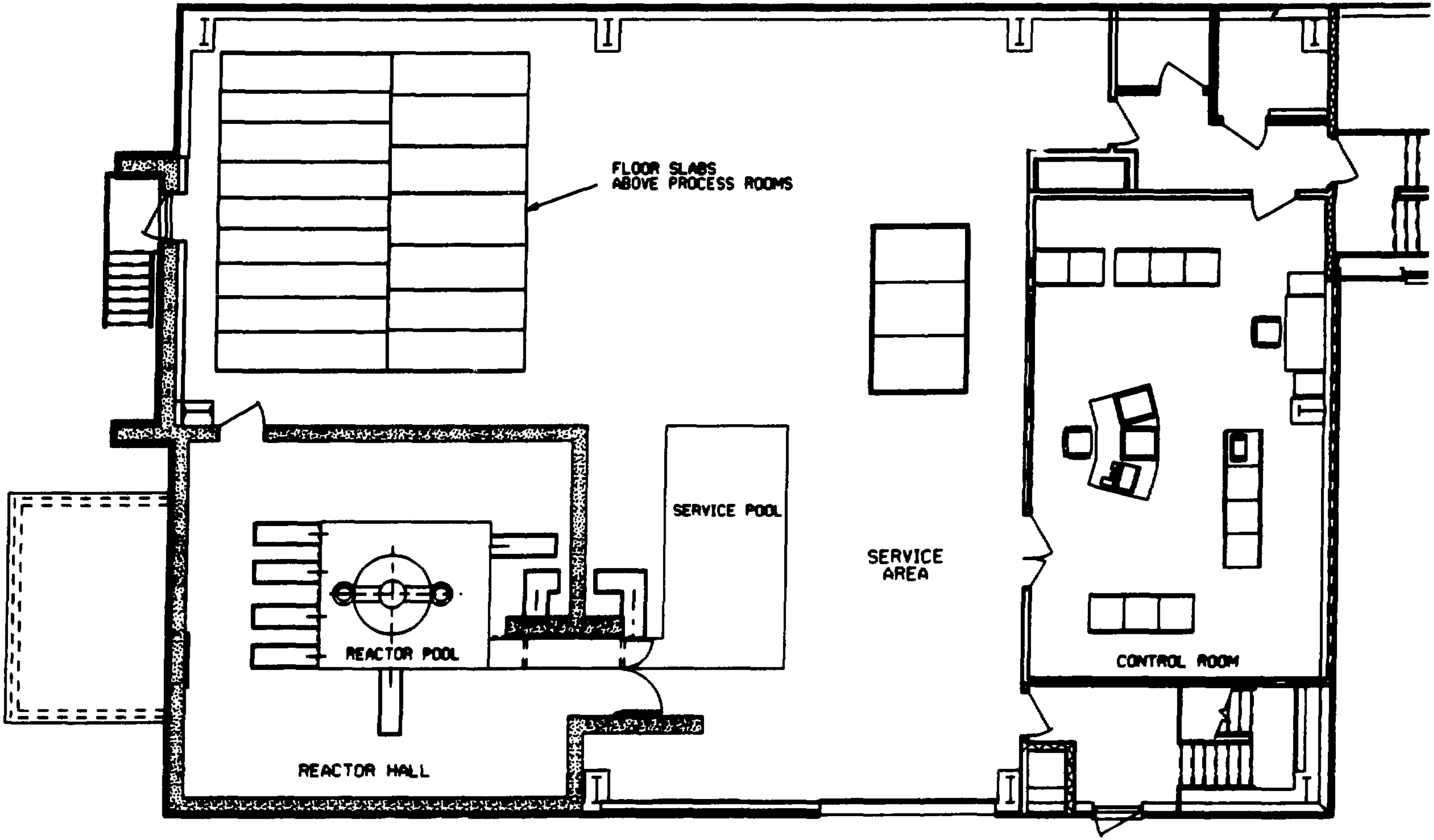


Figure 2. MAPLE-X10 Main Floor Layout

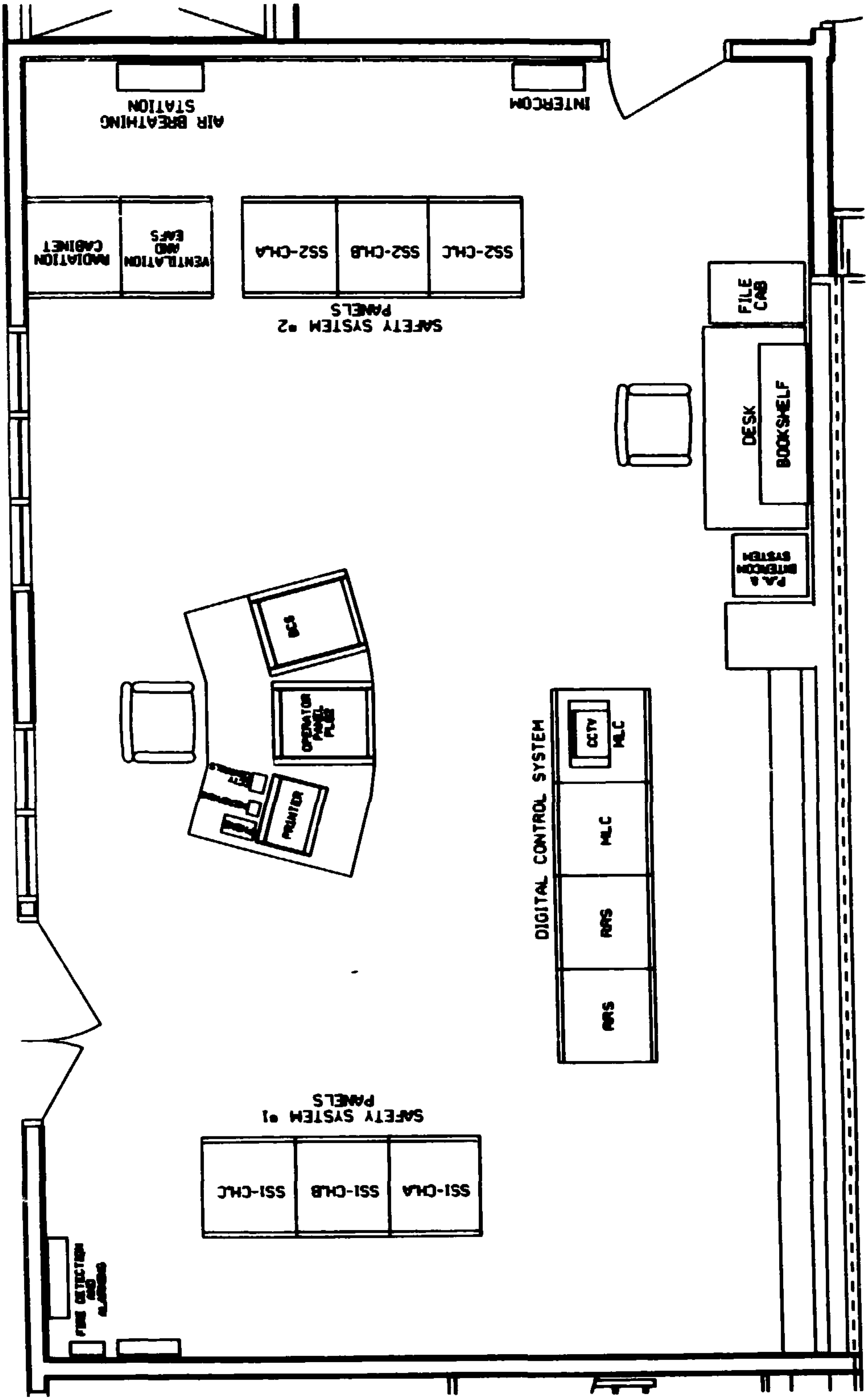


Figure 3. MAPLE-10 Control Room Layout

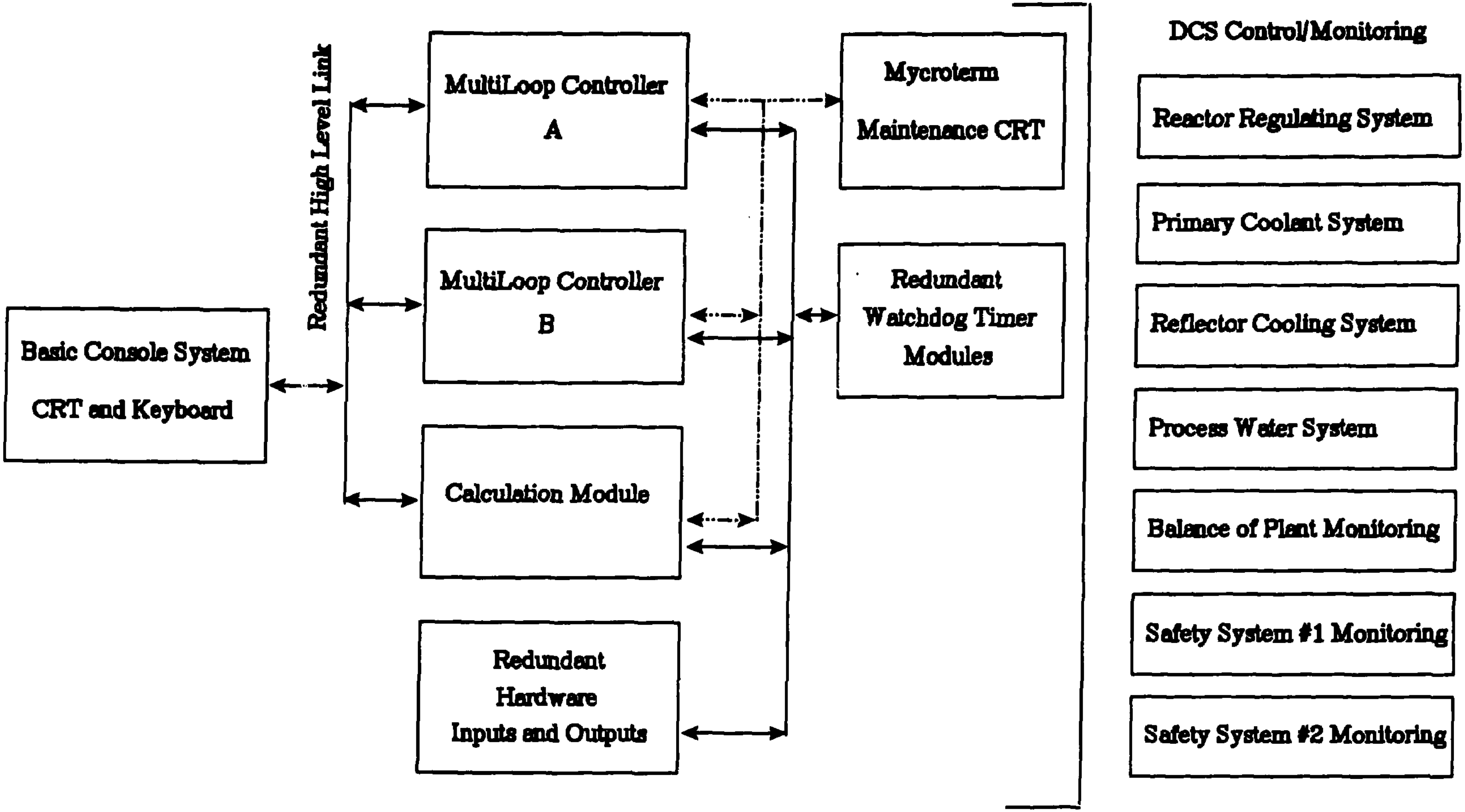
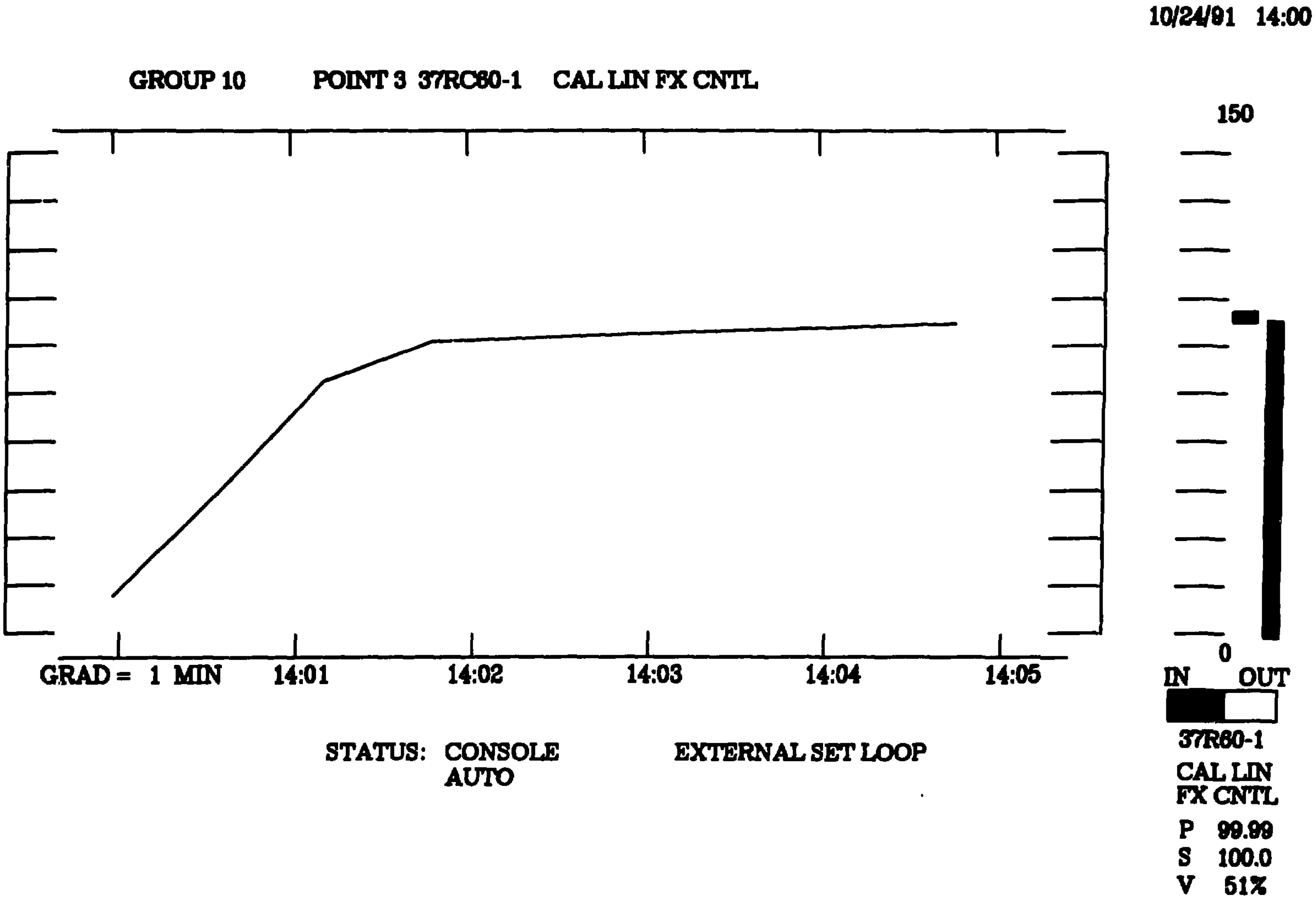


Figure 4. Digital Control System Functional Block Diagram



STATUS: CONSOLE
AUTO

EXTERNAL SET LOOP

P 99.99
S 100.0
V 51%

Figure 5. BCS Display Point, Calibrated Linear Flux Controller.

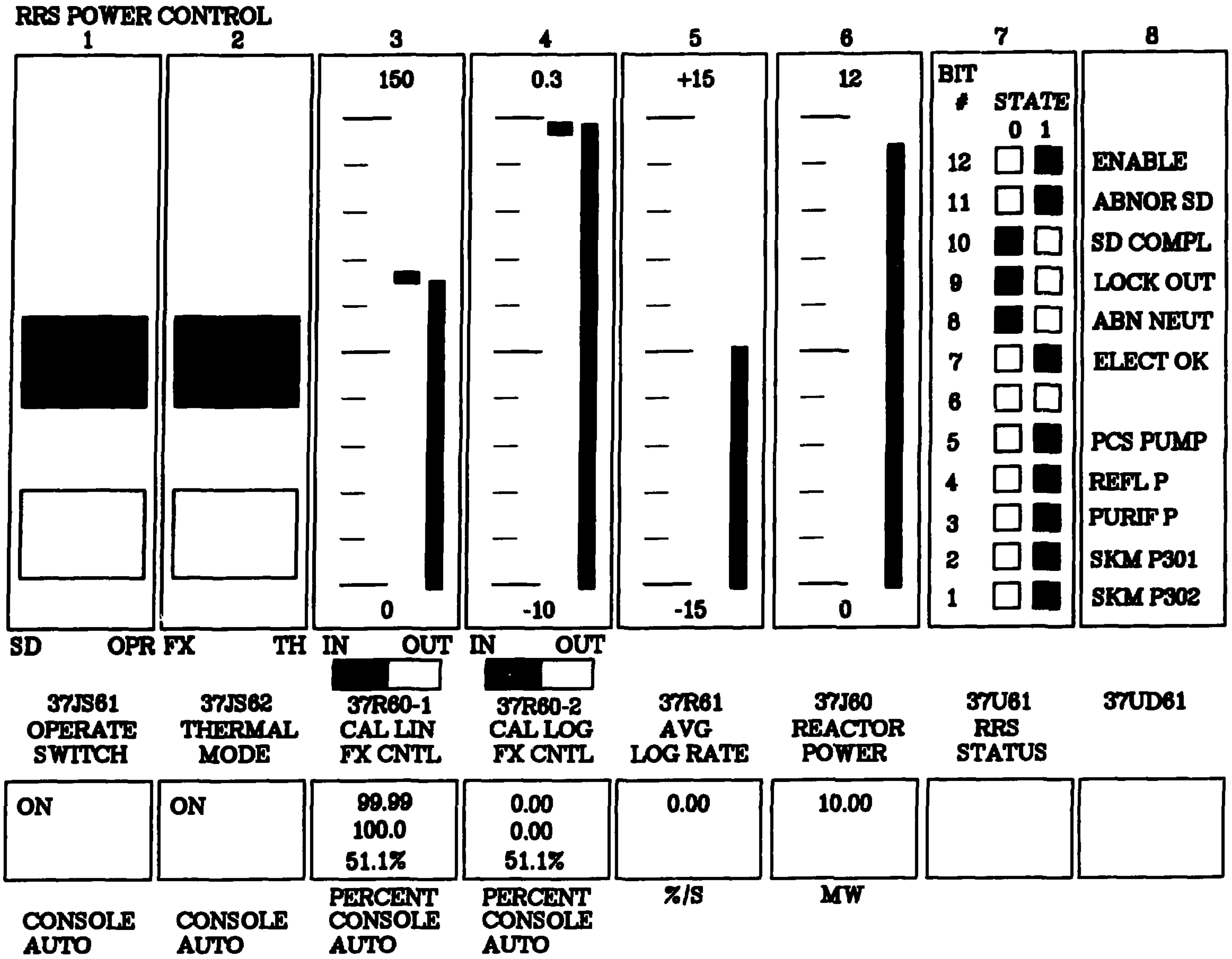


Figure 6. Reactor Regulating System Power Control Group Display

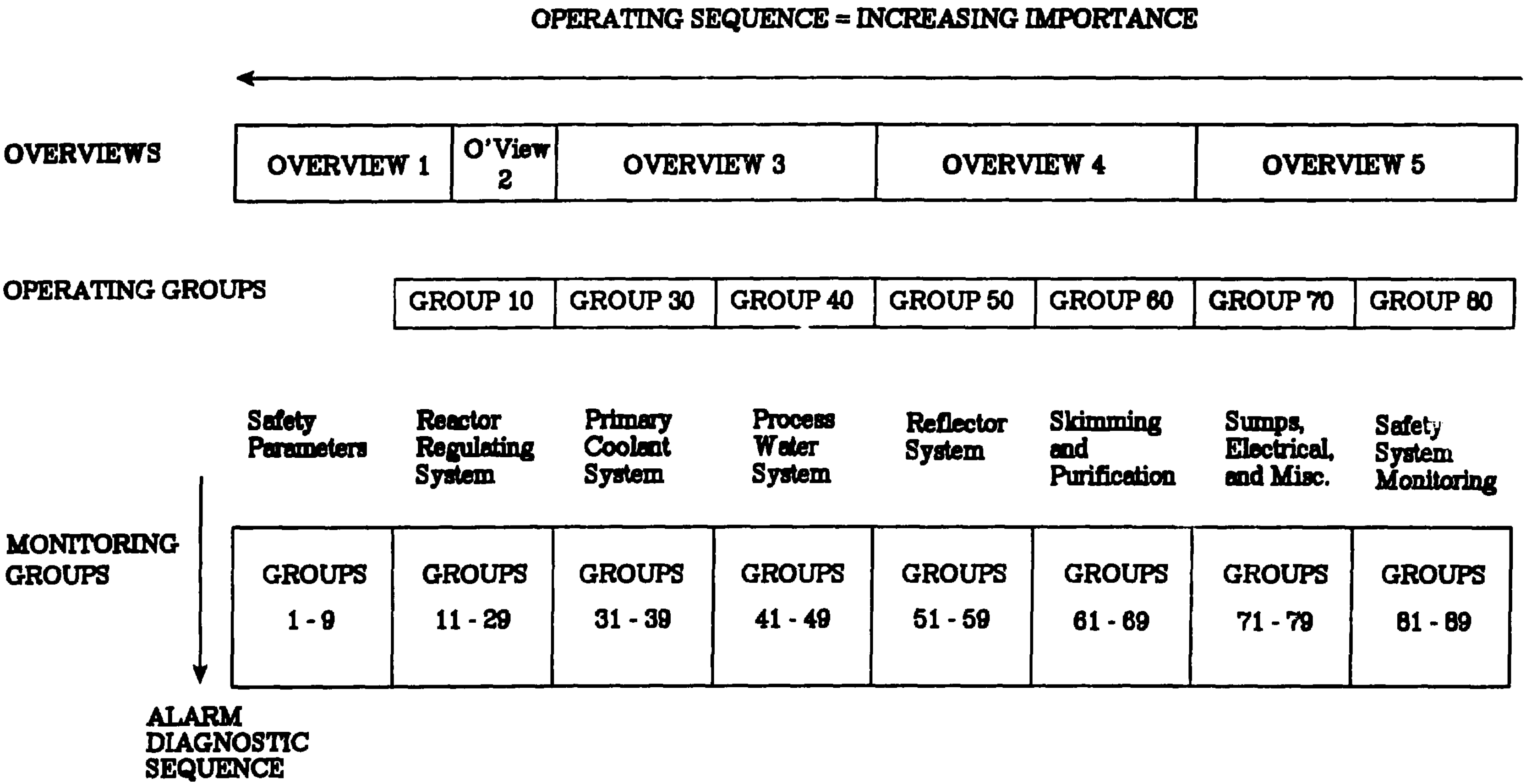
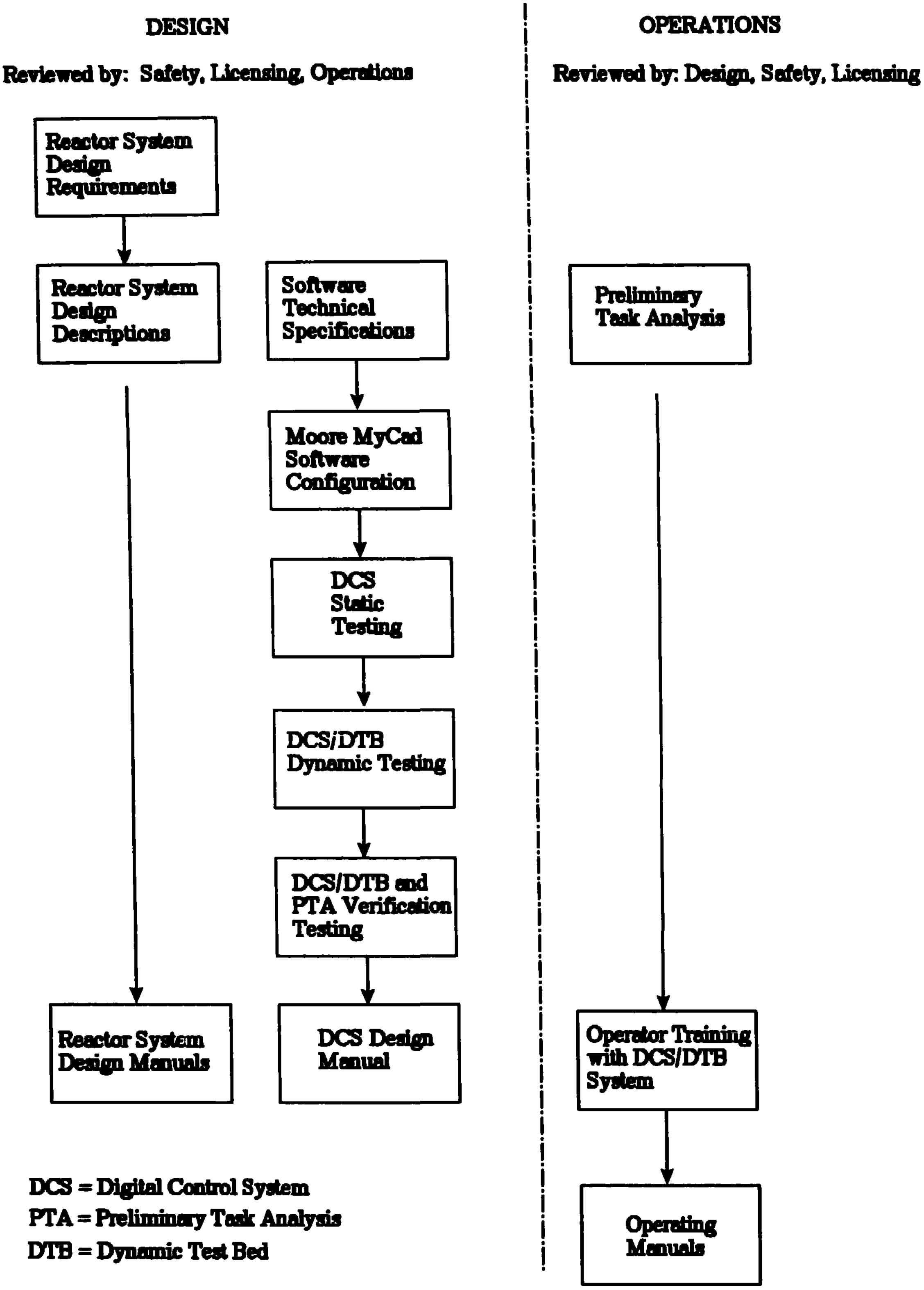


Figure 7. Organization of DCS Operator Interface Showing Operating and Diagnostic Display Sequences



DCS = Digital Control System
PTA = Preliminary Task Analysis
DTB = Dynamic Test Bed

Figure 8. Digital Control System Design Plan and Interactions.

ISSN 0067-0367

To identify individual documents in the series we have assigned an AECL- number to each.

Please refer to the AECL- number when requesting additional copies of this document

from

Scientific Document Distribution Office
Atomic Energy of Canada Limited
Chalk River, Ontario, Canada
K0J 1J0

Price: A

ISSN 0067-0367

Pour identifier les rapports individuels faisant partie de cette série nous avons assigné un numéro AECL- à chacun.

Veuillez faire mention du numéro AECL- si vous demandez d'autres exemplaires de ce rapport

au

Service de Distribution des Documents Officiels
Énergie atomique du Canada limitée
Chalk River, Ontario, Canada
K0J 1J0

Prix: A

2676-91