



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

February 18, 1993

Docket No. 52-001

APPLICANT: Westinghouse Electric Corporation

PROJECT: AP600

SUBJECT: SUMMARY OF MEETING TO DISCUSS THE INSTRUMENTATION AND CONTROL
SYSTEMS OF THE WESTINGHOUSE AP600 DESIGN

On October 6 and 7, 1992, representatives of the Nuclear Regulatory Commission (NRC) and the Westinghouse Electric Corporation met in Monroeville, Pennsylvania to discuss instrumentation and control (I&C) systems of the AP600 design. Enclosure 1 is the list of attendees. Enclosure 2 is a copy of the slide presentation made to the staff.

Westinghouse opened the meeting with a discussion of the general philosophy behind the design. The applicant indicated that much of the design of the AP600 was governed by the EPRI Requirements Document for passive plant designs. Westinghouse indicated that it wants to discuss the relationship of inspections, tests, analyses, and acceptance criteria (ITAAC) and its design process early in the certification review, so that NRC audit points of the process could be established.

The applicant stated that the I&C design uses mostly fibre optics technology, where it makes sense to use that technology. The design does incorporate hard wire at the integrated logic cabinet and integrated protection cabinets. The AP600 uses three kinds of control systems: soft (touch screen), dedicated switches, and diverse actuation switches.

Westinghouse then discussed, in detail, the design of the Protection and Safety Monitoring System, Integrated Protection Cabinets, ESF Actuation Cabinets, Protection Logic Cabinets, Plant Control System, Data Display and Processing System, and Operations and Control Center System. In addition, they discussed the testing methods that will be employed on the systems.

The applicant stated that the I&C system meets the single failure criteria. The AP600 design meets the first three of the four positions in the July 6, 1992 draft Commission paper. However, the fourth position requires a safety-grade backup system. Westinghouse is developing a non-safety Diverse Display System. Because the focus of the issue is on the failure of the software, and not the hardware, the applicant proposed to make the system non-safety. The staff indicated it would evaluate Westinghouse's proposal.

Westinghouse proposed to use the probabilistic risk assessment (PRA) in lieu of a failure modes effects analysis (FMEA) because the PRA addresses common-cause failures and the FMEA does not. Westinghouse stated that the PRA only

February 18, 1993

looked at worst-case failures that affect safety, and does not address nuisance failures. The FMEA does not allow quantification or identification of system dependencies, unavailabilities due to test and maintenance, common-cause failures, or human error, while the PRA does. The staff indicated that Westinghouse may need to provide a way to use the PRA to demonstrate clearly the information that an FMEA provides.

Westinghouse then discussed its verification and validation program.

The applicant then discussed the ITAAC for the I&C system. Westinghouse intends to develop ITAACs for systems that perform safety and defense functions. The applicant believed that items such as electromagnetic interference (EMI), radio-frequency interference (RFI), and separation would be covered under Appendix B of 10 CFR Part 50 and 10 CFR 50.49. Therefore, Westinghouse indicated that they do not believe it is necessary to develop a generic ITAAC to specifically address these issues, and proposed to use a different approach to address the generic ITAACs that are being developed for the ABWR. The staff indicated it would evaluate Westinghouse's proposal.

Original Signed By:

Thomas J. Kenyon, Project Manager
Standardization Project Directorate
Associate Director for Advanced Reactors
and License Renewal
Office of Nuclear Reactor Regulation

Enclosures:

1. List of Attendees
2. Slides

cc w/enclosures:
See next page

DISTRIBUTION: w/encls.

Docket File PDST R/F
PDR WTraver
RHasselberg

TMurley/FMiraglia, 12G18
PShea

DCrutchfield
RBorchardt

w/o enclosures:

MChiramal, 8H3 HLi, 8H3
ACRS (11) EJordan, 3701

TKenyon
JMoore, 15B18

OFC:	LA:PDST:ADAR	PM:PDST:ADAR	(AD):PDST:ADAR	
NAME:	PShea	TKenyon:sg	RBorchardt	
DATE:	02/17/93	02/16/93	02/18/93	

OFFICIAL RECORD COPY:

DOCUMENT NAME: I&C_MTG.SUM

Docket No. 52-003

Westinghouse Electric Corporation

cc: Mr. Nicholas J. Liparulo
Nuclear Safety and Regulatory Analysis
Nuclear and Advanced Technology Division
Westinghouse Electric Corporation
P.O. Box 355
Pittsburgh, Pennsylvania 15230

Mr. B. A. McIntyre
Advanced Plant Safety & Licensing
Westinghouse Electric Corporation
Energy Systems Business Unit
Box 355
Pittsburgh, Pennsylvania 15230

Mr. John C. Butler
Advanced Plant Safety & Licensing
Westinghouse Electric Corporation
Energy Systems Business Unit
Box 355
Pittsburgh, Pennsylvania 15230

Mr. M. D. Beaumont
Nuclear and Advanced Technology Division
Westinghouse Electric Corporation
One Montrose Metro
11921 Rockville Pike
Suite 350
Rockville, Maryland 20852

Mr. Sterling Franks
U. S. Department of Energy
NE-42
Washington, D.C. 20585

Mr. S. M. Modro
EG&G Idaho Inc.
Post Office Box 1625
Idaho Falls, Idaho 83415

Mr. Steve Goldberg
Budget Examiner
725 17th Street, N.W.
Room 8002
Washington, D.C. 20503

I&C MEETING ATTENDEES

OCTOBER 6 AND 7, 1992

NAME

BRIAN BELEY
JOSEPH BIRSA
KAZUHIRO TSURU
JOSEPH LEWI
MATT CHIRAMAL
HULBERT LI
THOMAS KENYON
ALAIN GOUFFON
JEAN HULST
BERTRAND DE L'EPINOTS
BOB WYMAN
ALLISON NEGUS
WIESLAW SZMEK
J. BRIAN REID
SCOTT NEWBERRY
PHILLIPE GROS-GEAN
SHELEGH MORANDINI
EDWARD A. HART
ANDREA STERDIS
GILBERT W. REMLEY

ORGANIZATION

W PED MARKETING
W NATD PI&CS
W NATD PI&CS
CEA/IPSN (FRANK)
NRC/HICB
NRC/HICB
NRC/PDST
CEA/IPSN/France
DSIN/France
DSIN/France
NRC/LLNL
W NATD/MMD
W NATD
W NATD
NRC/PDLR
NATD-INTERNATIONAL
NATD-PRA
NATD-NUCLEAR EQUIP. ENG.
NATD
WPCD

Enclosure 1

AP600

INSTRUMENTATION AND CONTROL

•

October 6 and 7, 1992

AP600

INSTRUMENTATION AND CONTROL

•

INTRODUCTION

AGENDA FOR USNRC MEETING ON I&C, OCTOBER 6,7 1992

OCT. 6	WESTINGHOUSE ENERGY CENTER	
TIME	TOPIC	RESP.
8:30 - 9:00	INTRODUCTIONS / REVIEW AGENDA	NRC\ (W)
9:00 - 9:30	OVERVIEW	JBR
9:30 - 10:30	PROTECTION AND SAFETY MONITORING SYSTEM - ARCHITECTURE - HARDWARE	JJB
10:30 - 11:45	PLANT CONTROL SYSTEM [420.6] - ARCHITECTURE - HARDWARE	JJB
11:45 - 12:15	LUNCH	
12:15 - 1:00	DIVERSE ACTUATION SYSTEM - ARCHITECTURE - HARDWARE	JBR
1:00 - 1:45	DATA DISPLAY AND PROCESSING SYSTEM - ARCHITECTURE - HARDWARE	JJB
1:45 - 2:15	OPERATIONS AND CONTROL CENTERS SYSTEM [420.5] - ARCHITECTURE - HARDWARE	AKN
2:15 - 2:45	VERIFICATION AND VALIDATION PROGRAM	JJB
2:45 - 4:00	PMS ITAAC	AS/ JJB
4:00 - 4:15	PROCESS BLOCK DIAGRAMS [420.3]	JJB
4:15 - 5:15	PRA ISSUES [420.2]	SM
5:15 - 5:30	EPRI URD COMPLIANCE - PARTICIPATION IN URD, CHAP 10 - SSD TABLE - URD COMPLIANCE MATRIX	JBR

OCT. 7	WESTINGHOUSE PROCESS CONTROL DIVISION	
TIME	TOPIC	RESP.
8:30 - 9:00	OVERVIEW OF DIVISION PRODUCTS/PROJECTS	PCD
9:00 - 9:30	PLANT TOUR (GENERAL)	PCD
9:30 - 10:30	IPS PROTOTYPE ROOM	PCD
10:30 - 10:45	EMI/RFI FEATURES [420.1]	JJB
10:45 - 11:15	NOK BEZNAU COMPUTER SYSTEM TEST AREA	PCD
11:15 - 12:15	SIZEWELL WISCO SYSTEM TEST AREA	PCD
12:15 - 1:15	LUNCH	
1:15 - 2:00	WRAPUP	ALL
1002nc:m .wpf	J. B. Reid, 10/2/92	

NATD ATTENDEES

J. J. BIRSA
R. B. MILLER
S. MORANDINI
A. K. NEGUS
J. B. REID
A. L. STERDIS
W. SZMEK
K. TSURU

NRC ATTENDEES

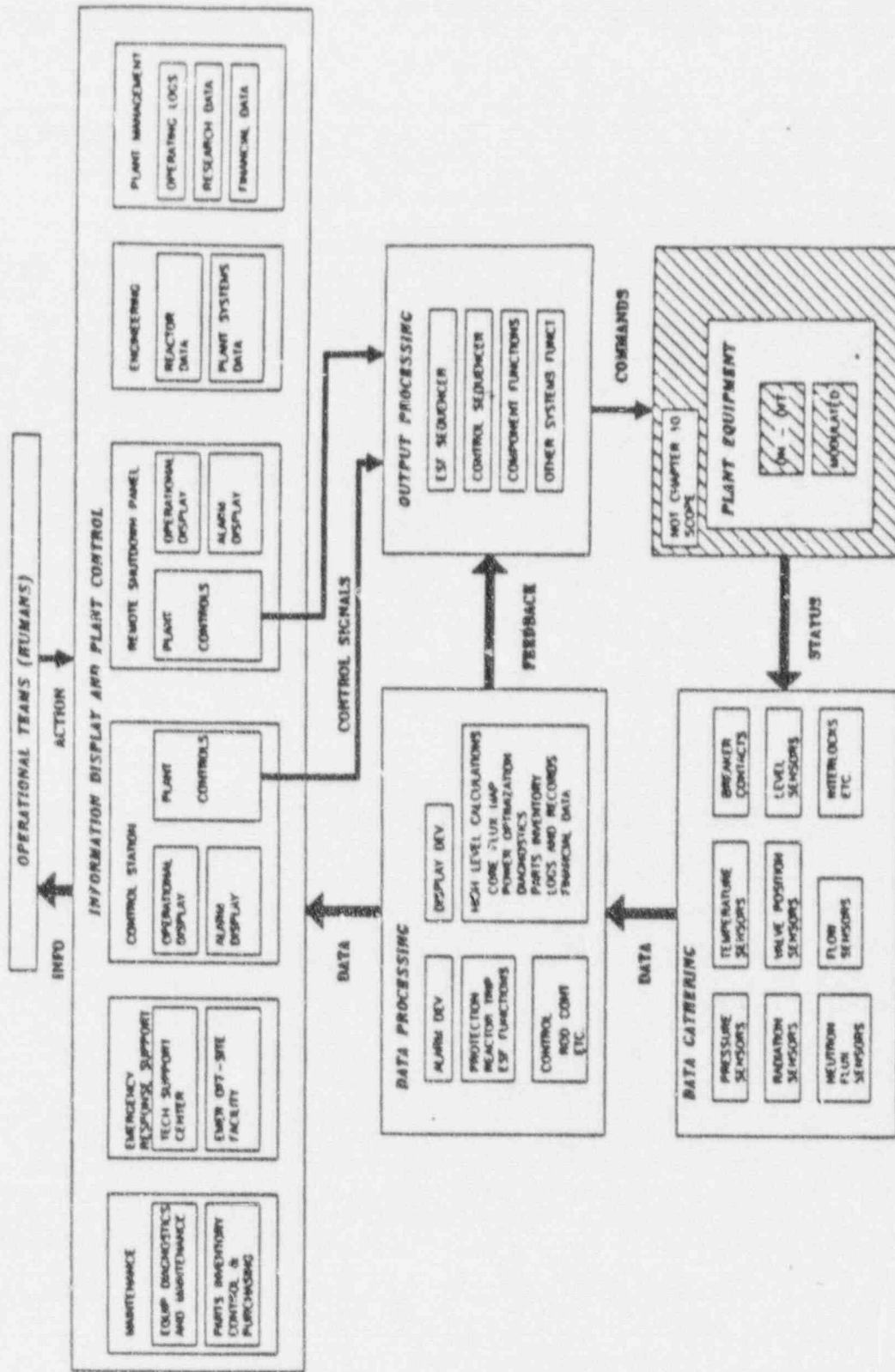
S. NEWBERRY
H. LI
M. CHIRANAMAL

AP600

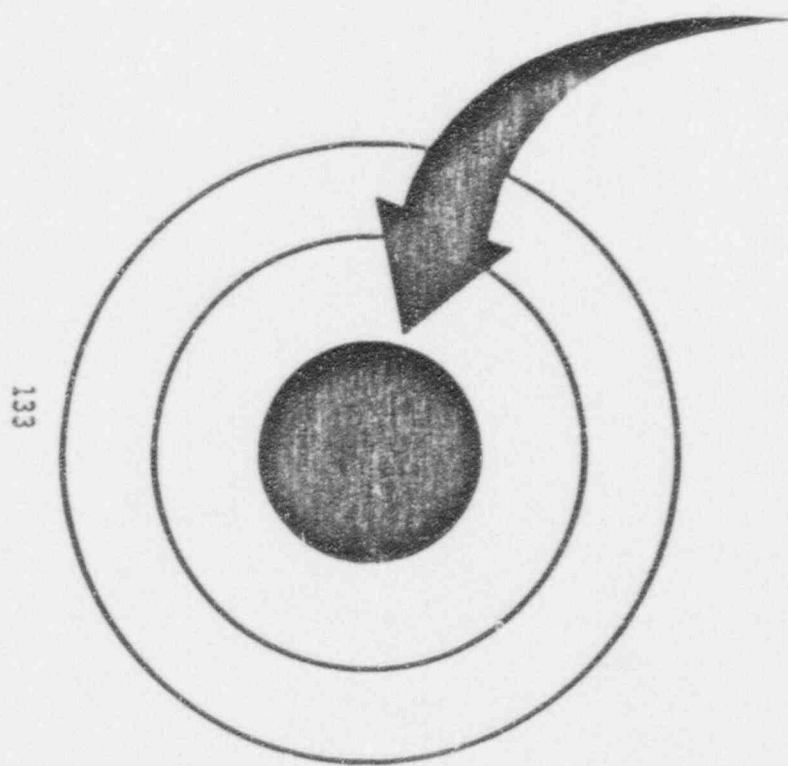
INSTRUMENTATION AND CONTROL

OVERVIEW

FIGURE 10.1-1 ADVANCED LIGHT WATER REACTOR
M-MIS INTEGRATED SYSTEM ARCHITECTURE



Equipment Design Philosophy



Core Digital Processors

Characteristics:

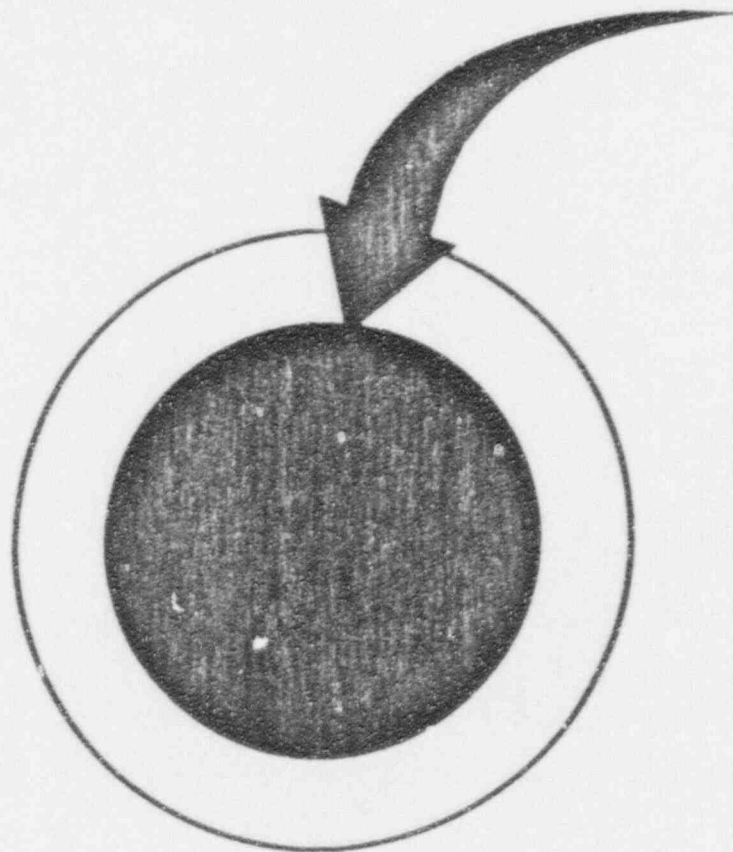
- Rapid technology evolution
- Large development cost
- Other industries set standard
- Complex modules

Design Approach:

- Purchase from vendor
- Select board level modules
- Relies on broad-based experience
- Standard interface to next layer

Equipment Design Philosophy

134



Input/ Output Modules

Characteristics:

- Established technology
- Relatively large numbers
- Impact by Nuclear requirements

Design Approach:

- Custom design by (W)
- Integrate with diagnostics
- Design verification testing

Equipment Design Philosophy

Packaging

Characteristics:

- Seismic integrity
- Protection from interference
- Control of access

Design Approach:

- (w) designed cabinet
- EMI/ RFI shielding
- Modular replaceable units

Equipment Design Philosophy

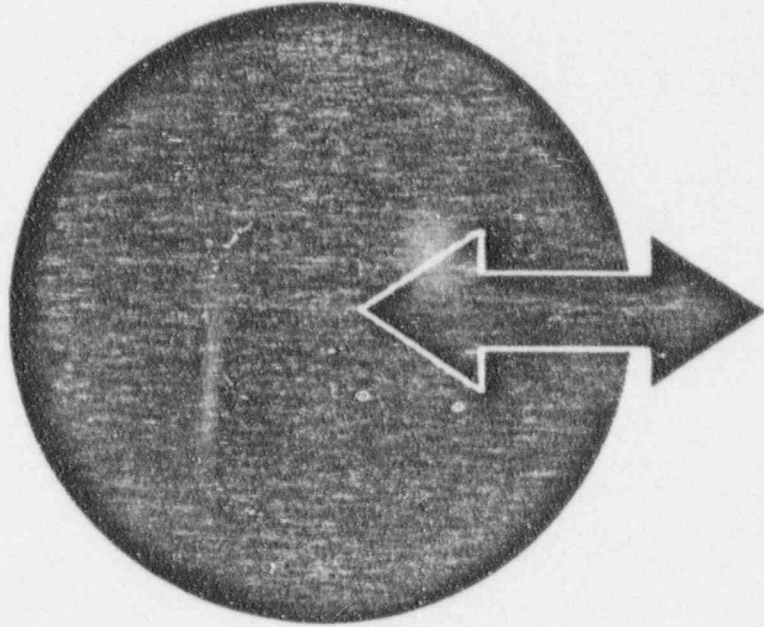
Interfaces to Other Systems

Characteristics:

- Multiple vendor interfaces
- Potential for interaction
- Requirements often vague

Design Approach:

- Use international standards
- Use fiber optic data links
- Keep data format flexible



Westinghouse Design Philosophy

MAINTENANCE FEATURES

Characteristics:

Complex functions

Diffuse symptoms

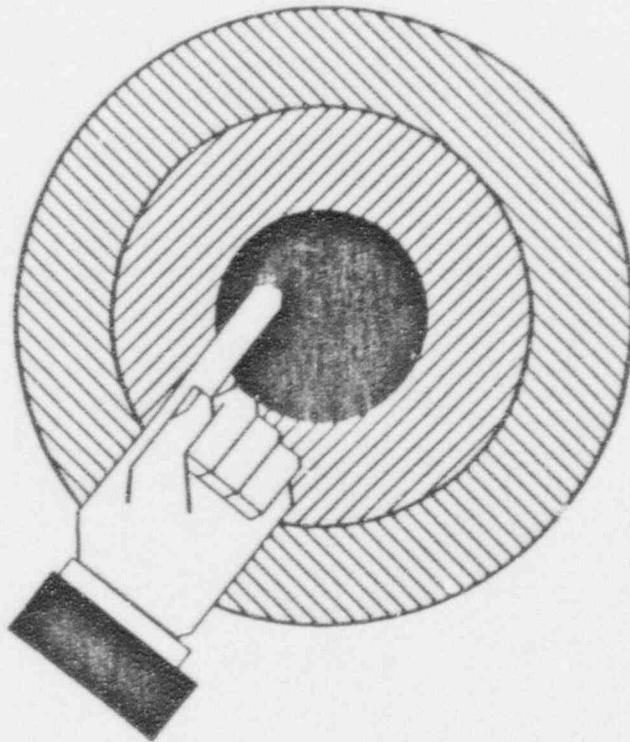
Key to reliability

Design Approach:

Automatic tester

Comprehensive diagnostics

Plug-in modules



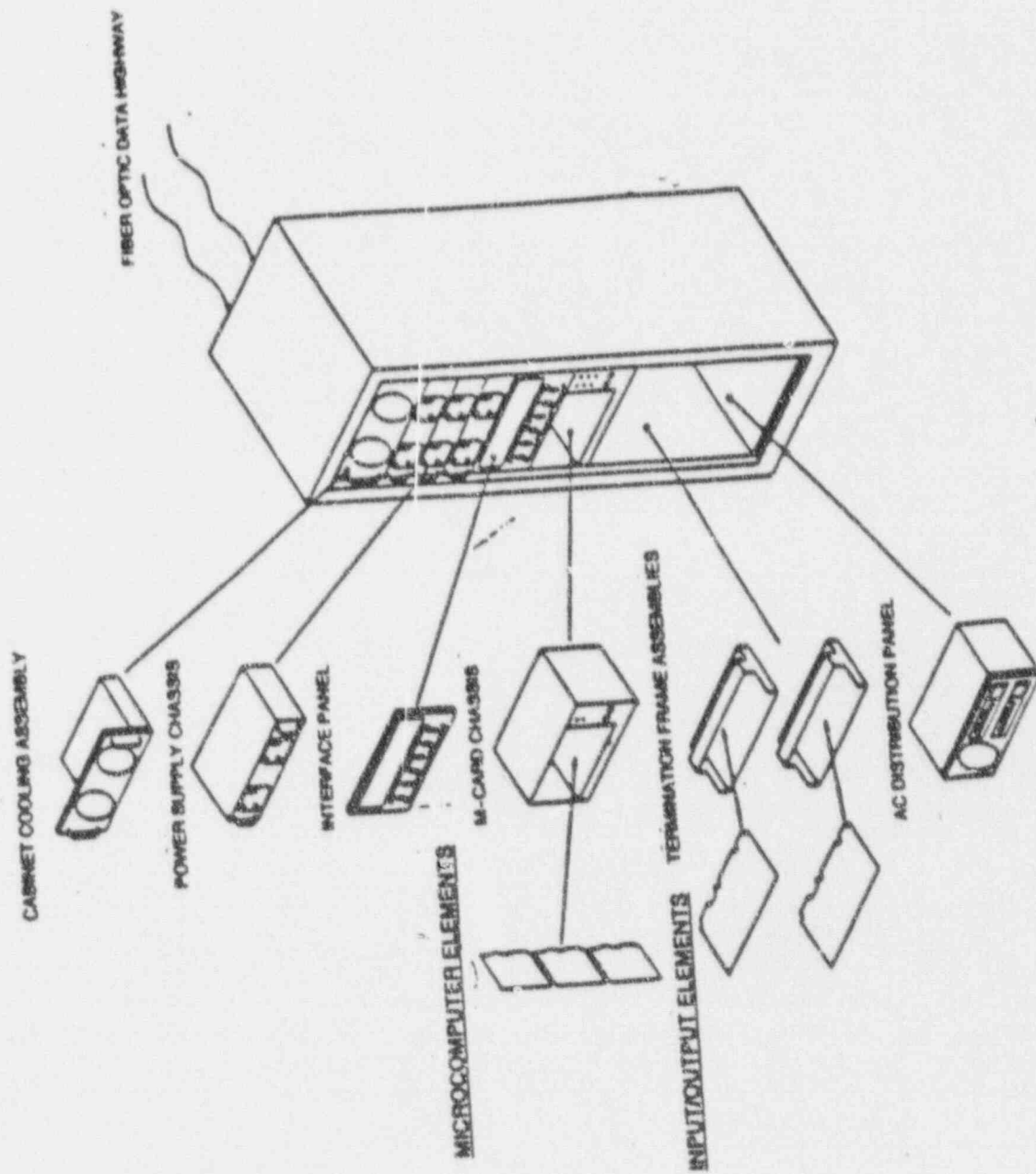


Figure 3 1-3 - Equipment Modular Design Philosophy

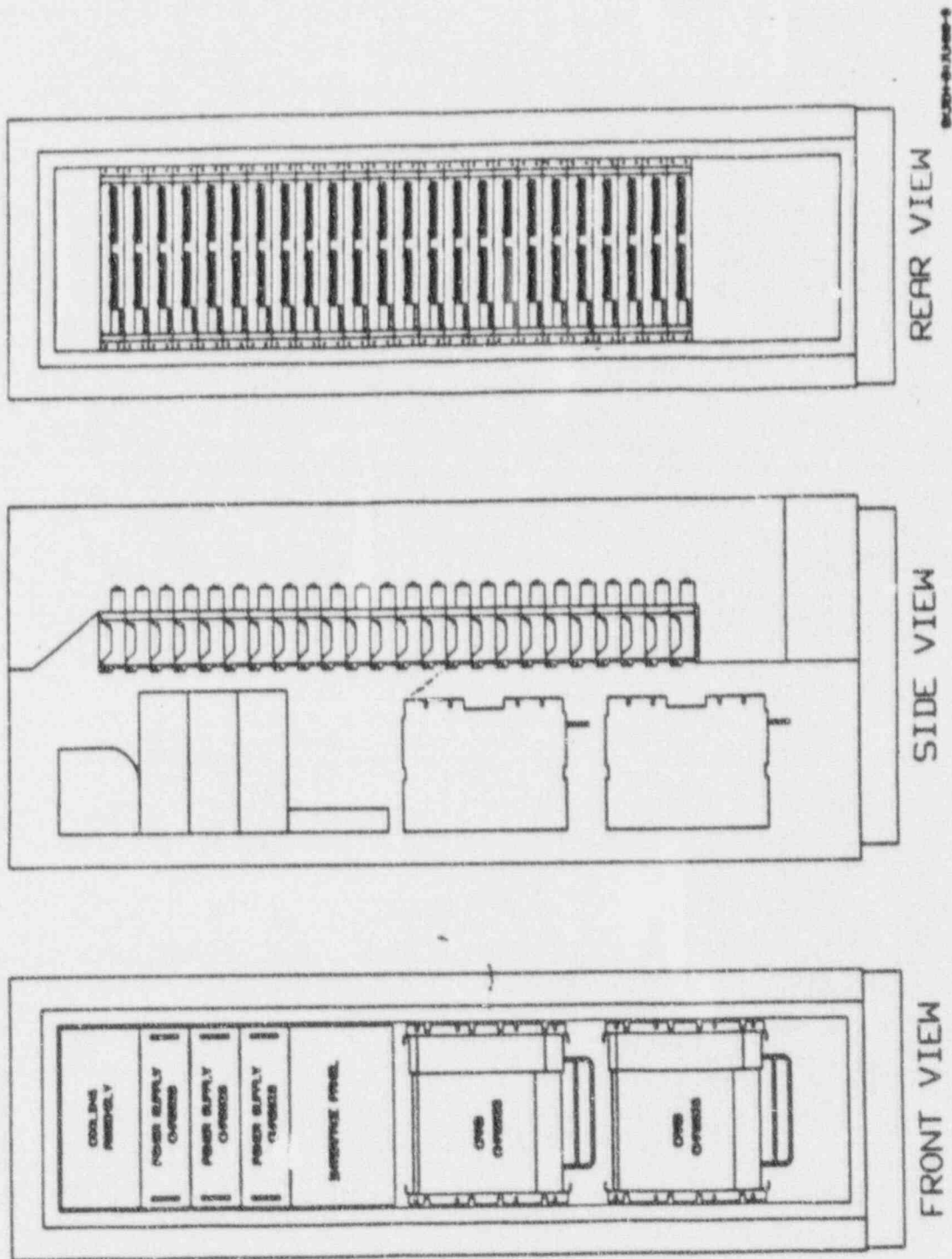


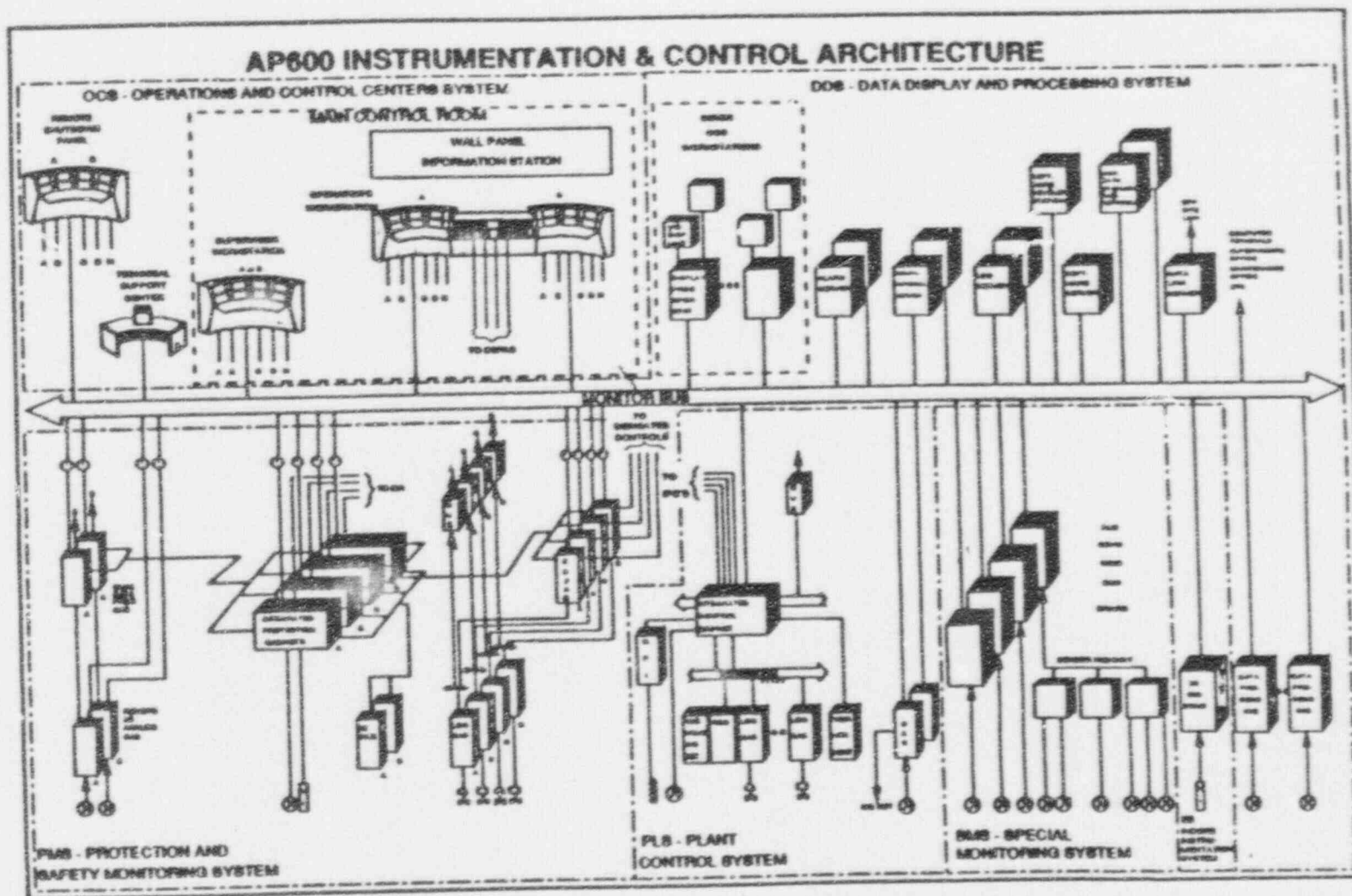
Figure 3.1-4 - General Cabinet Layout

AP600

PROTECTION AND SAFETY MONITORING SYSTEM

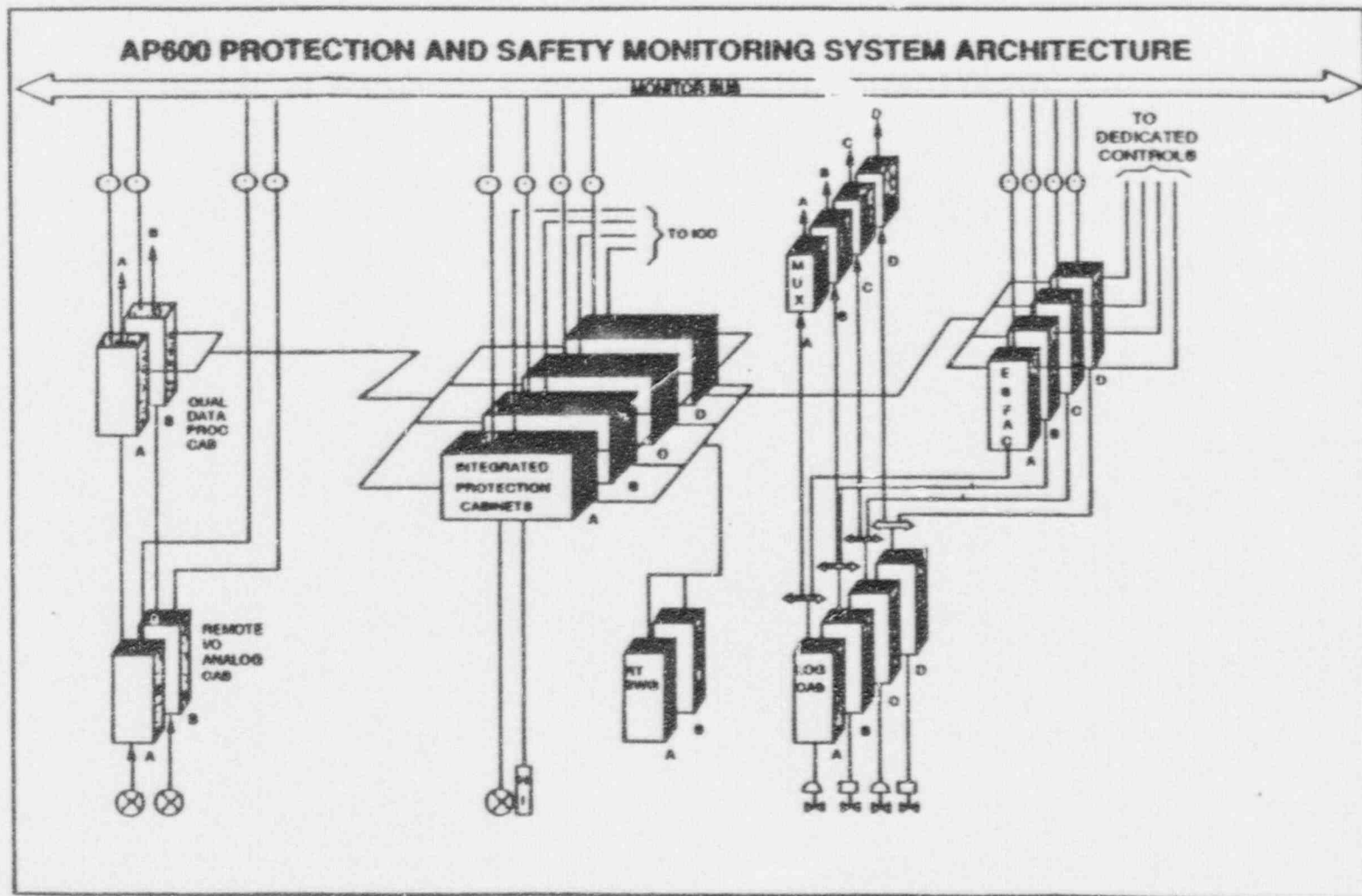


ARCHITECTURE



File: AP6ARCH.DRW
JMS - 04/30/92

Figure 1.0-1



AP600

PROTECTION AND SAFETY MONITORING SYSETM

•

INTEGRATED PROTECTION CABINETS

AP600

PROTECTION AND SAFETY MONITORING SYSTEM

•

**ENGINEERED SAFETY FEATURES
ACTUATION CABINETS**

AP600

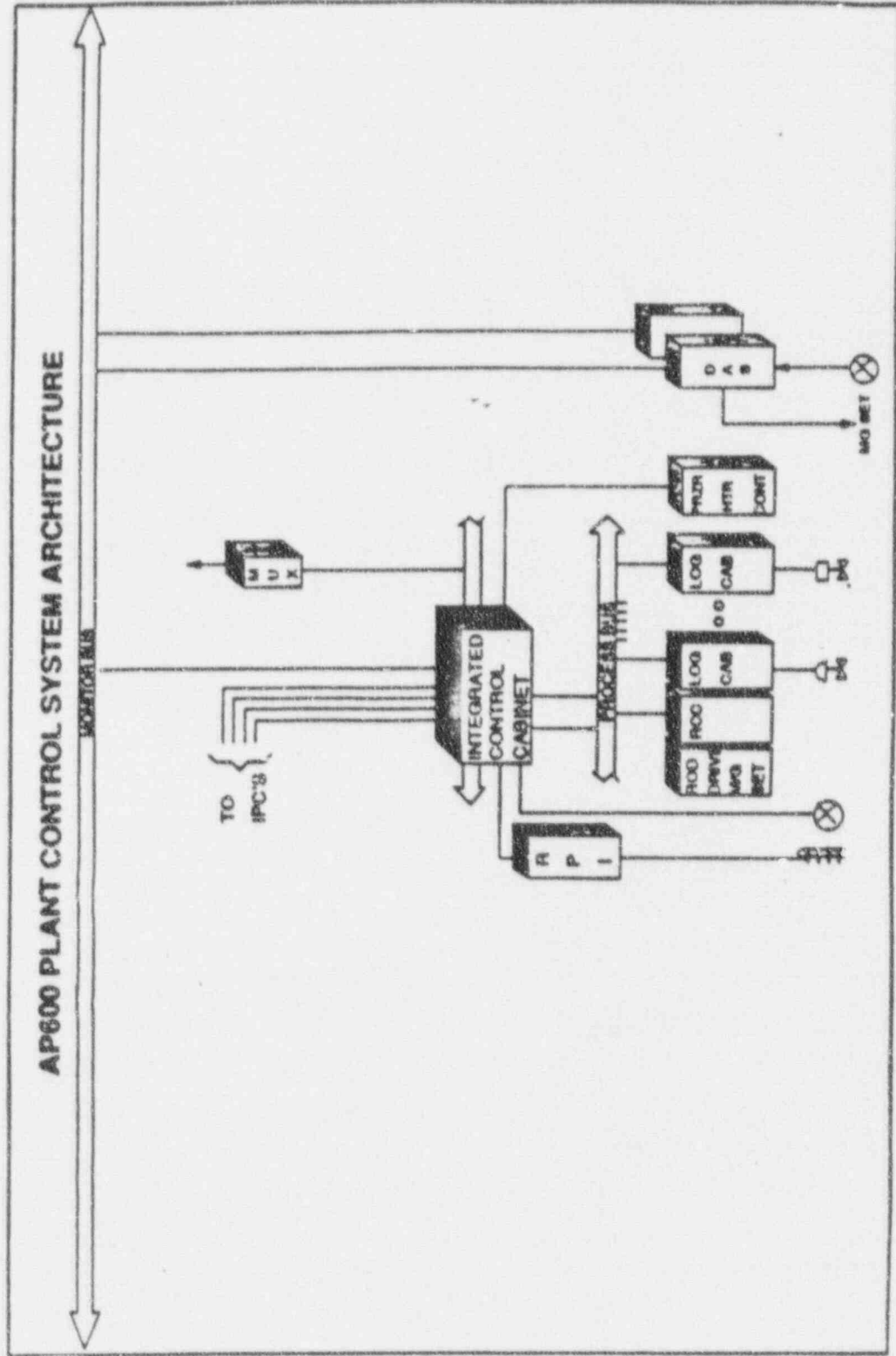
PROTECTION AND SAFETY MONITORING SYSTEM



PROTECTION LOGIC CABINETS

AP600

PLANT CONTROL SYSTEM



AP600

DIVERSE ACTUATION SYSTEM

AP600 DIVERSE ACTUATION

- **Current PWRs Provide Diverse Actuation**
 - ATWT Rule
 - Westinghouse provides diverse actuation (AMSAC) to trip turbine and start AFWS
- **Pressures To Increase Diverse Actuation**
 - Common mode failure of the IPS will limit the core damage frequency of advanced plants
 - NRC / ACRS concerns (SECY-91-292, 10/91)
 - Software common mode failure
 - Multiplexing / I/O card common mode failures
- **Westinghouse AP600 Approach**
 - Latest advanced I&C design uses the same micro processor based design for both the control and the protection system design
 - The AMSAC will be expanded somewhat so that the plant CDF / SRF goals are met
 - Some additional diverse automatic actuations
 - Some diverse manual controls
 - Some diverse control board indications
 - The diverse actuation hardware / software will be made diverse from the control & protection system
 - The diverse actuation equipment will be non-safety grade

AP600 DIVERSE I&C FUNCTIONS

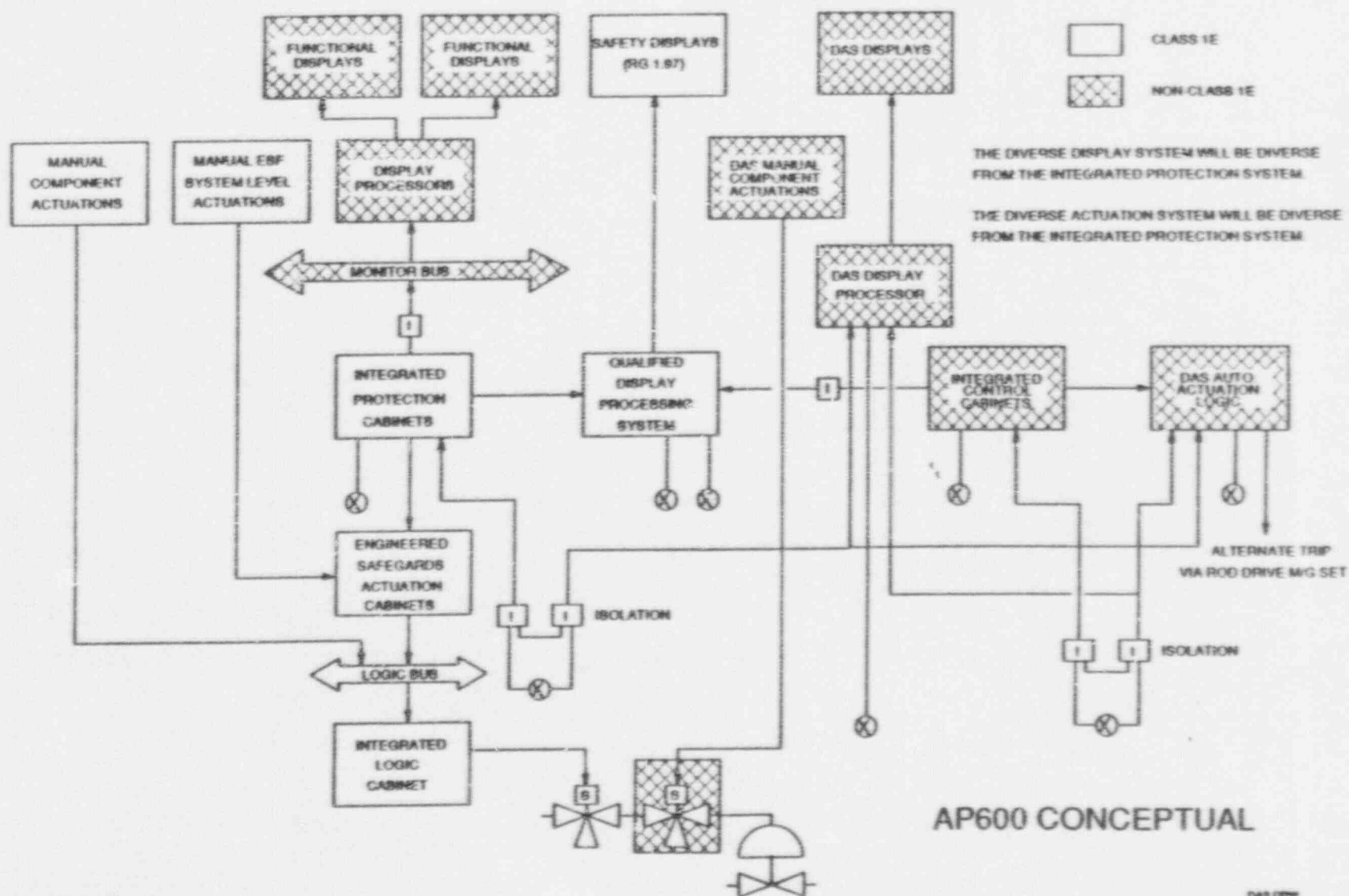
- **Diverse I&C Functions**
 - ATWT mitigation
 - Reduce core damage & containment failure probability
 - Reduce dependance on operator actions
- **Diverse Automatic Actuations**
 - Reactor trip (MG set)
 - Turbine trip (turbine isolation valves)
 - PRHR HX, CMT, PCCS actuation (valves)
 - Selected containment line isolation (valves)
- **Diverse Manual Controls**
 - Hard wired controls mounted on main control board, bypass IPS and DAS
 - Limited number hard wired controls
 - Backup for automatic DAS actuations
 - For ADS valves & H2 igniters
- **Diverse Control Board Indication**
 - Limited number diverse control board indication
 - To confirm diverse automatic actuations
 - To guide operators manual actions

AP600 DIVERSE ACTUATION

• Instruments used for Diverse Actuation

Instruments	Automatic Actuations	Manual Actions
1. SG wide range level	- Reactor trip - Turbine trip - PRHR HX	- Reactor trip - Turbine trip - PRHR HX
2. Pressurizer level	- CMT - RCP trip	- CMT - RCP trip
3. Hot leg temperature	- PRHR HX	- PRHR HX - ADS
4. Hot leg level	- IRWST MOV (shutdown)	- CMT - ADS
5. SG high level		- PRHR HX - ADS
6. Containment temperature	- PCCS - Cont isolation	- PCCS
7. Containment H2		- H2 Igniter

PROTECTION SYSTEM/DIVERSE ACTUATION SYSTEM BLOCK DIAGRAM



DIVERSITY GUIDELINES

DIFFERENT VENDOR'S PRODUCTS

DIFFERENT CIRCUITS

DIFFERENT PROGRAMMING LANGUAGES

DIFFERENT OPERATING SYSTEMS

BUT:


FUNDAMENTAL COMPONENTS SUCH AS RESISTORS,

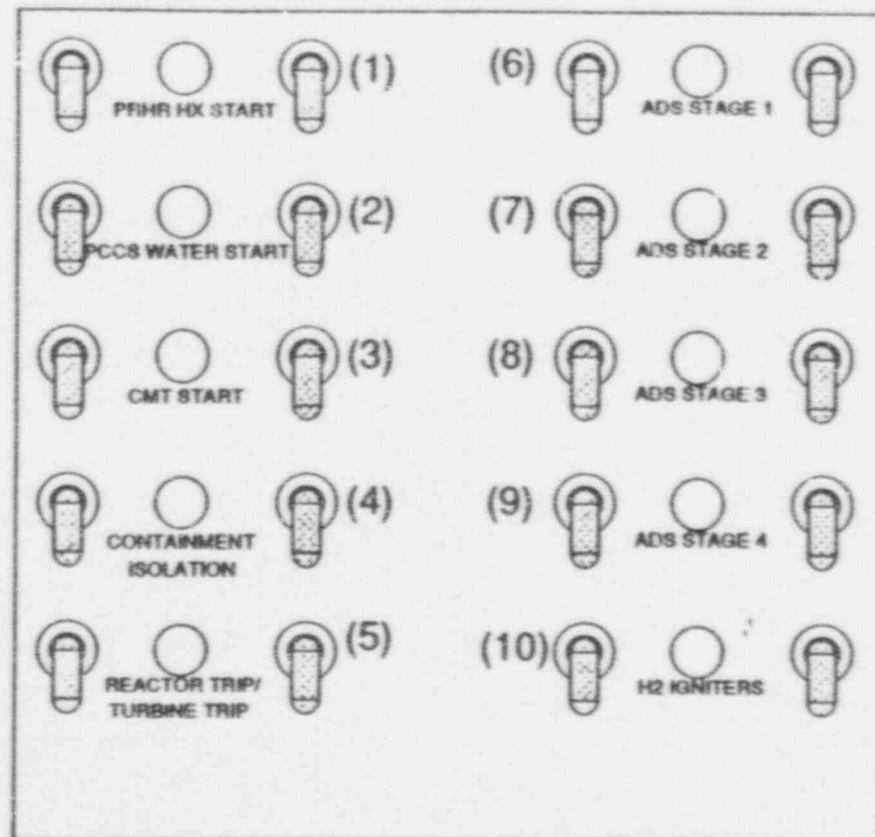
TRANSISTORS, LSI CHIPS MAY BE THE SAME

DIVERSITY IN THE DIVERSE ACTUATION SYSTEM

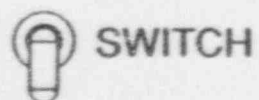
SYSTEM	PRIMARY PROTECTION SYSTEM	DIVERSE ACTUATION SYSTEM
INPUT SIGNAL CONDITIONING	WESTINGHOUSE I/O BOARDS	non-WESTINGHOUSE I/O BOARDS
INPUT SIGNAL CONVERSION	Intel A/D CONVERTER	non-Intel A/D CONVERTER
SIGNAL PROCESSING (SOFTWARE)	PLM/86 MACHINE LANGUAGE NO OPERATING SYSTEM	BASIC, ETC. DOS
SIGNAL PROCESSING (HARDWARE)	Intel SINGLE BOARD COMPUTERS '186, '286, '386 ... PROCESSORS	"XT-CLASS" PC COMPATIBLE 8088, 8086 PROCESSORS PROGRAMMABLE LOGIC CONTROLLER
OUTPUT SIGNAL CONDITIONING	WESTINGHOUSE I/O BOARDS SOLID STATE RELAYS	non-WESTINGHOUSE I/O BOARDS ELECTRO-MECHANICAL RELAYS
OPERATION	AUTOMATIC FUNCTIONAL TEST CONTINUOUS SELF-DIAGNOSTICS DE-ENERGIZE TO ACTUATE REDUNDANT FOR SAFETY	MANUAL FUNCTIONAL TEST NO DIAGNOSTICS ENERGIZE TO ACTUATE REDUNDANT FOR AVAILABILITY
POWER SOURCE	CLASS 1E	NON-CLASS 1E
HVAC	CLASS 1E	NON-CLASS 1E
LOCATION	SEPARATE ROOMS	DIFFERENT ROOM

DIVERSITY IN THE DIVERSE DISPLAY SYSTEM

SYSTEM	QUALIFIED DISPLAY PROCESSING SYSTEM	DIVERSE DISPLAY SYSTEM
INPUT SIGNAL CONDITIONING	WESTINGHOUSE I/O BOARDS	
INPUT SIGNAL CONVERSION	WESTINGHOUSE I/O BOARDS	
SIGNAL PROCESSING (SOFTWARE)	PLM/86 MACHINE LANGUAGE OPERATING SYSTEM	
SIGNAL PROCESSING (HARDWARE)	Intel SINGLE BOARD COMPUTERS '186, '286, '386 ... PROCESSORS	
INPUT SIGNAL CONVERSION	Intel A/D CONVERTER	
OUTPUT SIGNAL CONDITIONING	WESTINGHOUSE I/O BOARDS SOLID STATE RELAYS	
OPERATION	AUTOMATIC FUNCTIONAL TEST CONTINUOUS SELF-DIAGNOSTICS DE-ENERGIZE TO ACTUATE REDUNDANT FOR SAFETY	
POWER SOURCE	CLASS 1E	
HVAC	CLASS 1E	
LOCATION	SEPARATE ROOMS	



LEGEND



SWITCH



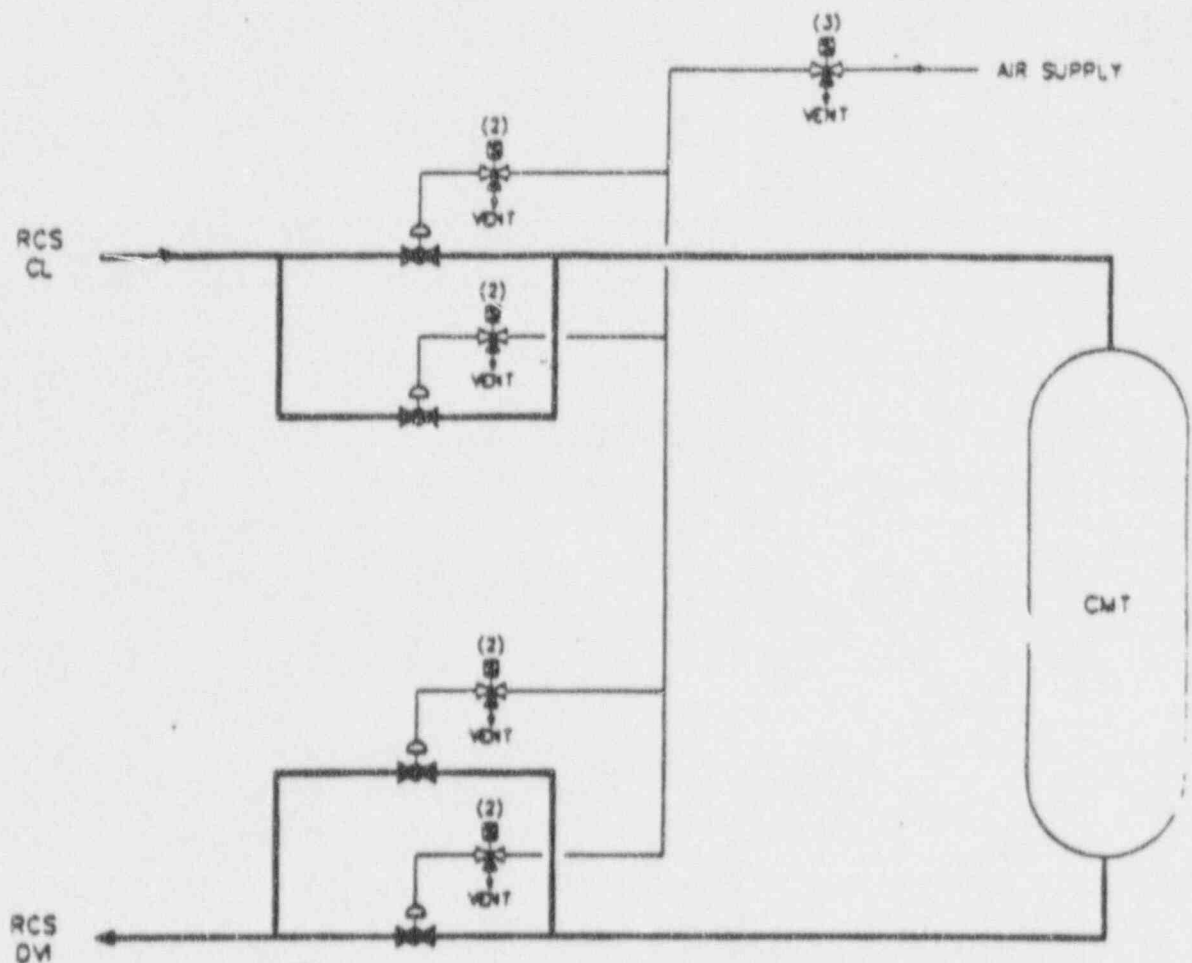
STATUS LAMP

(n) FUNCTION NUMBER

DIVERSE ACTUATION SYS

M MANUAL ACTUATION PANEL

Fig 2-1 Connection of DAS to Solenoid



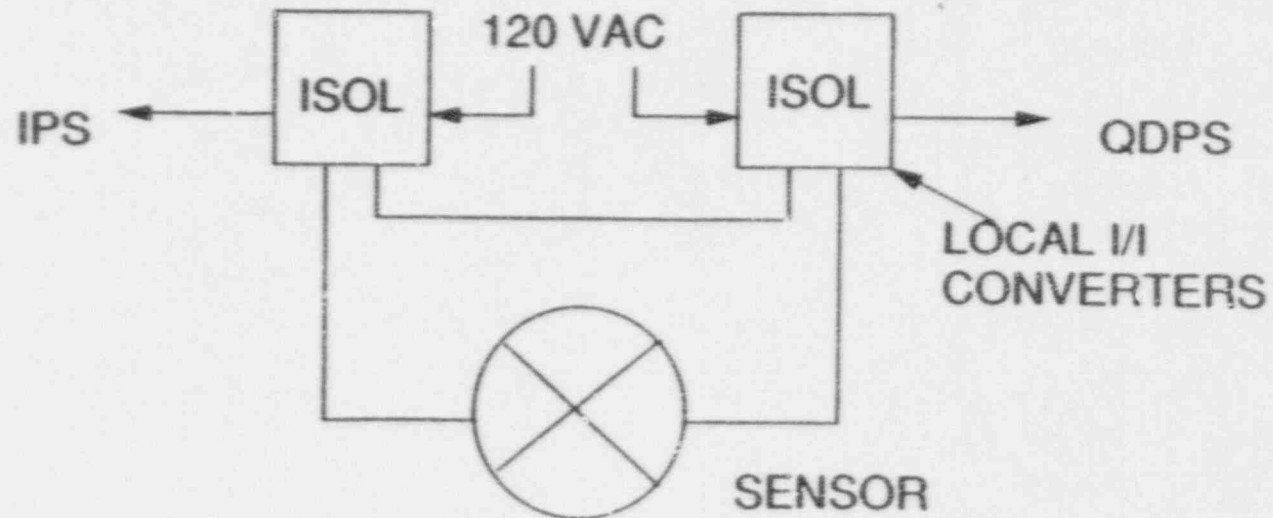
NOTES:

- (1) All valves shown in normal positions.
- (2) Safety grade solenoids are actuated by RPS. Loss of power to solenoids causes blocking of air supply and venting of operator causing main valve to open.
- (3) Non-safety solenoid actuated by DAS or hard wired manual switch. Solenoid fails in current position on loss of power to solenoid to reduce chance of inadvertent CMT actuations.

DIVERSE DISPLAY SYSTEM ISSUES

HOW TO SHARE SENSORS WITH IPS

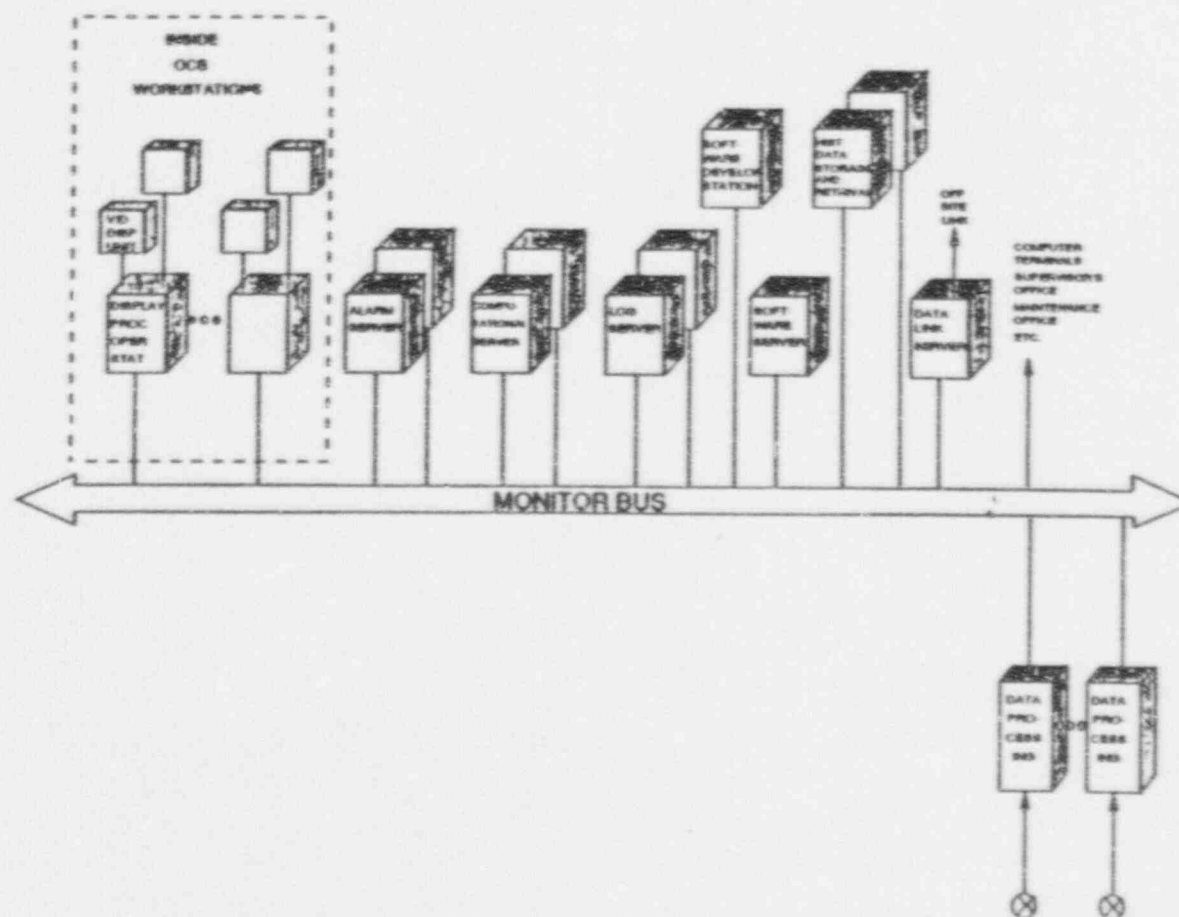
FAILURES IN EITHER SYSTEM MUST NOT PROPAGATE TO THE OTHER THROUGH THE SENSOR WIRING



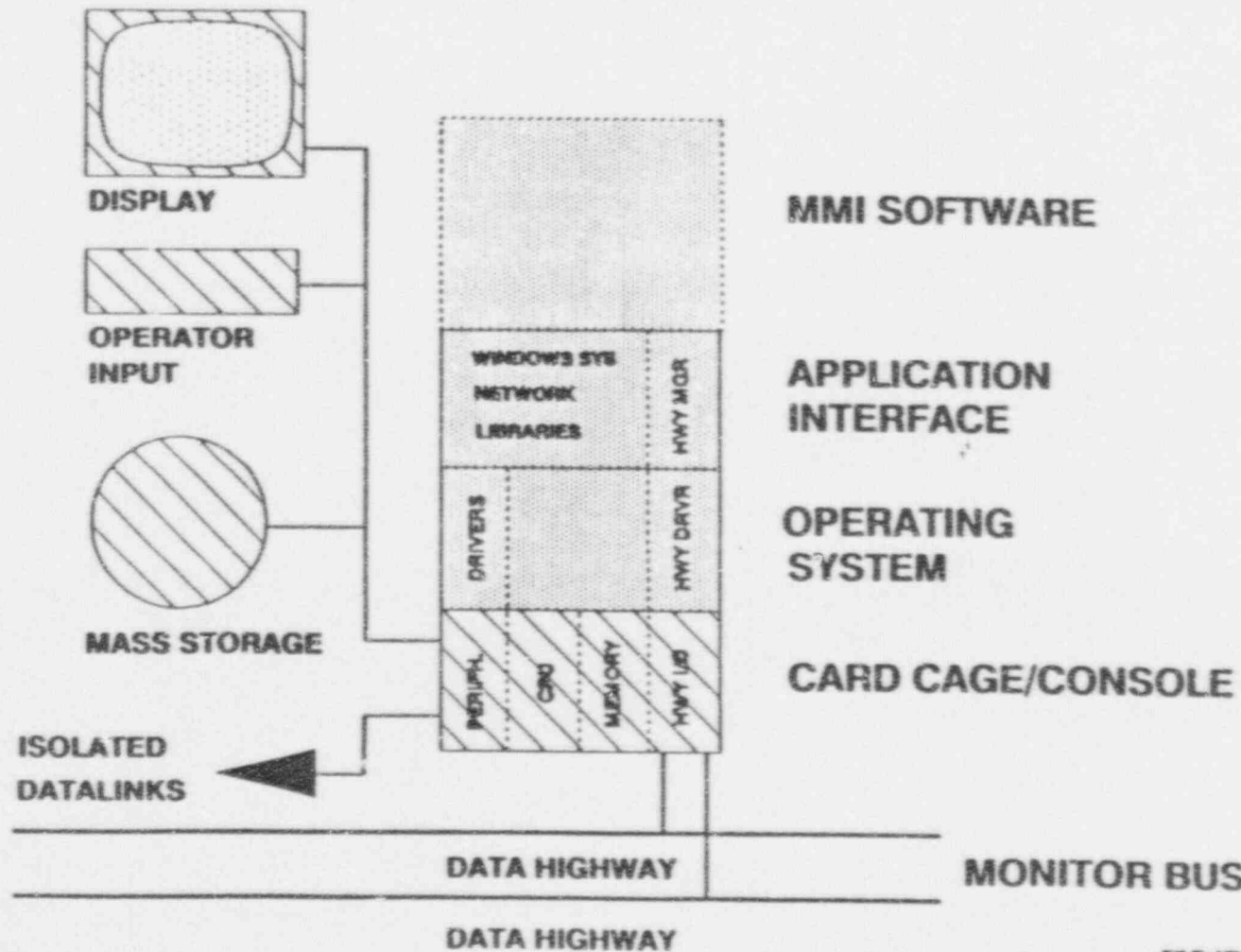
AP600

DATA DISPLAY AND PROCESSING SYSTEM

DATA DISPLAY AND PROCESSING SYSTEM ARCHITECTURE

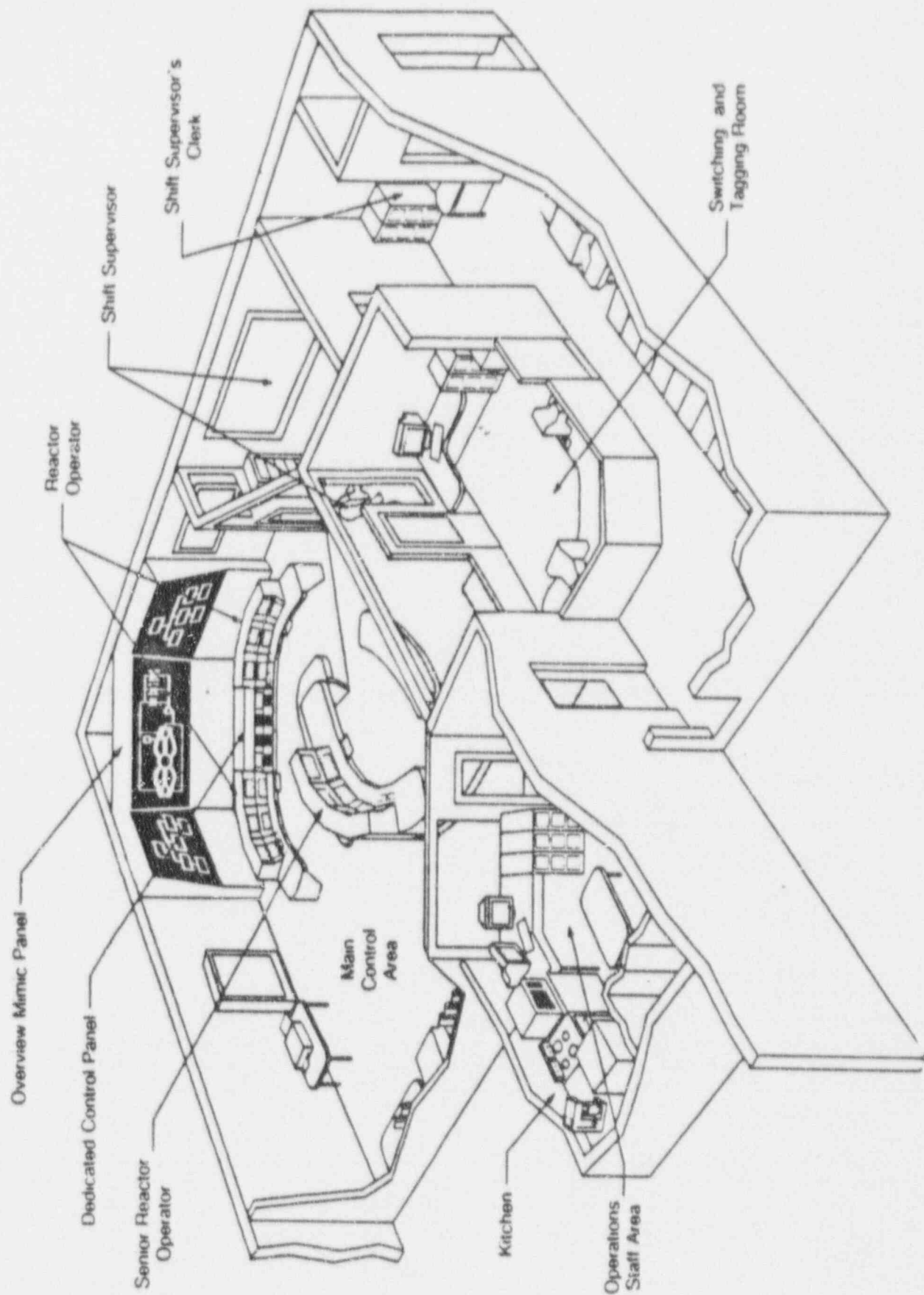


DISPLAY PROCESSOR ELEMENTS



AP600

OPERATIONS AND CONTROL CENTERS SYSTEM



OVERVIEW OF PLANT INFORMATION SYSTEM DISPLAYS

The following types of displays will be available to the operations staff in the main control room:

Accessible at the operator workstations:

- Plant Functional Displays representing a functional depiction of the process
- Plant Physical Displays representing a physical depiction of the process
- Computerized Procedures
- Alarm Support Displays which can show:
 - A plant-wide chronological list
 - A chronological list by function/category
 - An overflow display of messages of lower priority
 - A list of possible messages that may show in that category
 - A trigger logic display showing the logic that was used to generate the alarm
- Soft control panel displays depicting control devices

OVERVIEW OF PLANT INFORMATION SYSTEM DISPLAYS (cont'd)

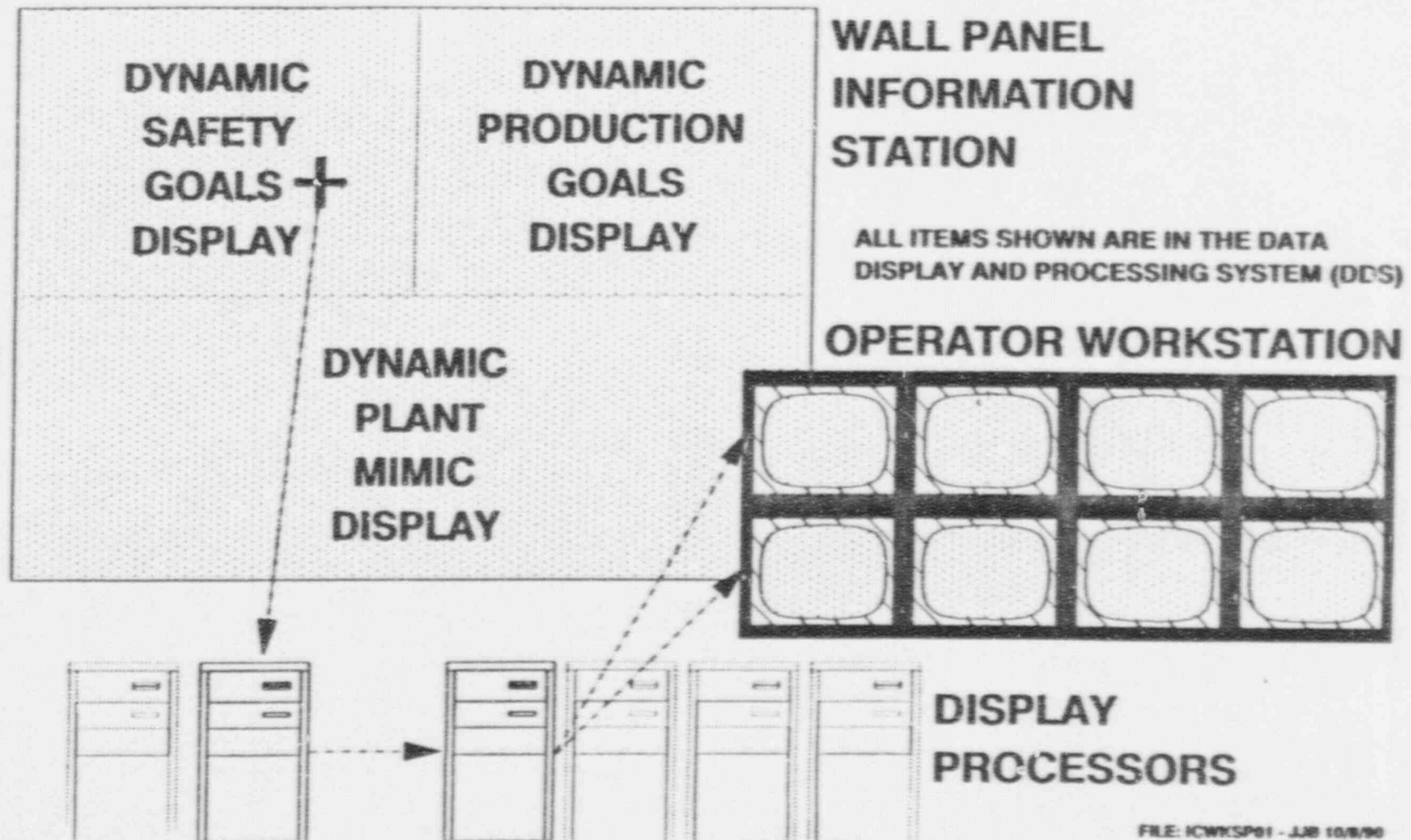
Also accessible in the main control room:

- QDPS displays for post-accident monitoring
- Wall Panel Information System displays for an overview of the plant state and alarm conditions

WALL PANEL INTERACTIONS



116



FILE: ICWYSP01 - JJB 10/8/90



- Alert Operators to Process Abnormalities, and Only Process Abnormalities (Black Board Design)
- Equally Capable of Handling Major Process Disturbances and Individual Minor Alarm Conditions
- Aid the Operator in Understanding the Severity and Consequences of Process Abnormalities
- Direct Operator to Location in Display System that Contains More Data Related to Eliminating, Diagnosing and Mitigating the Process Abnormality
- Distinguish Between Messages Which Convey Abnormalities vs. Equipment Status



- Alarm Overview Messages - Display Abnormality
- Alarm Support Messages - Provide Means for Operator To Query the Alarm System
- Auto Systems Actions Messages - Messages Telling the Operator What the Automatic Control Systems are Doing
- Emergency Safeguards Status Messages - Continuous Indication of the Binary State of the ESF



By Function:

- Alarms are Sorted by Function and Then by Process Units Within Function
- Each of These Alarm Categories Corresponds to a Static Label on the Overview Displays
- Static Labels are Arranged to Reflect the Functional Structure of the Plant

Local Prioritization:

- Prioritization Within Alarm Category, Not Over Entire Alarm System
- Identification of Most Important Alarm is Dependent on Overall Plant State

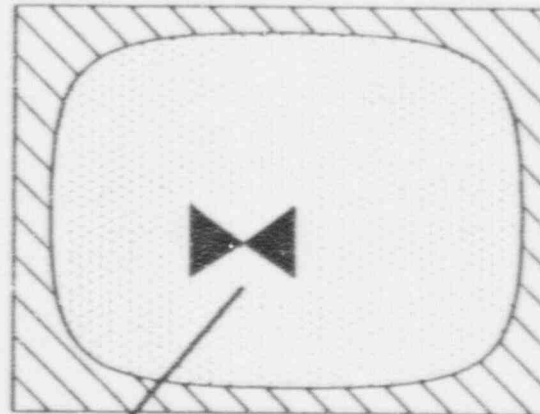
CRITERIA FOR ALLOCATING MANUAL OR AUTOMATIC CONTROL

- The time in which a response is required
- The number of tasks the operator might be expected to perform at the same time
- The consequences of a wrong action, or one made too hastily
- The level of difficulty of making a control automatic and its associated cost

SOFT CONTROL INTERACTIONS

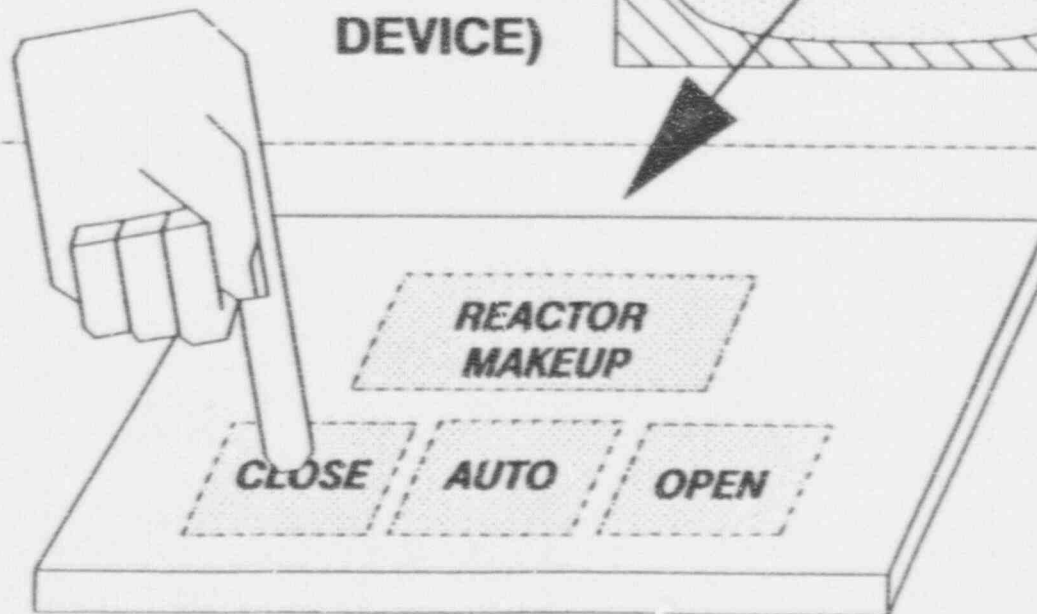
117

**GRAPHICS
WORKSTATION
DISPLAY
(OPERATOR
SELECTS
DEVICE)**



DDS

PMS or PLS



**SOFT
CONTROLS
(PROVIDE
OPERATOR
INTERFACE)**

FILE: ICWKSP04 JJB 10/8/90

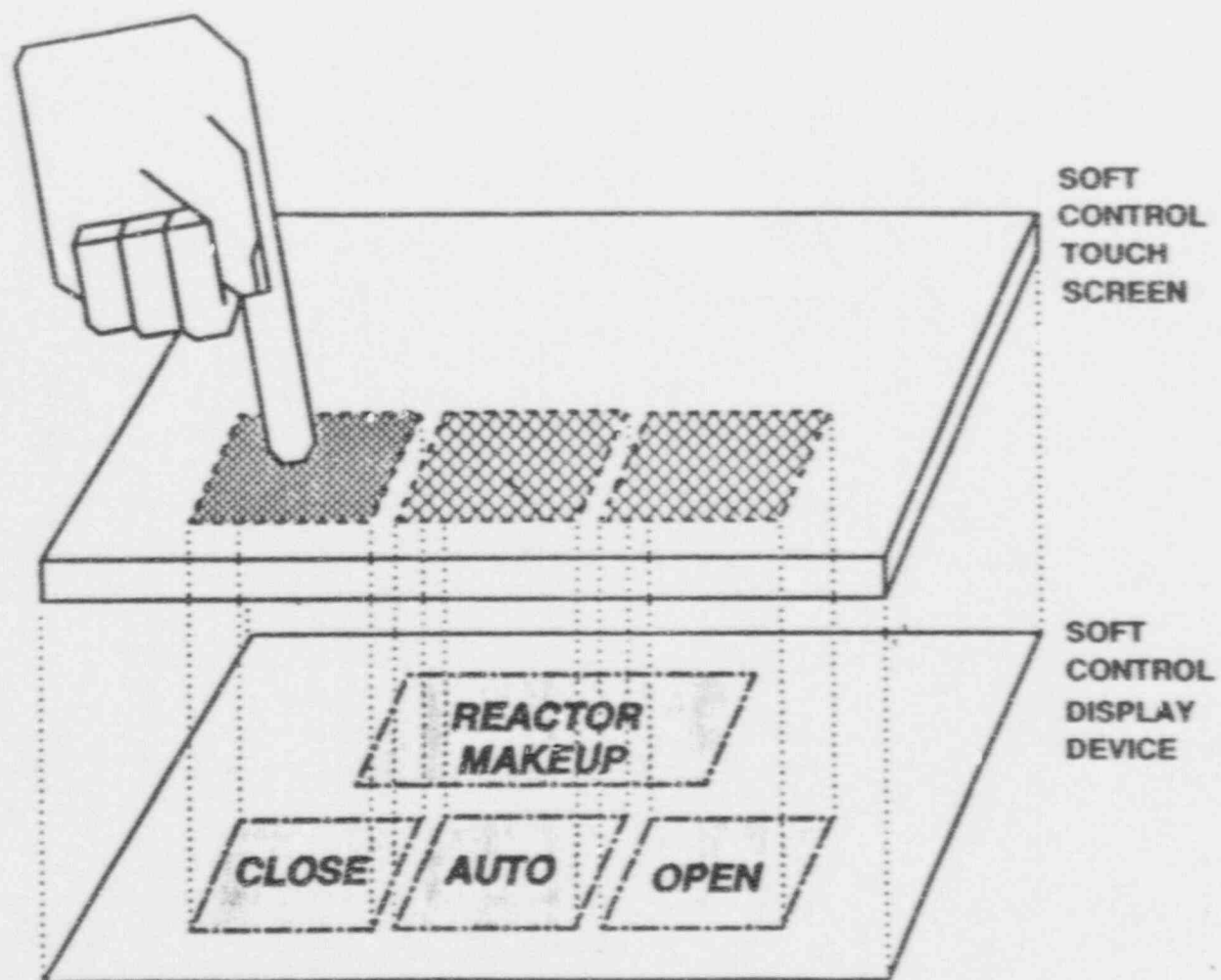
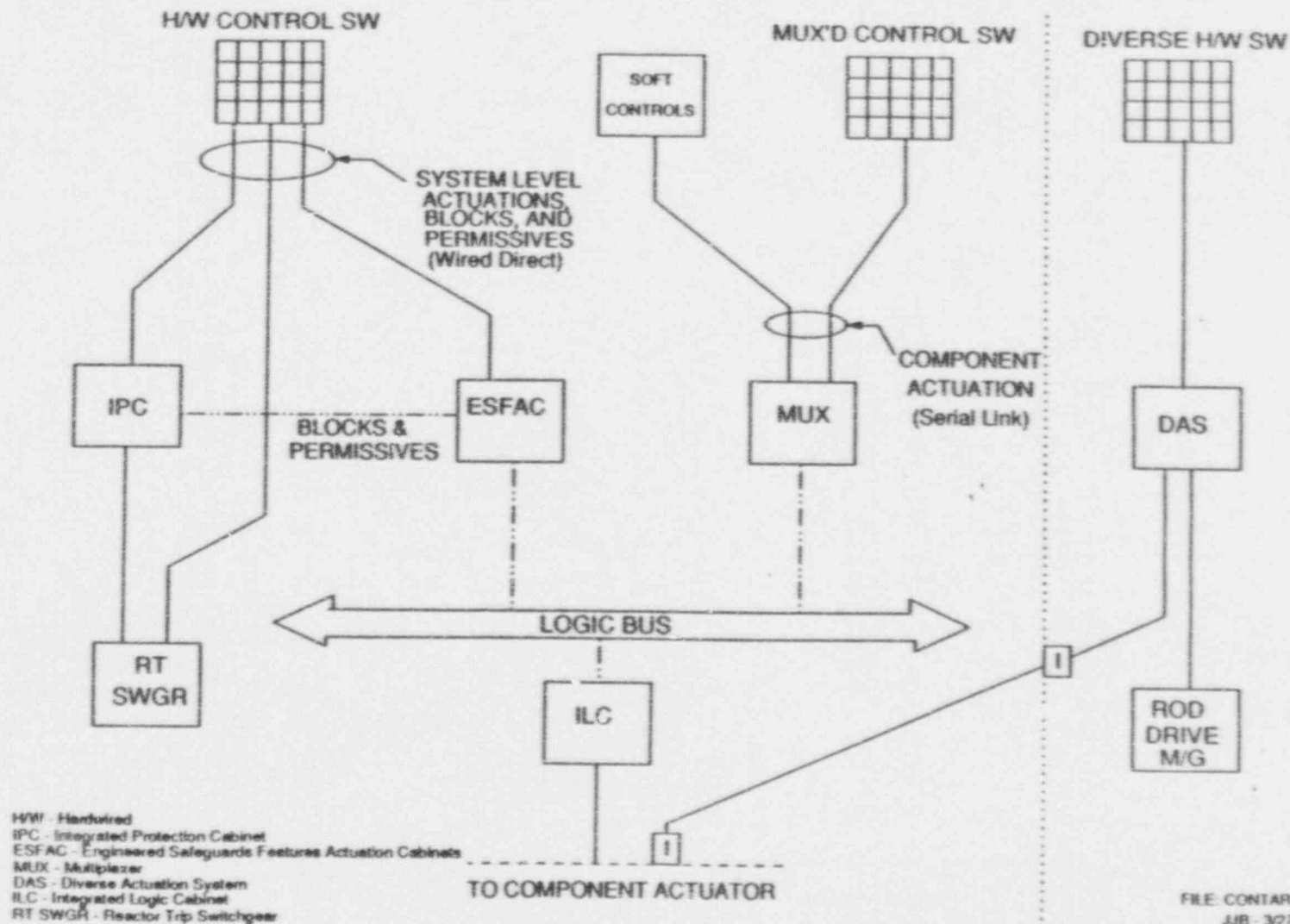


Figure 4.5-3 SOFT CONTROL STATION ARCHITECTURE

AP600 CONTROL SWITCH INTERFACE ARCHITECTURE



ONE DIVISION SHOWN

DESIGN, VERIFICATION, AND VALIDATION PROGRAM

Purposes of the Design, Verification, and Validation Process

To insure that System Functional Requirements are properly and correctly implemented in the Instrumentation and Control Architecture.

To aid in the development of high quality hardware, software, and systems designs.

To help ensure that the Instrumentation and Control Architecture conforms to customer, regulatory, and Westinghouse requirements

Direct the necessary activities in the design, implementation, verification, and validation of Instrumentation and Control Systems

Essential Features of the Design, Verification, and Validation Process

Verification Process Integrated with Design Process

Modular Design of Hardware and Software

Incremental Verification

Testing performed over intended (design) range of use.

Design, Verification, and Validation Process Implementation

Define Documentation Requirements

Define Standards for Content and Format of Each Document

Define Interactions Between the Development Activities and Verification and Validation Activities

Ensure that Documents generated are Correct, Complete, and Without Ambiguity

Design for Verification

"All module and assembly design work is done in such a fashion that the result be immediately verifiable to an independent party."

AP600

**PROTECTION AND SAFETY
MONITORING SYSTEM**

**TIER I DESIGN DESCRIPTION
ITAAC**

WESTINGHOUSE AP600

I&C PRA

Shelagh Morandini

PRA

October 6, 1992

- **PRA Goals:** To assess risk to the public through the use of a probabilistic risk assessment
- **Core Damage Frequency was Quantified for many Events:**

Initiating Event	Core Damage Frequency (per year)	Percentage of Total
Transients (except LOOP):		
- Turbine or Reactor Trip	4.3E-8	12.9
- Others	2.9E-8	8.6
LOOP	2.9E-9	0.9
Small LOCA	2.3E-8	6.9
Very Small LOCA	1.2E-8	3.6
PRHR Tube Rupture	4.2E-8	12.6

Initiating Event	Core Damage Frequency (per year)	Percentage of Total
Medium LOCA	1.2E-8	3.6
Safety Injection Line Break	7.3E-8	21.9
CMT Line Break	2.7E-9	0.8
Large LOCA	1.6E-8	4.8
SG Tube Rupture	2.6E-9	0.8
ATWS (loss of feedwater w/o scram)	4.5E-8	13.6
Vessel Rupture	3.0E-8	9.0
Total	3.3E-7	100.0

- **I&C PRA is not a standalone model, but is instead integrated with the rest of the PRA model**
- **PRA modeled all signals required for safety functions, from automatic recognition of the need for a safety function to function actuation**

- **I&C systems were modeled as a part of all these accident sequences**
 - **Input Signal Failure (Analog inputs, Contact inputs, Nuclear Instrumentation)**
 - **Random Failures of Protection and Control System Hardware**
 - **Test and Maintenance**
 - **Common Cause Failures (Hardware and Software)**
 - **Support System Failure (AC and DC Power, Equipment Cooling)**

- **Common Cause:**
- **Multiple Greek Letter (MGL) method was selected to assess potential common cause failures**
- **Possible common cause failure mechanisms were identified (hardware and software)**
- **System performance of non-nuclear digital I&C systems was assessed. MGL factors were estimated based on engineering judgement.**
- **Preliminary studies showed I&C common cause failures to be a dominant risk contributor**

- Westinghouse performed sensitivity studies and determined diversity would improve results
- NRC SECL 90-016 also addressed this issue
- Diversity was modeled in the final PRA
- DAS and DIS were assigned failure probabilities, which the design group will use as a reliability goal
- With DAS and DIS, I&C common cause failures are no longer dominant contributors to core damage.

PROTECTION AND SAFETY MONITORING SYSTEM

Revision: 0

Effective: 09/04/92



X.X PROTECTION AND SAFETY MONITORING SYSTEM

Design Description

The Protection and Safety Monitoring System (PMS) for the AP600 provides the following safety-related functions:

- Tripping the reactor by opening the reactor trip breakers.
- Actuation of the engineered safety features equipment.
- Safety-related plant parameter monitoring prior to, during, and after an accident or plant transient.

For this design description, the PMS consists of the sensors, detectors, signal conditioning, data acquisition, data processors, datalinks and data highways, operator interfaces, displays, and other equipment necessary for the execution of the functions of the system. The PMS for the AP600 implements its functions by software logic installed in programmable digital devices (data processors). Plant data and other signals are exchanged between data processors by means of isolated datalinks and data highways.

The necessary sensors and logic for generating the reactor trips, engineered safety features actuations, and safety-related plant parameter monitoring are discussed within this design description. PMS components and equipment are electrically isolated from nonsafety-related plant instrumentation and electrical equipment. Signals from the PMS to other plant instrumentation and control systems, such as the plant control system and the data display and processing system, are transmitted through isolation devices. Certain sensor signals originating in the PMS are shared with the diverse actuation system through isolation devices.

The PMS is a four division system which automatically or manually initiates a reactor trip or engineered safety features actuation coincident with a

single failure in the PMS. Additionally, the PMS protects against unnecessary reactor trips or engineered safety features actuations resulting from single failures in the PMS. Loss of power or input signals, or disconnection of portions of the system results in a trip or actuation initiating state.

Reactor Trip Function

The reactor trip function of the PMS is implemented by plant sensors, the reactor trip processors, and the reactor trip switchgear. The reactor is tripped by opening the circuit breakers in the reactor trip switchgear, thereby removing electrical power to the control rod drive mechanisms, causing the control rods to drop into the reactor core due to gravity. The reactor trip breakers are arranged so that tripping any two out of four divisions results in interruption of power to the control rod drive mechanisms. Tripping any single division will not interrupt power to the control rod drive mechanisms. Once a reactor trip has been initiated, the reactor trip breakers in the reactor trip switchgear latch open, and must be manually reset before the control rods can be withdrawn.

The reactor trip function utilizes the four independent PMS divisions, using 2-out-of-4 logic for automatic trips based on plant sensor inputs. The manual reactor trip function uses 1-out-of-2 logic.

The sensors monitor plant conditions and send signals to the reactor trip processors where these signals are compared to setpoints. When two or more unbypassed signals monitoring the same plant parameter in different divisions exceed the setpoint, and permissive or interlock logic is satisfied, a reactor trip is initiated. Plant parameters that are monitored to produce a reactor trip include:

- Neutron flux



Westinghouse



PROTECTION AND SAFETY MONITORING SYSTEM

Revision: 0

Effective: 09/04/92

- Reactor coolant pump speed
- Reactor coolant flow
- Overtemperature ΔT
- Overpower ΔT
- Pressurizer level
- Pressurizer pressure
- Steam generator level
- Reactor trip on safeguards actuation.

A manual reactor trip and a reactor trip on manual safeguards actuation are implemented by directly opening the reactor trip switchgear.

Engineered Safety Features Functions

The engineered safety features functions of the PMS are implemented by plant sensors, the engineered safety features processors, the engineered safety features actuation processors, the protection logic, the logic buses, and manual actuation devices. The protection logic provides actuating signals to operate the plant components. Several engineered safety features sensors are shared with the reactor trip function.

The engineered safety features functions utilize the four independent PMS divisions, using 2-out-of-4 logic for automatic actuations based on sensor inputs. An exception is the startup feedwater signal, which utilizes two divisions and 1-out-of-2 logic. Manual, systems level actuations are provided for individual functions.

The sensors monitor plant conditions and send signals to the engineered safety features processors, where these signals are compared to setpoints. When two or more unbypassed signals monitoring the same plant parameter in different divisions exceed the setpoint, and permissive or interlock logic is satisfied, a system level actuation signal is produced in the engineered safety features actuation processors. This system level signal is transmitted to the associated protection logic in the same division by the logic bus data highway. The protection logic then provides actuation signals to the component if the component interlock logic is satisfied. Plant parameters that are

monitored to produce engineered safety features functions include:

- Neutron flux
- Pressurizer pressure
- Pressurizer level
- Steam generator level
- Steam line pressure
- Cold leg temperature
- Startup feedwater flow
- Containment pressure
- Core makeup tank level.

The engineered safety features actuation signals include:

- Safeguards actuation
- Passive residual heat removal
- Core makeup tank injection
- Reactor coolant pump trip
- Containment cooling
- Containment isolation
- Main feedwater line isolation
- Steam line isolation
- Reactor coolant system depressurization
- Startup feedwater isolation
- Chemical volume control system isolation.
- Turbine trip
- Steam generator blowdown system isolation
- Block of boron dilution
- Block steam dump
- Letdown line isolation
- Containment sump pH control
- Normal residual heat removal system isolation

Safety-Related Plant Parameter Monitoring Function

The safety-related plant parameter monitoring function is implemented by plant sensors, communications processors or data acquisition processors, qualified display processors, and qualified operator displays. Plant sensors may be shared with the



PROTECTION AND SAFETY MONITORING SYSTEM

Revision: 0

Effective: 09/04/92



reactor trip and engineered safety features functions. For plant sensors shared with either of these functions, data acquisition takes place at the communications processors, for sensors which are not shared, data acquisition is performed by the qualified display data acquisition processors. The plant data is then transmitted to the qualified display processors, where it is prepared for display on the qualified operator displays.

The safety-related plant parameter monitoring function utilizes two of the four independent PMS divisions. A minimum of two operator display devices, one per division, are provided at each location. Operator display devices are provided in the main control room and at the remote shutdown workstation.

The sensors monitor plant conditions and send signals to either the communications processors, or the qualified display data acquisition processors. This data is transmitted to the qualified display processors, where it is collected, organized, and prepared for display. The final data is displayed on the qualified operator displays. The plant parameters that are collected and displayed by the safety-related plant parameter monitoring function include:

- Reactor coolant system pressure
- Reactor coolant system temperature
- Pressurizer level
- Neutron flux
- Containment water level
- Core exit temperature
- Passive residual heat removal heat exchanger outlet temperature
- Passive residual heat removal flow
- Incontainment refueling water storage tank water level
- Passive containment cooling flow
- Passive containment cooling storage tank level
- Containment pressure
- Containment radiation
- Containment hydrogen concentration
- Pressurizer safety valve status
- Automatic depressurization system first stage valve status
- Automatic depressurization system second stage valve status
- Automatic depressurization system third stage valve status
- Automatic depressurization system fourth stage valve status.



Westinghouse

PROTECTION AND SAFETY MONITORING SYSTEM

Revision: 0

Effective: 09/04/92



Table PMS-1 - Protection and Safety Monitoring System
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analysis	Acceptance Criteria
1. The protection and safety monitoring system performs the safety-related reactor trip, engineered safety features actuation, and plant parameter monitoring functions.	1(a). System functional tests shall be conducted to verify that reactor trip breakers open when system logic has been satisfied.	1(a). Reactor trip breakers open when trip logic is satisfied from the following plant parameters: <ul style="list-style-type: none"> • Neutron flux • Reactor coolant pump speed • Reactor coolant flow • Overtemperature ΔT • Overpower ΔT • Pressurizer level • Pressurizer pressure • Steam generator level
1. (continued)	1(b). System functional tests shall be conducted to verify that engineered safety features actuation signals are initiated when system logic has been satisfied.	1(b). Component actuation signals are generated when engineered safety features actuation logic is satisfied from the following plant parameters: <ul style="list-style-type: none"> • Neutron flux • Pressurizer pressure • Pressurizer level • Steam generator level • Steam line pressure • Cold leg temperature • Startup feedwater flow • Containment pressure • Core makeup tank level

PROTECTION AND SAFETY MONITORING SYSTEM

Revision: 0

Effective: 09/04/92



**Table PMS-1 - Protection and Safety Monitoring System
Inspections, Tests, Analyses and Acceptance Criteria**

Certified Design Commitment	Inspections, Tests, Analysis	Acceptance Criteria
1. (continued)	1(c). An inspection shall be performed to verify that the designated plant parameters are displayed.	<p>1(c). The Protection and Safety Monitoring System displays the following plant parameters in the main control room and at the remote shutdown workstation:</p> <ul style="list-style-type: none"> • Reactor coolant system pressure • Reactor coolant system temperature • Pressurizer level • Neutron flux • Containment water level • Core exit temperature • Passive residual heat removal system heat exchanger outlet temperature • Passive residual heat removal flow • Incontainment refueling water storage tank water level • Passive containment cooling flow • Passive containment cooling storage tank level • Containment pressure • Containment radiation • Containment hydrogen concentration • Pressurizer safety valve status • ADS system first stage valve status • ADS second stage valve status • ADS third stage valve status • ADS fourth stage valve status

PROTECTION AND SAFETY MONITORING SYSTEM

Revision: 0

Effective: 09/04/92



Table PMS-1 - Protection and Safety Monitoring System
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analysis	Acceptance Criteria
I. (continued)	I(d). System functional tests shall be conducted to verify that operational permissives and interlocks are generated and removed when system logic has been satisfied.	I(d). Operational permissives and interlocks are generated and removed when reactor trip and engineered safety features actuation logic is satisfied from the following plant parameters: <ul style="list-style-type: none">• Neutron flux• Pressurizer pressure

PROTECTION AND SAFETY MONITORING SYSTEM

Revision: 0

Effective: 09/04/92



**Table PMS-1 - Protection and Safety Monitoring System
Inspections, Tests, Analyses and Acceptance Criteria**

Certified Design Commitment	Inspections, Tests, Analysis	Acceptance Criteria
2. The Protection and Safety Monitoring System design provides timely initiation of safety-related reactor trip and engineered safety features actuations.	<p>2(a). Tests shall be conducted to measure the response times to initiate reactor trip when trip setpoints have been exceeded.</p> <p>Time response is defined as the maximum allowable time for the reactor trip breakers to open following a step change by a simulated sensor from 5% below the setpoint to 5% above the setpoint with each externally adjustable time delay set to OFF.</p>	<p>2(a). The time to satisfy trip logic, the trip signal to reach the reactor trip breakers, and the reactor trip breakers to open is less than or equal to the time response requirement listed for the following channels:</p> <ul style="list-style-type: none"> • Power range neutron flux \leq [TBD sec] • Reactor coolant pump speed \leq [TBD sec] • Reactor coolant flow \leq [TBD sec] • Overtemperature $\Delta T \leq$ [TBD sec] • Overpressure $\Delta T \leq$ [TBD sec] • Pressurizer level \leq [TBD sec] • Pressurizer pressure \leq [TBD sec] • Steam generator narrow range level \leq [TBD sec]

PROTECTION AND SAFETY MONITORING SYSTEM

Revision: 0

Effective: 09/04/92



Table PMS-1 - Protection and Safety Monitoring System
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analysis	Acceptance Criteria
2. (continued)	<p>2(b). Tests shall be conducted to measure the response times to initiate engineered safety features actuation signals when trip setpoints have been exceeded.</p> <p>Time response is defined as the maximum allowable time for component actuation signals to be produced following a step change by a simulated sensor from 5% below the setpoint to 5% above the setpoint with each externally adjustable time delay set to OFF. Time response shall not include the engineered safety features components.</p>	<p>2(b). The time to satisfy engineered safety features actuation logic and the component actuation signal to be produced is less than or equal to the time response requirement listed for the following channels:</p> <ul style="list-style-type: none"> • Source range neutron flux (rate) \leq [TBD sec] • Pressurizer pressure \leq [TBD sec] • Pressurizer level \leq [TBD sec] • Steam generator narrow range level \leq [TBD sec] • Steam generator wide range level \leq [TBD sec] • Steam line pressure \leq [TBD sec] • Cold leg temperature \leq [TBD sec] • Startup feedwater flow \leq [TBD sec] • Containment pressure \leq [TBD sec] • Core makeup tank level \leq [TBD sec]

PROTECTION AND SAFETY MONITORING SYSTEM

Revision: 0

Effective: 09/04/92



**Table PMS-1 - Protection and Safety Monitoring System
Inspections, Tests, Analyses and Acceptance Criteria**

Certified Design Commitment	Inspections, Tests, Analysis	Acceptance Criteria
3(a). The Protection and Safety Monitoring System provides a manual reactor trip capability.	3(a). The manual reactor trip switches shall be tested.	3(a). The reactor trip breakers open when the manual reactor trip switches are operated.
3(b). The Protection and Safety Monitoring System initiates a reactor trip coincident with manual safeguards actuation.	3(b). The manual safeguards actuation switches shall be tested.	3(b). The reactor trip breakers open when the manual safeguards actuation switches are operated.
3(c). The Protection and Safety Monitoring System provides manual engineered safety features actuation capability.	<p>3(c). The following manual engineered safety features actuation switches shall be tested:</p> <ul style="list-style-type: none"> • Manual safeguards actuation • Manual passive residual heat removal actuation • Manual steam line isolation • Manual steam/feedwater isolation • Manual feedwater isolation • Manual containment cooling actuation • Manual containment isolation actuation • Manual depressurization system actuation 	3(c). Component actuation signals are generated in accordance with engineered safety features actuation logic when manual engineered safety features actuation switches are operated.

PROTECTION AND SAFETY MONITORING SYSTEM

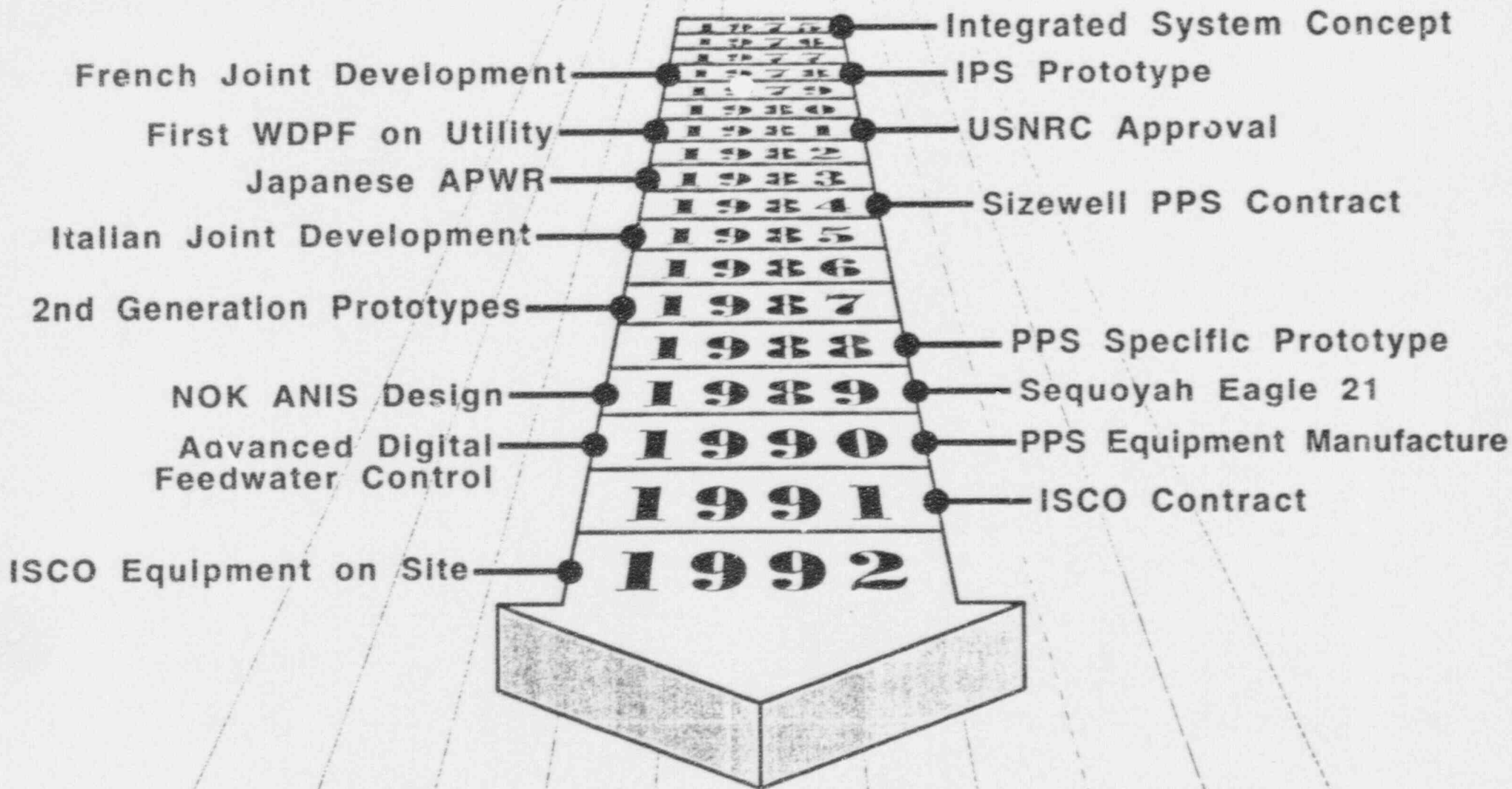
Revision: 0

Effective: 09/04/92



Table PMS-1 - Protection and Safety Monitoring System
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analysis	Acceptance Criteria
4. The four redundant divisions of Protection and Safety Monitoring System equipment are independent from each other except for isolated data communications required for voting logic. The four redundant divisions of Protection and Safety Monitoring System equipment are powered from independent power sources.	4. One Protection and Safety Monitoring System division shall be selected and deenergized. The tests of ITAACs 1(a), 1(b), 1(c), and 1(d) shall be repeated.	4. The acceptance criteria is the same as the acceptance criteria for ITAACs 1(a), 1(b), 1(c), and 1(d) except for the division that is deenergized.



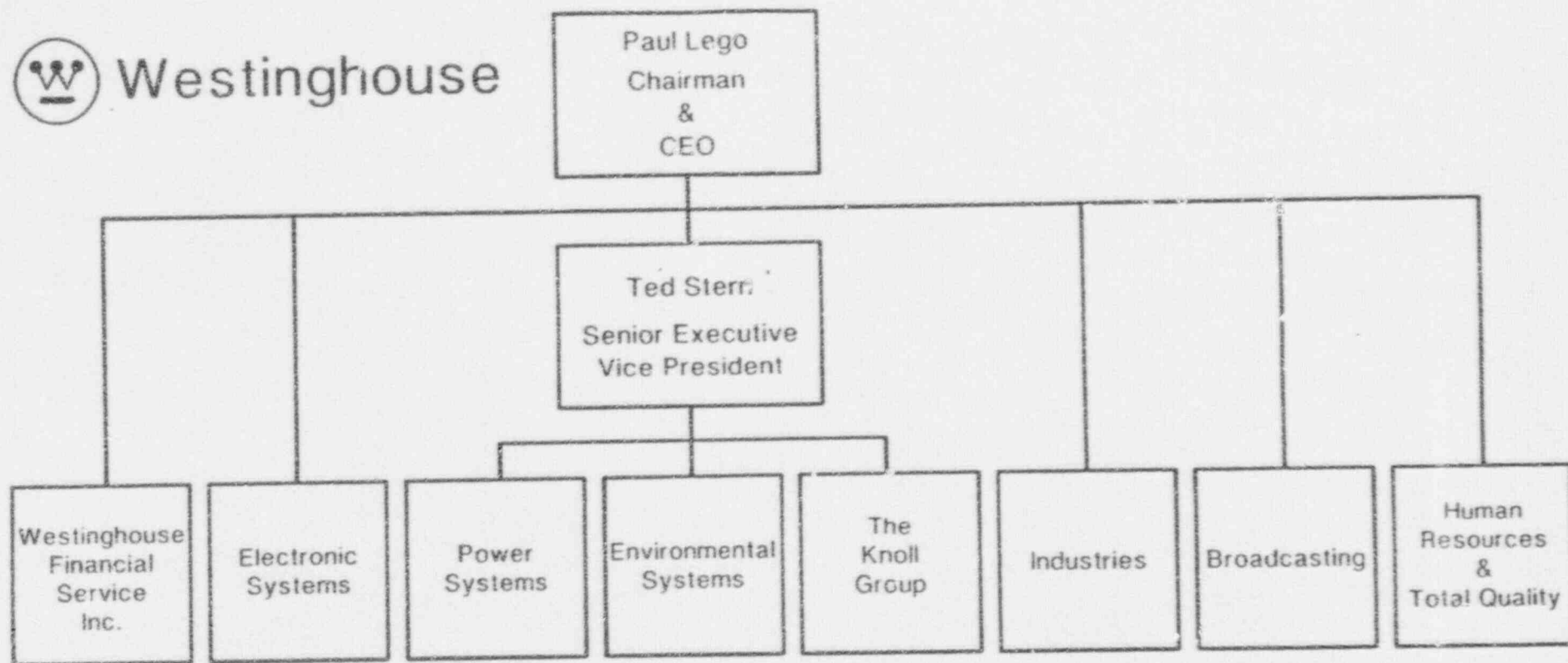
Sizewell ISCO

Process Control Division

Overview



Westinghouse



Westinghouse Electric Corporation

Founded 1886

Employees 110,000

Headquarters Pittsburgh, PA

Locations 619 U.S.

200 International



Westinghouse

Energy Systems
Business Unit

Power Systems

John Yasinsky
Executive
Vice President

Energy Systems
Business Unit

Nat Woodson
Vice President &
General Manager

Power Generation
Business Unit

Frank Bakos
Vice President &
General Manager

Process Control
Division

Nuclear Services
Division

Commercial
Nuclear Fuel
Division

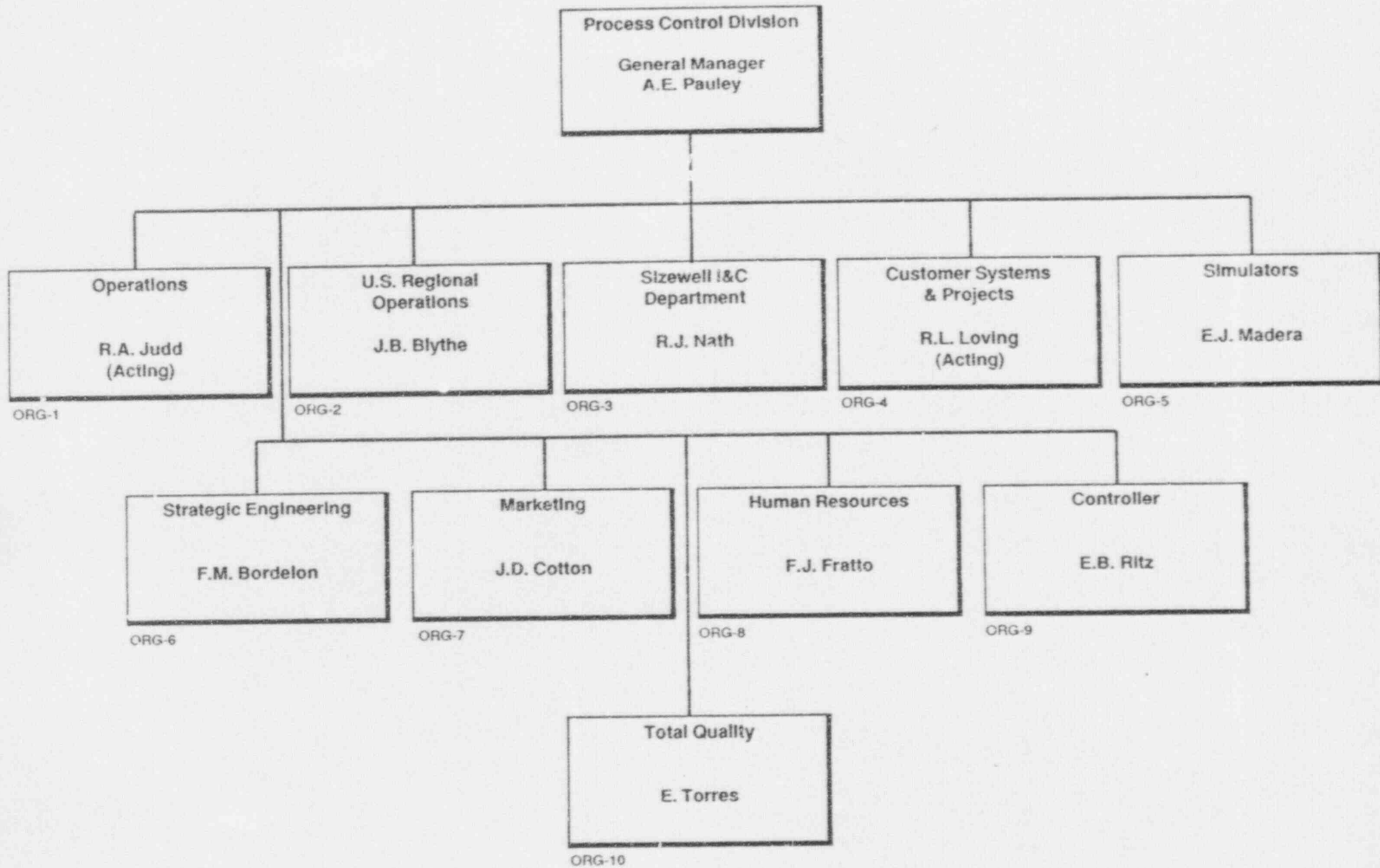
Nuclear & Advanced
Technology Division

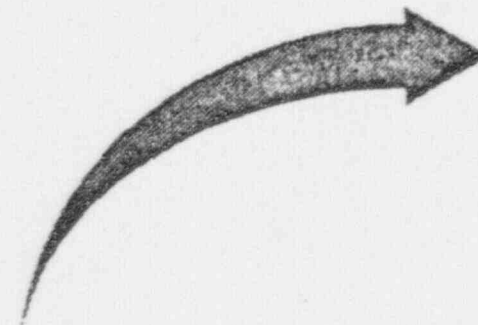
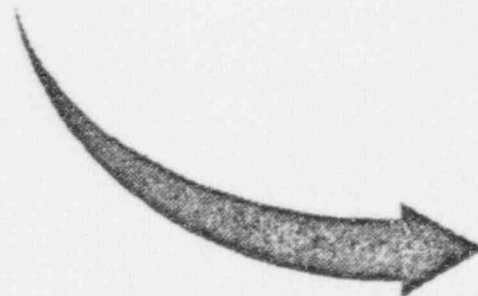
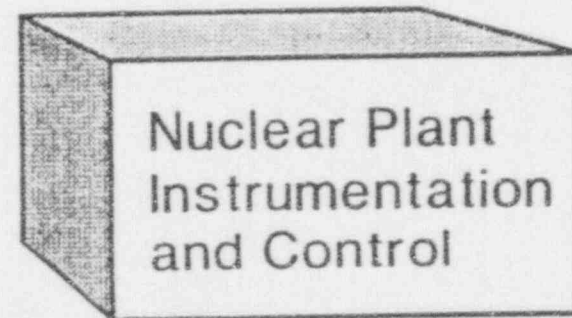
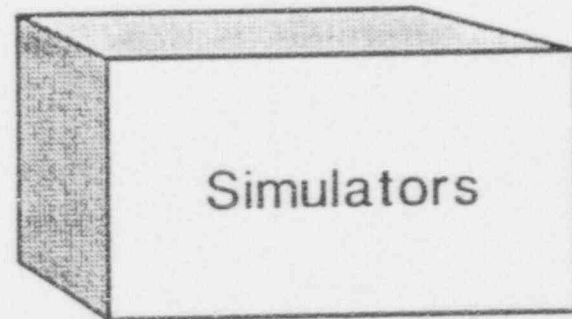
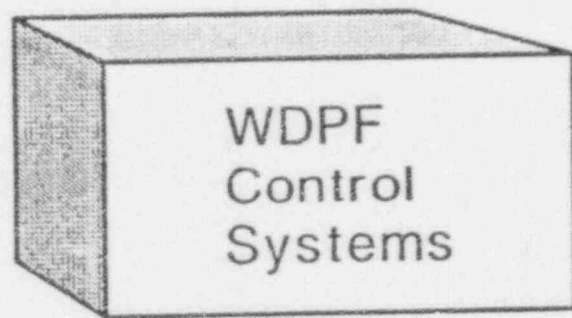
Electro-Mechanical
Division

Process Control Division

October 1, 1992

ORG-0

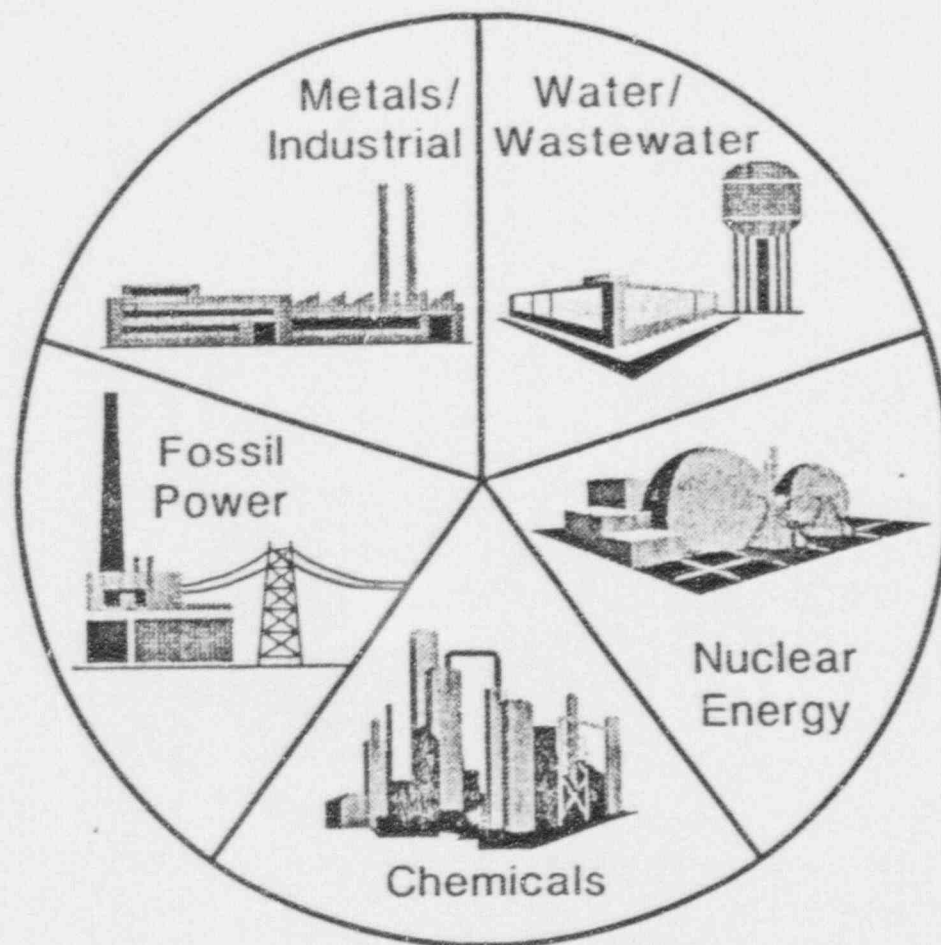




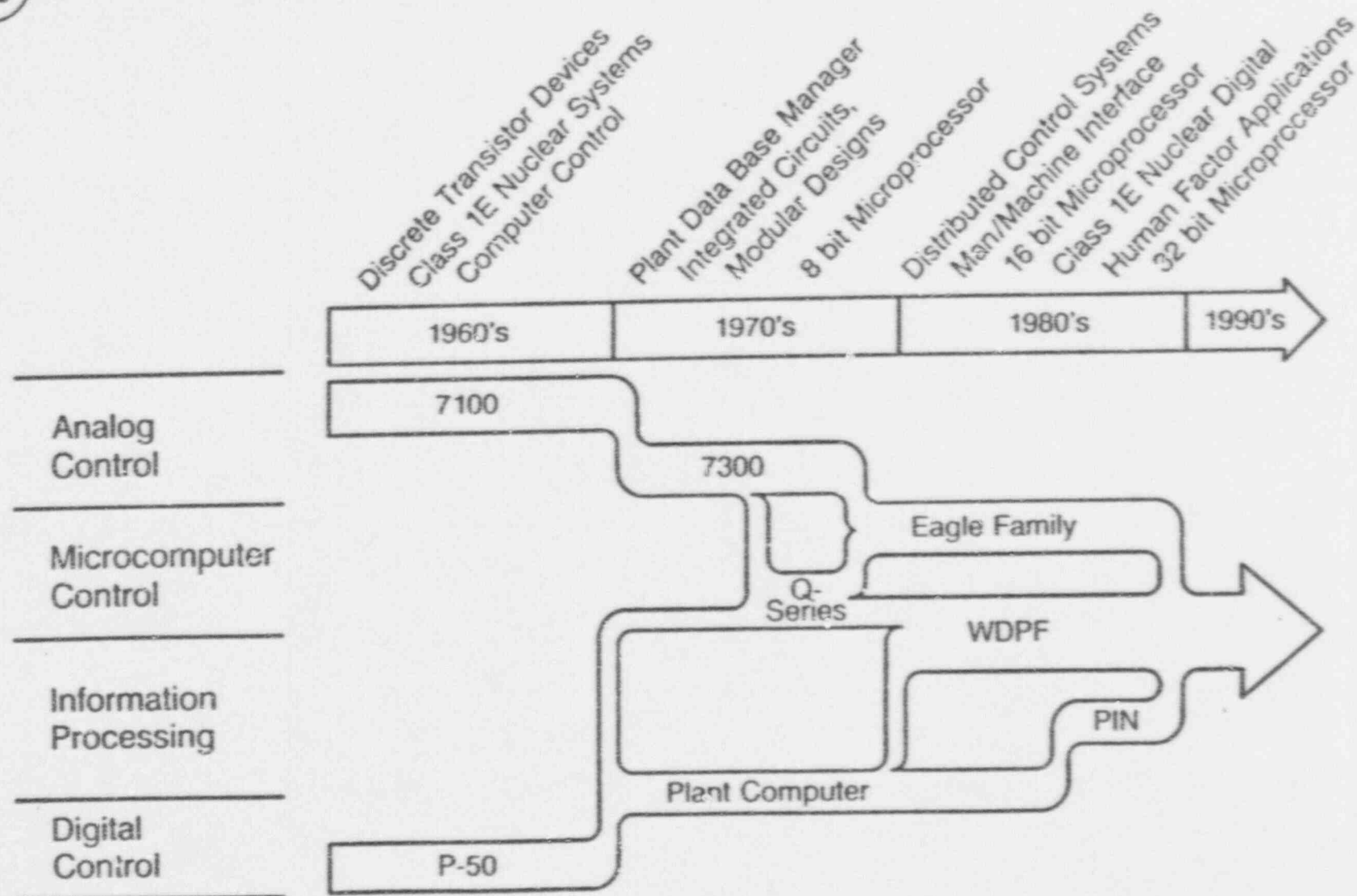
- 1400 Employees
- 12 Major Facilities

Westinghouse

Process Control Division



Instrumentation & Computer Product Evolution



PCD Products

- WDPF - Distributed Processing Family
- Eagle 21 Protection System
- Eagle DPF Control System
- Plant Process Computers
- Plant Information Systems
- Nuclear Instrumentation System
- Flux Mapping System
- Reactor Vessel Level Instrumentation
- Rod Position Indication
- Sensor Highway
- Diagnostic Equipment

Process Control Division Installations

	<u>Nuclear</u>	<u>Industrial</u>	<u>Total</u>
Miscellaneous Process Control	26	100	126
7100 Process Control	16	44	60
7300 Process Control	41	167	208
WDPF Process Control	7	602	609
Plant Process Computers	48	108	156
Turbine Control Computers	29	255	284
Emergency Response Facilities	17	-	17
Reactor Protection & Control Systems	90	-	90
Eagle RVLIS Systems	26	-	26
Eagle QDPS/PSMS Systems	5	-	5
Eagle-21 Upgrade Protection Sets	9	-	9
Integrated Protection Systems	1	-	1
Rod Control Systems	118	-	118
Nuclear Instrumentation	118	-	118
Rod Position Indication Systems	118	-	118
Digital Flux Mapping Systems	10	-	10

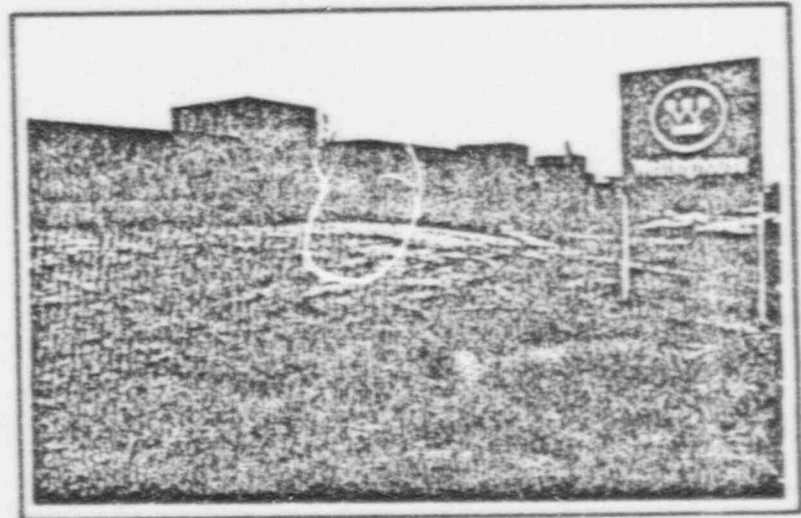
Recent Westinghouse Nuclear Digital I&C Experience

Instrumentation and Control

Sequoyah Units 1 & 2	-	Eagle 21 Protection System
Watts Bar Unit 1	-	Eagle 21 Protection System
Turkey Point 3 & 4	-	Eagle 21 Protection System RTD Bypass Elimination
Zion 1 & 2	-	Eagle 21 Protection System
Diablo Canyon 1 & 2	-	Eagle 21 Protection System WDPF Advanced Digital Feedwater Control System
Prairie Island 1 & 2	-	WDPF Advanced Digital Feedwater Control System
Ginna	-	WDPF Advanced Digital Feedwater Control System
Catawba 1 & 2	-	WDPF Advanced Digital Feedwater Control System
Beznau 1 & 2	-	ANIS Information Network Advanced Flux Mapping System
ASCO 1 & 2	-	SAMO Plant Computer
Farley 1 & 2		Plant Computer System DEH Turbine Control System
Temelin	-	Total Plant Protection, Control and Information System

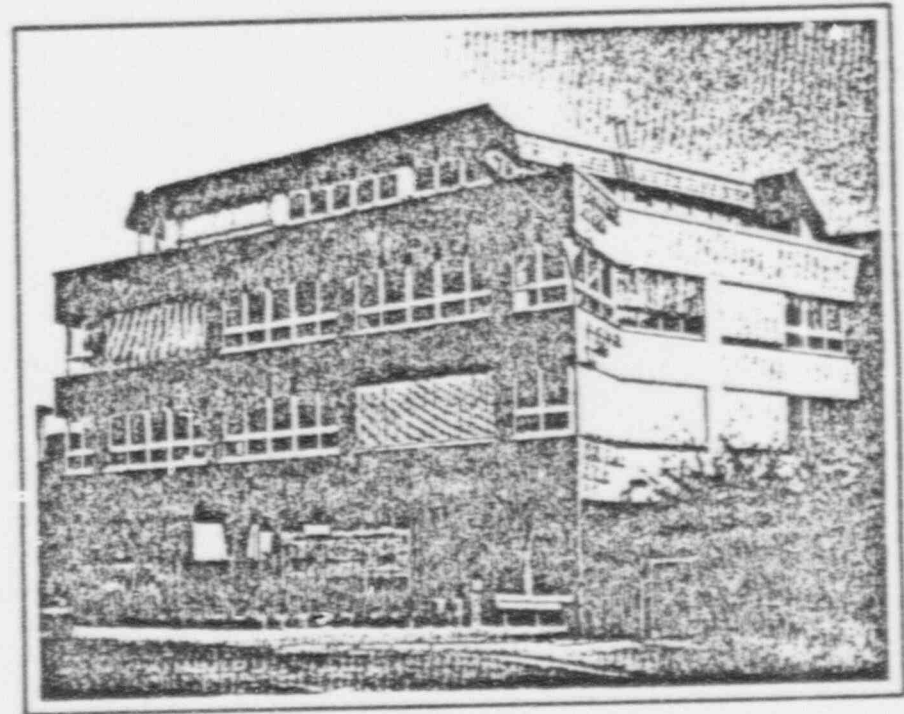
Process Control Division Headquarters


- Located in Pittsburgh, PA (C'Hara Township)
- 280,000 square-foot facility
 - State-of-the-art manufacturing
 - Project engineering/ management
 - Staging and testing
 - Strategic engineering
 - Training
 - Marketing
- More than 1400 full-time employees
- Average engineer has more than 15 years of process control experience
- Four additional major manufacturing facilities



Process Control Europe

- Located in Frankfurt, Germany
- Service to:
 - Western Europe
 - Eastern Europe
 - Middle East
 - Africa
- Seven partners



 Process Control
 Europe - Frankfurt

• Sales Offices
 ■ Partners

Partners

Czechoslovakia	Euromatic
France	Jeumont Schneider
Germany	Controlmatic
Israel	Ardan Controls
Spain	DISEL
Turkey	EKA
United Kingdom	NEI Control Systems

① Process Control Division Summary

- Long heritage of advanced control & computer systems
- Recognized leading supplier to electric utility, steel and other important industrial segments
- Business structured on global participation
- Very creative engineering-based solutions to customer needs - long list of "industry firsts"
- Management team and other employees dedicated to long-term success of the enterprise