DRS Consolidated Controls
PLμS 32 Distributed Control System

U.S. Nuclear Regulatory Commission
October 2009

Project Number: 778
DRS-2009-01 Attachment 3-NP

DRS TECHNOLOGIES

Presentation Segments

- Introduction
- Nuclear Quality Assurance
- Design Process
- Hardware Design
- Software Design
- Application Software
- Plant Applications
- Qualification
- Cyber Security

Consolidated Controls History

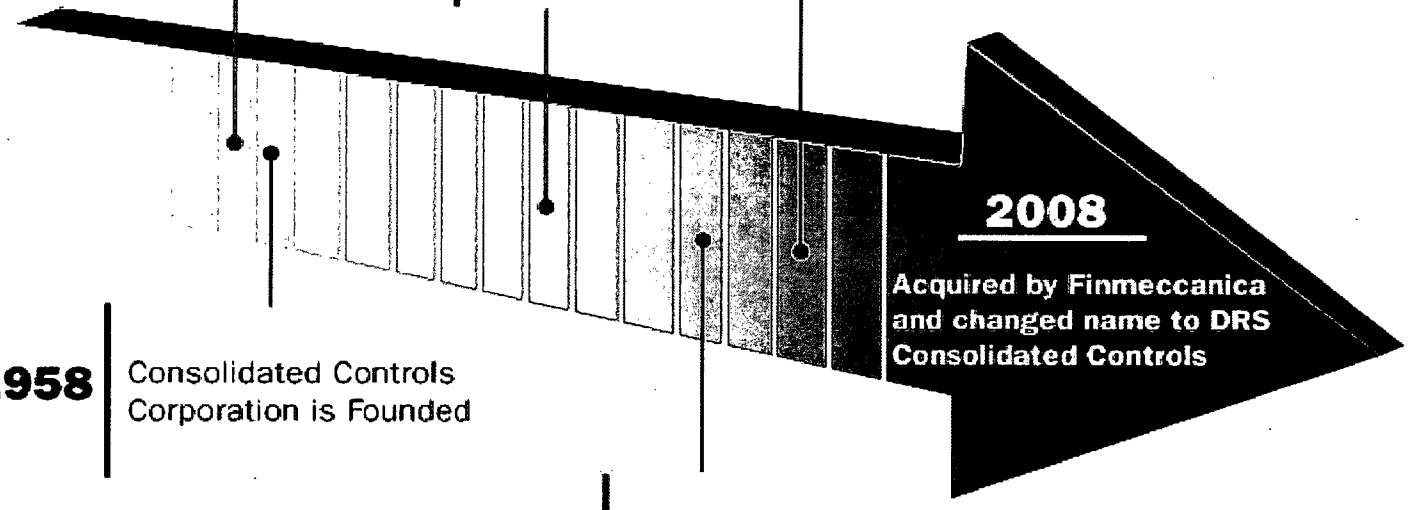
1953 Manning, Maxwell & Moore provides Nuclear Controls for USS Nautilus

1958 Consolidated Controls Corporation is Founded

1986 Acquired by Eaton Corporation

1995 Formed Eaton Navy Controls Division

2002 DRS purchased Eaton Navy Controls Division and formed DRS Power & Control Technologies



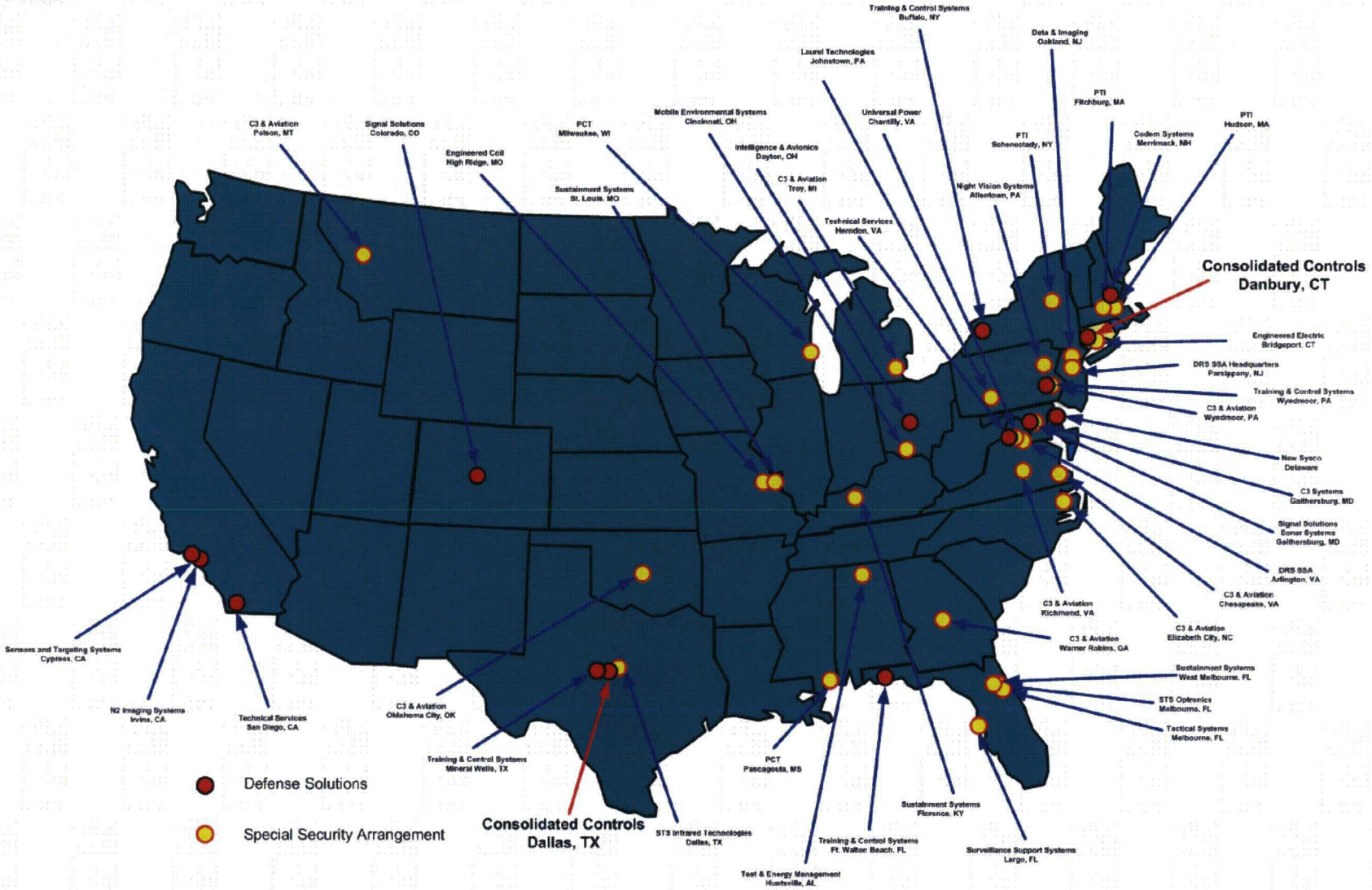
2008

Acquired by Finmeccanica and changed name to DRS Consolidated Controls

Finmeccanica and DRS Technologies

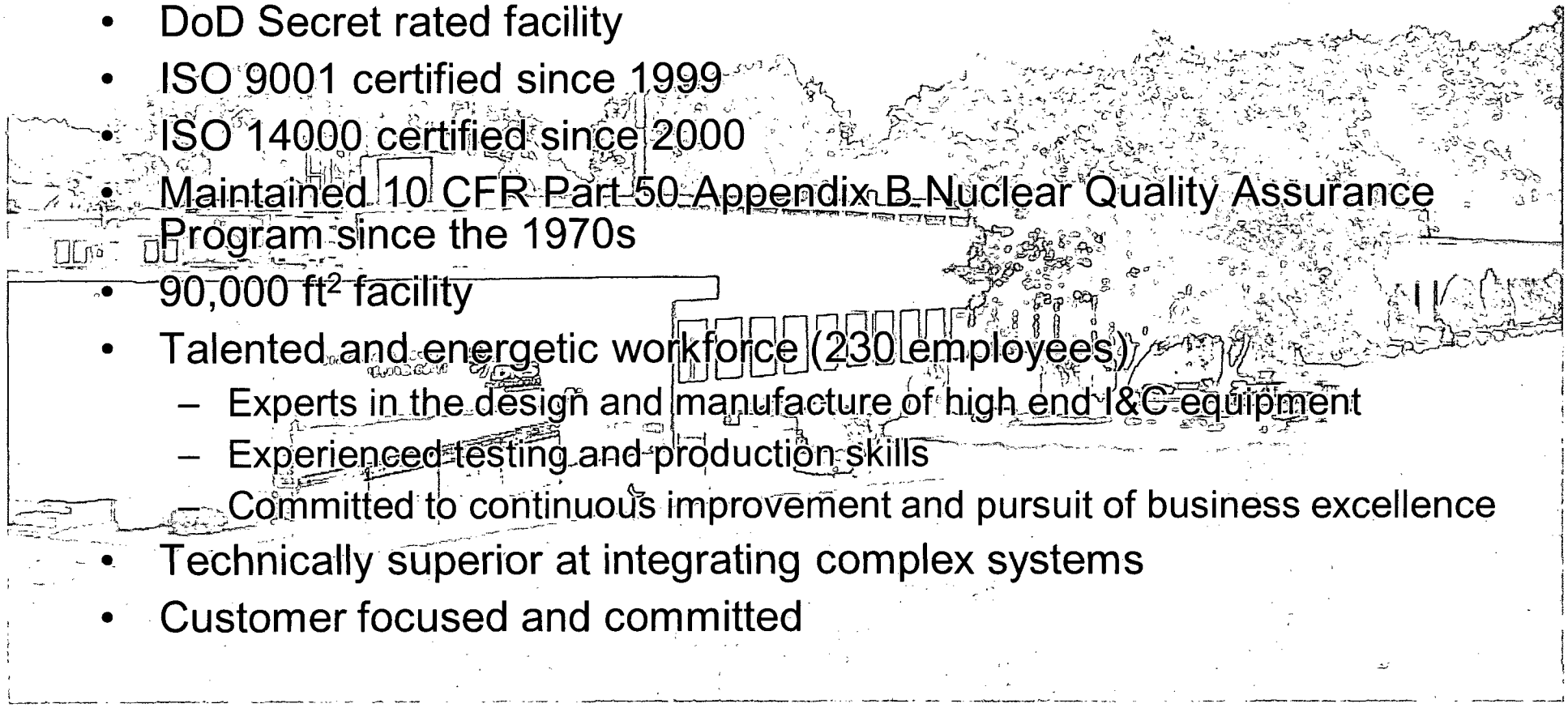
- DRS acquired by Finmeccanica for $5.2B in October 2008.
- Business units segregated to assure foreign ownership control or influence mitigation is achieved.
- Danbury business name returned to legacy Consolidated Controls

DRS Locations in the United States



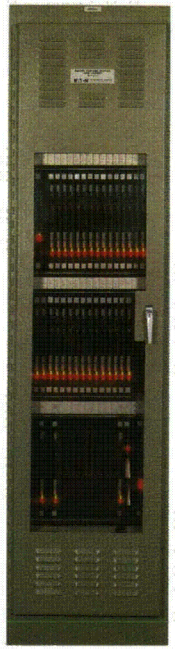
Danbury Facility

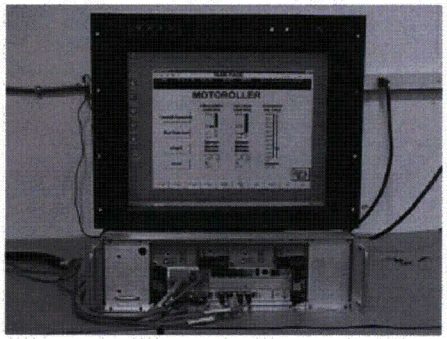
- Design, manufacture, and test of Instrumentation and Control, Automation, and Drive Actuation products for the Navy and commercial markets
- In-house facilities to manage all product development and manufacturing
- DoD Secret rated facility
- ISO 9001 certified since 1999
- ISO 14000 certified since 2000
- Maintained 10 CFR Part 50 Appendix B Nuclear Quality Assurance Program since the 1970s
- 90,000 ft^2 facility
- Talented and energetic workforce (230 employees)
  - Experts in the design and manufacture of high end I&C equipment
  - Experienced testing and production skills
  - Committed to continuous improvement and pursuit of business excellence
- Technically superior at integrating complex systems
- Customer focused and committed

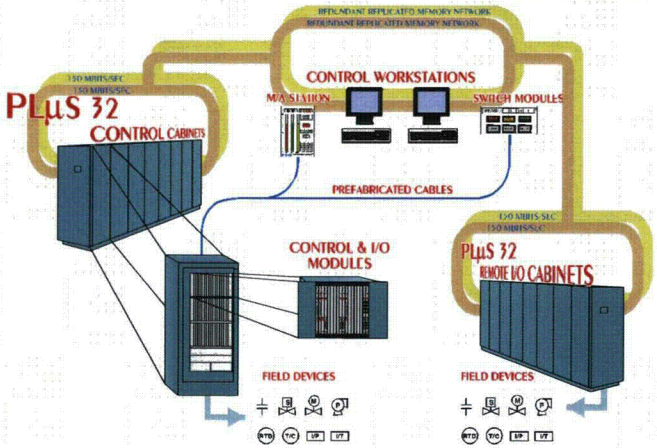


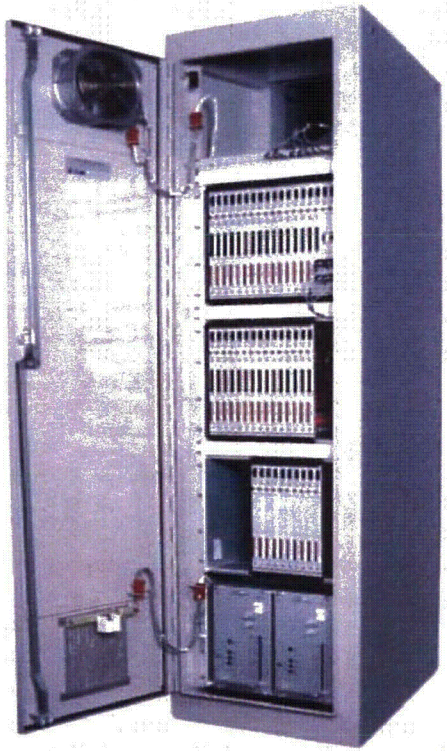
Key Products

- Commercial Nuclear Controls
  - ATWS (Anticipated Transient Without Scram)
  - ESFAS (Engineered Safety Features Actuation System)
  - EDLS (Emergency Diesel Logic Sequence
  - MSFR (Main Steam Feed Water Regulator
  - ESF (Engineered Safety Features
  - EFW (Emergency Feed Water)
  - SSLC (Safety System Logic Control)
  - BOP (Balance of Plant)





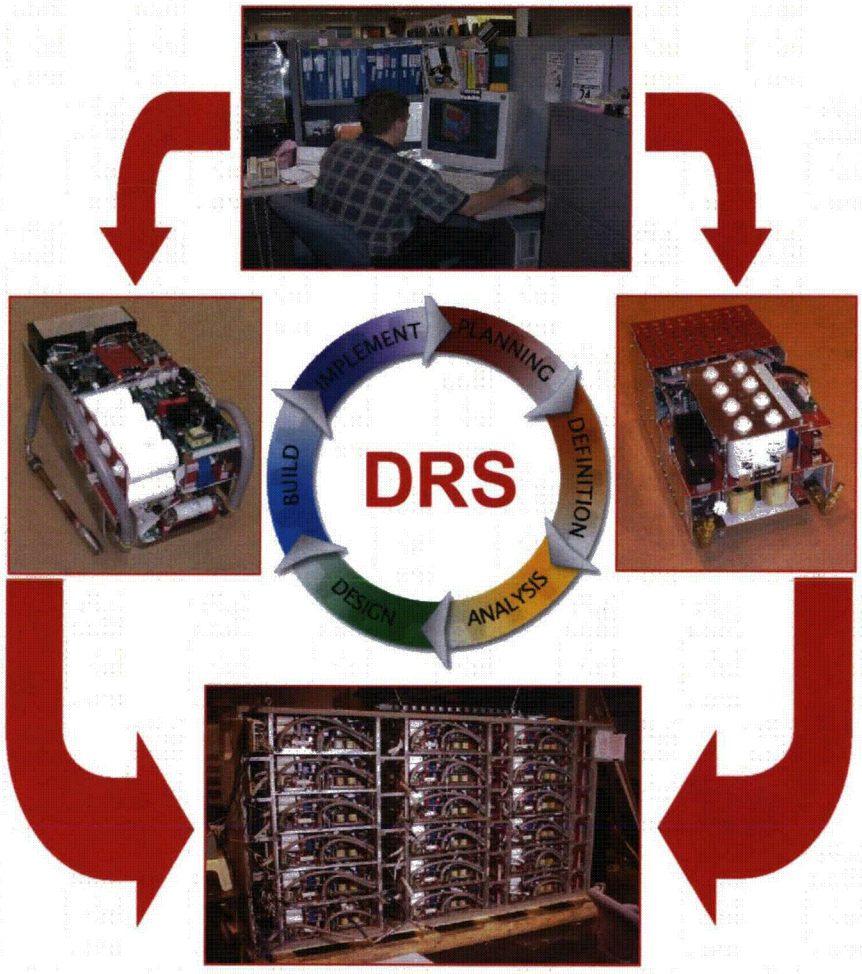




Design, Development, and Test Capabilities

- DRS has substantial capabilities to develop, manufacture and test electronic equipment
  - Facilities
    - Development laboratory
    - Environmental chambers
  - Capable Personnel
  - Equipment
  - State of art design tools for design and analysis
- All processes executed per :
  - NQA for Commercial Nuclear or
  - ISO 9001 Procedures
- Navy's world-class power electronics supplier of choice
  - Number One Supplier of I&C Equipment
  - 50 Years of experience
- Expertise in Commercial Nuclear Controls (over 37 years)

From Concept



To Production Deliverable

International Commercial Nuclear Plants with DRS Controls

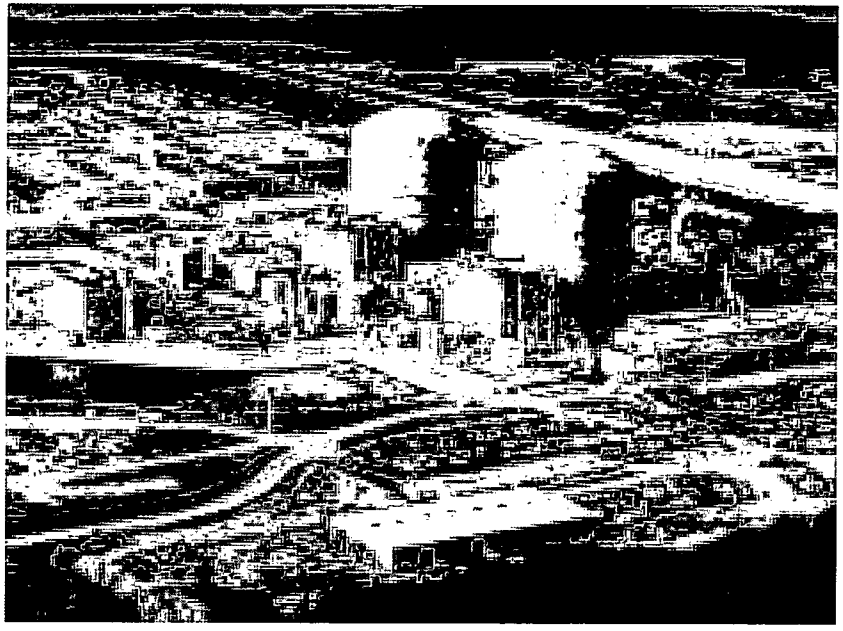
• Taiwan Power Co.	Maanshan 1&2 (W-PWR)(SSLC)
• Korea Electric Power Co.	Kori 3&4 (W-PWR) (SSLC, BOP, ESFAS, MSI)
• Korea Electric Power Co.	Yonggwang 1&2 (W-PWR) (SSLC, BOP, ESFAS, MSI)
• Korea Electric Power Co.	Ulchin 3&4 (KHI/CE-PWR) (ESF/BOP)
• Korea Electric Power Co.	Yonggwang 5&6 (KHI/CE-PWR) (ESF/BOP)
• Taiwan Power Co.	GE Lungmen 1 & 2 ESF Controls

Domestically Chosen By The Nuclear Power Industry

DRS TECHNOLOGIES

U.S. Commercial Nuclear Plants with DRS Controls

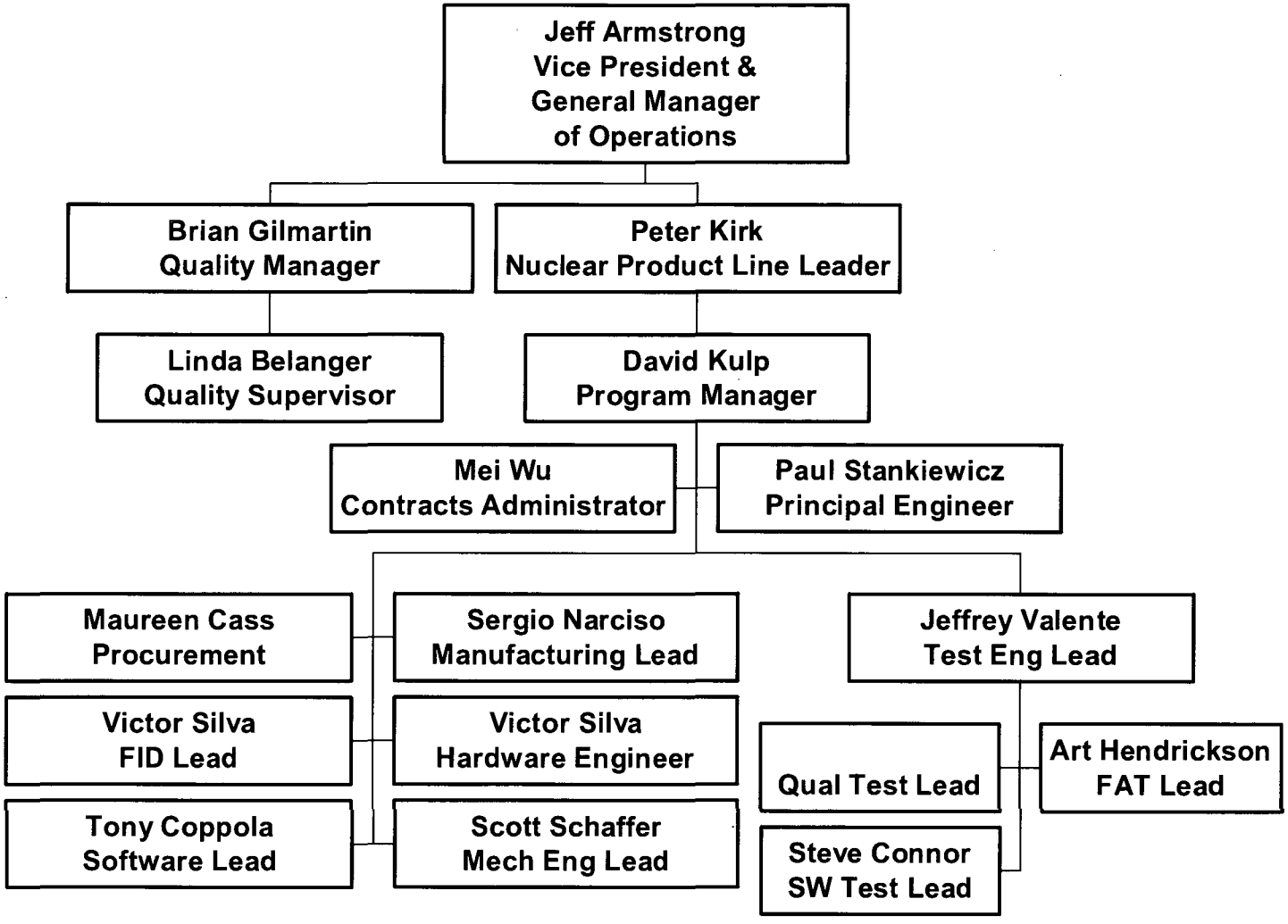
- Millstone 1&2 (ATWS, ESFAS)
- Saint Lucie 1&2 (ESFAS)
- Davis Besse (ESFAS, MSFR)
- Callaway (ESFAS, EDLS)
- Wolf Creek (ESFAS, EDLS)
- Hope Creek (SSLC, EDLS)
- Arkansas Nuclear One (EFW)
- Vogtle 1&2 (EDLS)
- Shearon Harris (IS)
- Seabrook (MSI)
- Salem 1&2 (EDLS)



Industry Services

- DRS offers products and services to keep nuclear power plants operating safely and competitively worldwide.
  - Extensive engineering / test capacities supporting
    - Complete design engineering
    - Obsolescence redesign and qualification of single components or entire systems
    - Design consulting providing solutions to complex problems
  - Field service to support deployed systems

DRS-CCI Project Structure



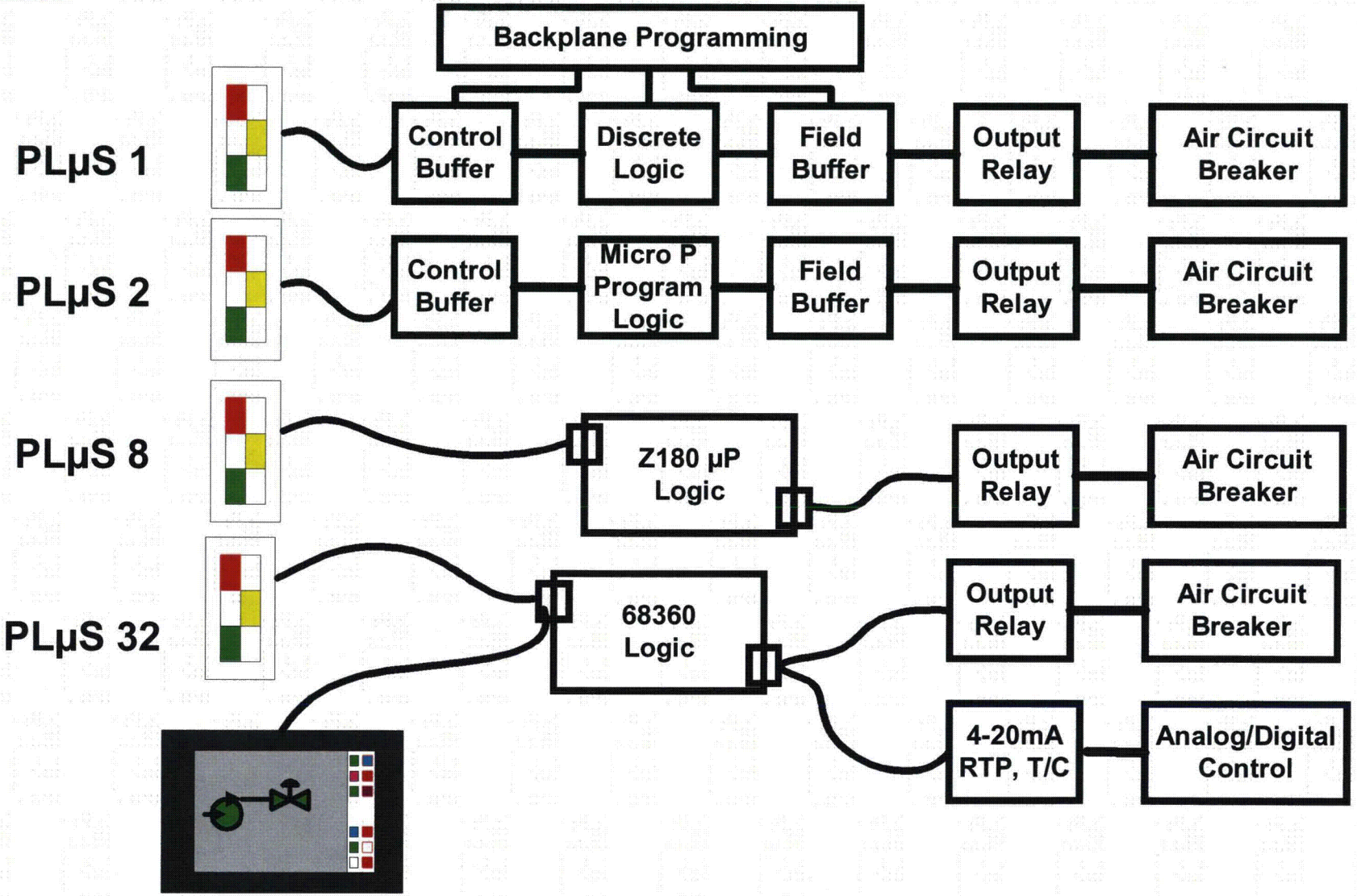
Topical Report Goals

- To Move Forward Toward Seeking Placement on NRC Docket - DRS TR Submittal to NRC in 2-4 Weeks
- Shall Cover A System That Has Been Designed & Qualified For Nuclear Safety-Related, Class 1E Applications - Is Not A Commercial Off The Shelf System
- Shall Focus on: Supplementing Utilities' Licensing Efforts

Three Basic Premises

- The PLµS 32 System Is Based on:
  - 1.0 Safety & Redundancy
  - 2.0 Safety & Redundancy
  - 3.0 Safety & Redundancy

Generations of The PLµS Series



PLµS 32 PRODUCT FEATURES

- PLµS 32 **Designed** as Nuclear Class 1E Distributed Control System
- PLµS 32 Software & Hardware are **Modular**
- PLµS 32 allows an Architectural Solution that Ranges From Control of a **Single** Plant Subsystem to an **Integrated** Distributed Control System
- Major Components Are:
  - Control I/O Modules
  - Communications Modules
  - Operator Interfaces - Consisting of:
    - Panel Mounted Devices (PMD): Control Switch Modules, Monitoring Light Modules, Manual Auto Station,
    - Video Display Units, and
    - Operator Interface Station

PLµS 32 PRODUCT FEATURES

- PLµS 32 Is **Supplied** with Redundant Deterministic High-Speed Fiber Optic Network
- PLµS 32 Is **Designed** with Hot Swappable Modules
- **Control & I/O Modules:** Powered by Redundant Power Supply That are Powered from Two Separate Power Sources
- 1996 PLµS 32 Installation Has been **Continuously Operational** For Over 750,000 Hours **Without** A Major Incident

PLμS 32 PRODUCT FEATURES

- Compliant With (Not all Inclusive):
  - 10 CFR Appendix B
  - Reg. Guide 1.75 (Physical Class 1E Separation)
  - Reg. Guide 1.89 (Qualification)
  - IEEE-603, 338, 344 (Seismic),323 (Mild Environment)
  - MIL-STD-461D/462D (EMI/RFI - Test Methods)
  - EPRI TR102323 Rev.1 (EMI/RFI - Acceptance Criterions)
- Software Design Verification & Validation (V&V) to IEEE and U.S. NRC Guidelines for Digital Systems in Safety Related Applications
  - ANSI 7-4.3.2-1993
  - IEEE-829, 1012, 1028, etc. &
  - U.S. NRC Reg. Guide 1.152, 168, 169, etc
- Manufactured Under Applicable Provisions
  - 10CFR50 Appendix B, NQA-1, and NQA-2a-1990 Part 2.7 Nuclear Quality Assurance Requirements

RETURN

DRS Consolidated Controls

PLµS 32 SYSTEM

NUCLEAR QUALITY ASSURANCE (NQA)

DRS TECHNOLOGIES

Quality Program Overview

- Compliance with 10CFR50 Appendix B/ NQA-1 including supplements (1983)
  - Internalized via Nuclear Quality Assurance Manual and Administrative Procedures (AP), Instructions, Forms, & Records
- Compliance with ASME NQA-2a, Part 2.7 - Software
  - BTP HICB-14, IEEE Std. 7-4.3.2, Reg. Guides 1.152 & 1.168
  - Internalized via Administrative Procedure AP-3.2
- Compliance with 10CFR Part 21
  - Internalized via Administrative Procedure AP-15.1
- Dedication of Commercial Grade Items -
  - EPRI TR-106439, EPRI NP-5652; EPRI NP-6406; NRC Generic Letters 89-02 & 91-05
  - Internalized via Administrative Procedures AP-7.3

Quality Assurance Responsibilities

- Quality Planning (AP-2.1)
- Qualification and Certification of Personnel (AP-2.3)
- Design & Document Review (AP-3.1 & AP-5.1)
- Software V & V - Issue Phase Summary reports (AP-3.2)
- Procurement and Supplier Control (AP-4.1, AP-7.1)
- Dedication Package Support (AP-7.3)
- Manufacturing Process Control (AP-9.1)
- Product Compliance - (AP-10.1 & AP-11.1)
- Evaluation of Non Compliances (AP-15.1 & AP-16.1)
- Control of Quality Records (AP-17.1)
- Audit - Internal/Supplier (AP-18.1)

Quality Planning

- Project Level Quality Plans
  - Quality Plans are developed to incorporate customer quality requirements identified during contract reviews.
- Sub-Assembly Quality Plans (major projects)
  - Major steps of assembly
  - Customer Approval of Documentation Requirements
  - Internal and customer witness & hold points identified
- Inspection Point Plans
  - Developed to provide a consistent and methodical process for performing inspections of assemblies.
    - Identifies specific inspection activities including inspection methods and sample sizes
    - Identifies necessary internal and customer hold points
- Quality Procurement Requirements
  - Developed for flow down of quality requirements to suppliers
    - Right of Access
    - Quality Systems
    - Technical Requirements
    - MRB Authority
    - Hold Points
    - Supplier Documentation Requirements

Certification of Personnel

- Qualification of Inspection and Test Personnel in accordance with NQA-1 1983 and Appendix 2A-1
  - Inspectors
  - Test Technicians
  - Test Engineers
    - Software Test
    - Qualification Test
    - Integrated System Testing
- Qualification of Auditors and Lead Auditors in accordance with NQA-1 1983 and Appendix 2A-3

Design Control - Hardware Quality Assurance

- Design Review
  - Participate in meetings; Follow-up & close-out of Open Items
- Document Review - Sign-off Release
  - Work Product Review Forms (WPRF)
- Verification/Prototype Testing - Module Level
  - Witness; Review & Approve Results/Reports
- Class 1E Qualification - IEEE 323, IEEE 344, MIL-Std 461 & EPRI TR102323
  - Audit Laboratories performing Qualification Tests
  - Witness; Review & Approve Results/Reports
- Integrated System Testing - Witness; Review/Approve Results

Design Control Software Quality Assurance

- Review Contract documents for requirements
- Generate Software QA Plan (Eng.) - IEEE 730
- Generate V&V Plan (NQA) - IEEE 1012
- Perform V&V activities
  - Attend Peer design review meetings
  - Review/Approve meeting minutes
  - Review/Approve design documents
  - Monitor ACE Analysis process (IEEE 7-4.3.2, Annex F)
  - Verify completion and documentation of Software Code Inspection
  - Witness Implementation & Installation Phase testing
  - Perform assessments and audits of software design activities and testing activities (IEEE 1028)
  - Issue Phase Summary reports certifying completion of all activities

Procurement and Supplier Control

- Assign Quality Requirements for each Purchase Order
- Maintain Approved Suppliers List
- Perform Supplier Quality Program Audits or Commercial Grade Surveys
- Perform Sub-Supplier QA Program Audits or Commercial Grade Surveys
- Product Verification at Supplier Facilities
  - Verify Controls of Special Processes
  - Witness testing
  - Review and Approve Test Results
  - Perform Inspections

Dedication Packages

- Review of Technical Evaluations
  - Host Component Data
  - Item Data
  - Item Procurement Evaluation
  - Justification and Analysis
  - Item Dedication Plan
- Inspection and Test of Critical Characteristics per Dedication Plan
  - QA witness of test Activities
  - QA sign review and approval of inspection and test results

Process Control

- Review and Approve Process Instructions
  - Assembly Steps
  - Required Tooling and Aids
  - Internal and Customer Witness and Hold Points
  - Required Documentation e.g. aids, test plans IPPs
- Review and Approve Aids used for Manufacturing Processes

Product Compliance

- Receiving Inspection
  - Review Shipping Release on Source Inspected Items
  - Perform Product Inspection (as required)
- In Process and Final Inspections
  - Design Drawings
  - Inspection Point Plans
  - Process Instructions
- Verification of Software Loading
  - Correct Device used
  - Checksum is verified
- Testing
  - Review and Approve Test Results
    - Production Level Testing
    - FID Logic Testing
    - Factory Acceptance Testing
    - Qualification Testing
- Packaging Inspections
  - Reviewed and Approved Packaging Procedures
  - ANSI N45.2.2

Evaluation of Non Compliances

- Product Issues Reported on Non Conforming Material Reports (NCMs)
  - MRB Review (Engineering and Quality Assurance)
    - Assign Disposition
    - Review Part 21 Applicability
    - Issue Corrective Actions as Necessary
    - Seek customer approval for Use-As-Is and Repair Dispositions
- Corrective Actions
  - Containment Action
    - Review issue for impact to product including Part 21
  - Root Cause Identification
  - Corrective/Preventative Actions taken
  - Follow Up

Quality Records

- Identified
- Classified as Life Time or Non-Permanent
- Retention Periods identified
- Duplicate Storage Locations Maintained
- Accessibility to Records Identified

Internal Audits

- Scheduled Annually
- All aspects of the Quality Program Reviewed
- Audit Plans and Check Lists Used
- Audits performed by Lead Auditors
- Results are Documented

External Audits of Quality Assurance Program

- October 2009 – EDG Provider NQA Audit
- April 2009 – General Electric Nuclear Engineering (GENE) performs annual audit of Nuclear Quality Program for the Lungmen 1&2 project
- April 2009 – Westinghouse initial assessment of DRS's Nuclear Quality Program
- March 2008 – General Electric Nuclear Engineering (GENE) performs annual audit of Nuclear Quality Program for the Lungmen 1&2 project
- January 2008 – Seven-member NUPIC team led by Progress Energy

RETURN

DRS Consolidated Controls

PLµS 32 SYSTEM

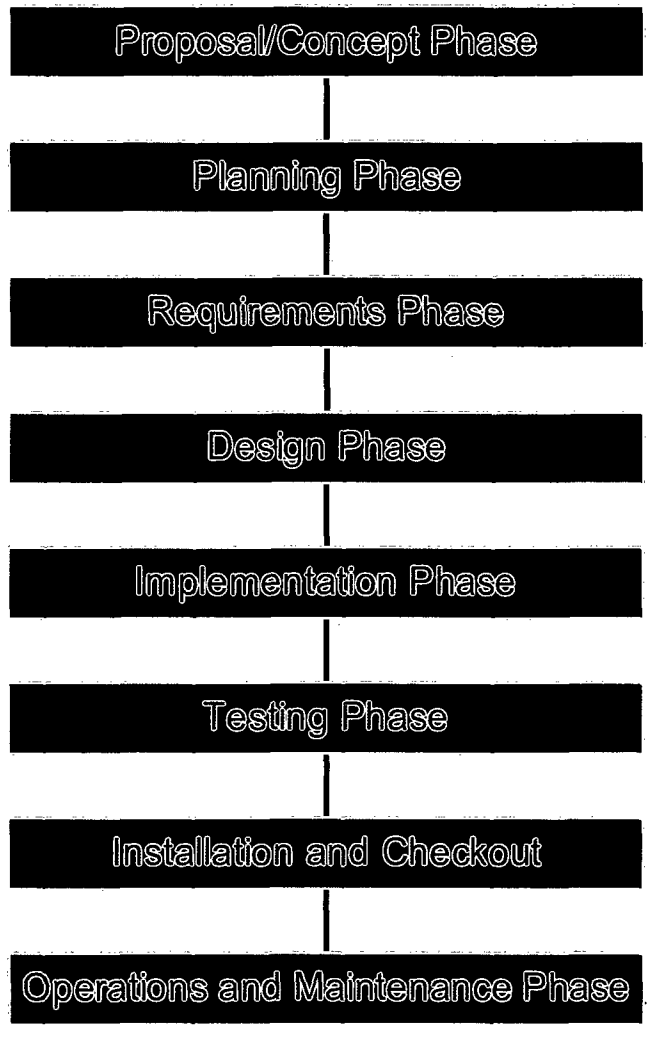
DESIGN PROCESS

DRS TECHNOLOGIES

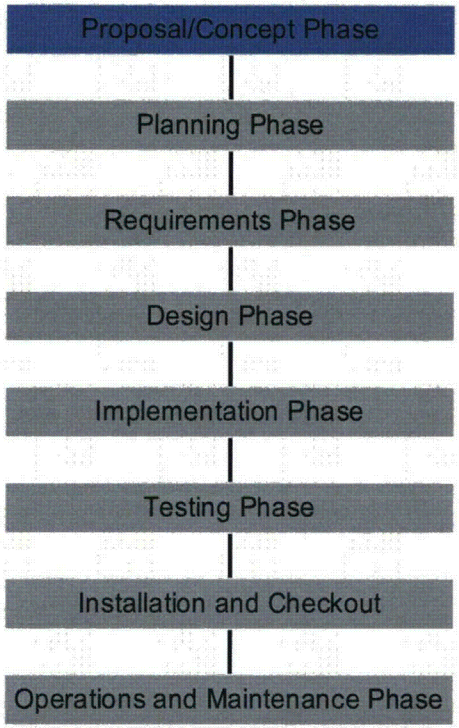
DESIGN PROCESS

- PLµS 32 developed and designed to IEEE and U.S. NRC Guidelines for Digital Systems in Safety Related Applications
  - IEEE 7-4.3.2, 1012, 1028, etc.
  - U.S. NRC Reg. Guide 1.152, etc.

DESIGN PROCESS

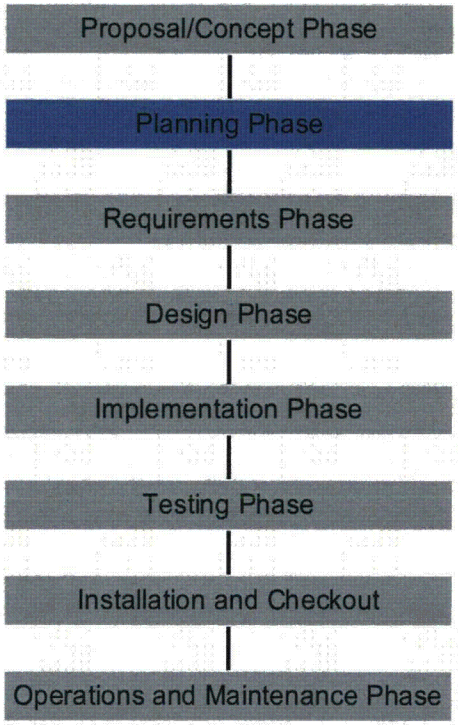


PROPOSAL/CONCEPT PHASE



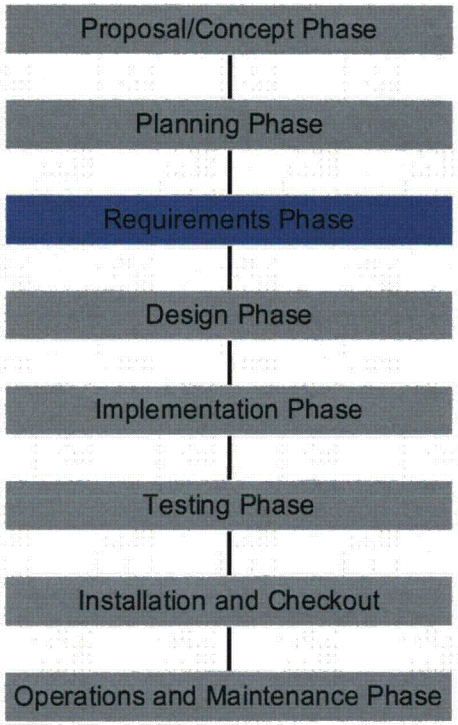
- Inputs
  - Customer Request for Quote
  - Sales and Marketing Information
  - Industry Guidelines and Standards
  - Internal Processes and Procedures
  - Clarifications and Exceptions
- Outputs
  - Contract
  - Rough Budget
  - Rough Schedule

PLANNING PHASE



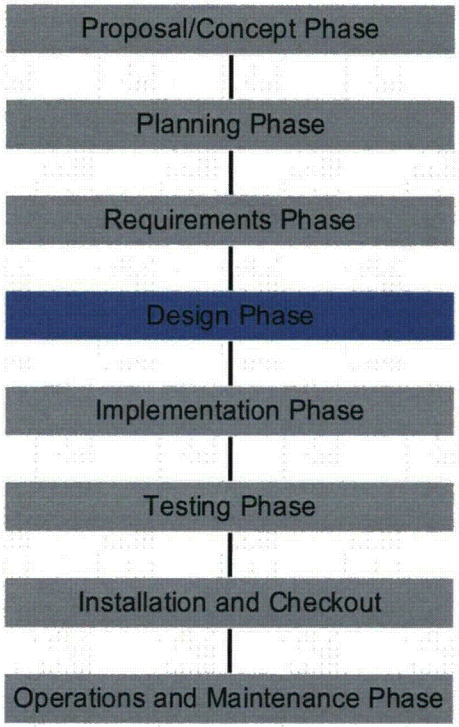
- Inputs
  - Contract
  - Industry Guidelines and Standards
  - Internal Processes and Procedures
- Outputs
  - Design Input Requirements Definition
  - Project Plan
  - Configuration Management Plan
  - Software Development Plan
  - Software V&V Plan
  - System Design Basis Specification
  - Baseline Schedule and Budget

REQUIREMENTS PHASE



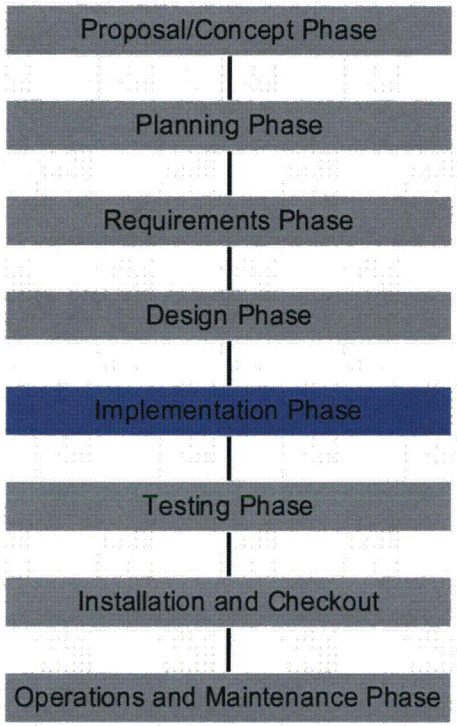
- Inputs
  - Plans from Previous Phase
  - System Design Basis Specification
  - Software Development Plan
- Outputs
  - System Test Plan
  - Specific Design Basis Specification(s)
  - Software Requirements Document(s)
  - Requirements Traceability Matrix
  - Abnormal Conditions and Events Analysis
  - Software V&V Report(s)

DESIGN PHASE



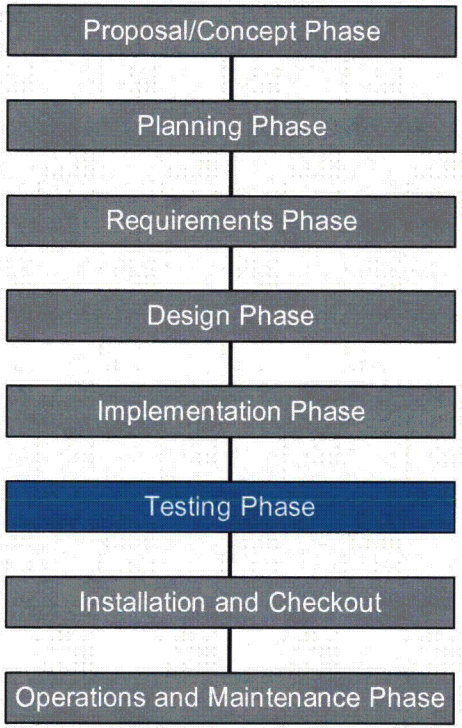
- Inputs
  - Plans from Previous Phases
  - Specific Design Basis Specification(s)
  - Software Requirements Document(s)
  - System Test Plan
- Outputs
  - Schematic(s) and Drawing(s)
  - Software Design Document(s)
  - Software Test Plan
  - Programming Style Guide
  - Requirements Traceability Matrix
  - Abnormal Conditions and Events Analysis
  - FMEA/Component Stress Analysis
  - Software V&V Report(s)

IMPLEMENTATION PHASE



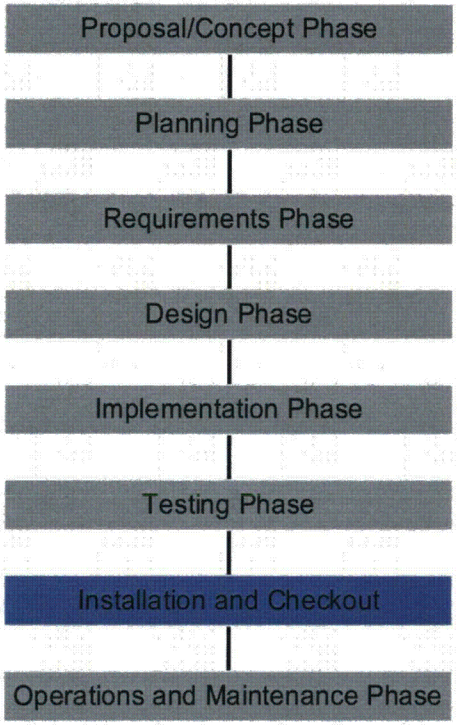
- Inputs
  - Plans from Previous Phases
  - Specific Design Basis Specification(s)
  - Software Design Document(s)
  - Programming Style Guide
- Outputs
  - Factory Acceptance, Qualification, Module, and Software Test Procedures
  - Source Code Listing Document(s)
  - Requirements Traceability Matrix
  - Abnormal Conditions and Events Analysis
  - Software V&V Report(s)

TESTING PHASE



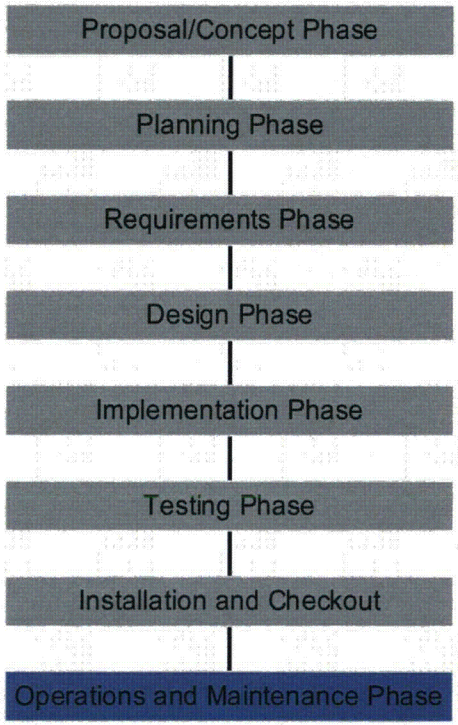
- Inputs
  - Plans from Previous Phases
  - Specific Design Basis Specification(s)
  - Factory Acceptance Test Procedure
    - This is a multi-phase procedure
  - Qualification, Module, System, and Software Test Procedures
- Outputs
  - Test Reports
  - Field Performance Test Plan
  - Requirements Traceability Matrix
  - Abnormal Conditions and Events Analysis
  - Software V&V Report(s)

INSTALLATION AND CHECKOUT PHASE



- Inputs
  - Plans from Previous Phases
  - Factory Acceptance Test Procedure
    - This is a multi-phase procedure
- Outputs
  - Factory Acceptance Test Report
  - Software Trouble Report(s) (if applicable)
  - Requirements Traceability Matrix
  - Abnormal Conditions and Events Analysis
  - Software V&V Report(s)

OPERATIONS AND MAINTENANCE PHASE



- Inputs
  - Plans from Previous Phases
- Outputs
  - Software Trouble Report(s) (if applicable)
  - Requirements Traceability Matrix
  - Abnormal Conditions and Events Analysis
  - Software V&V Report(s)

RETURN

DRS Consolidated Controls

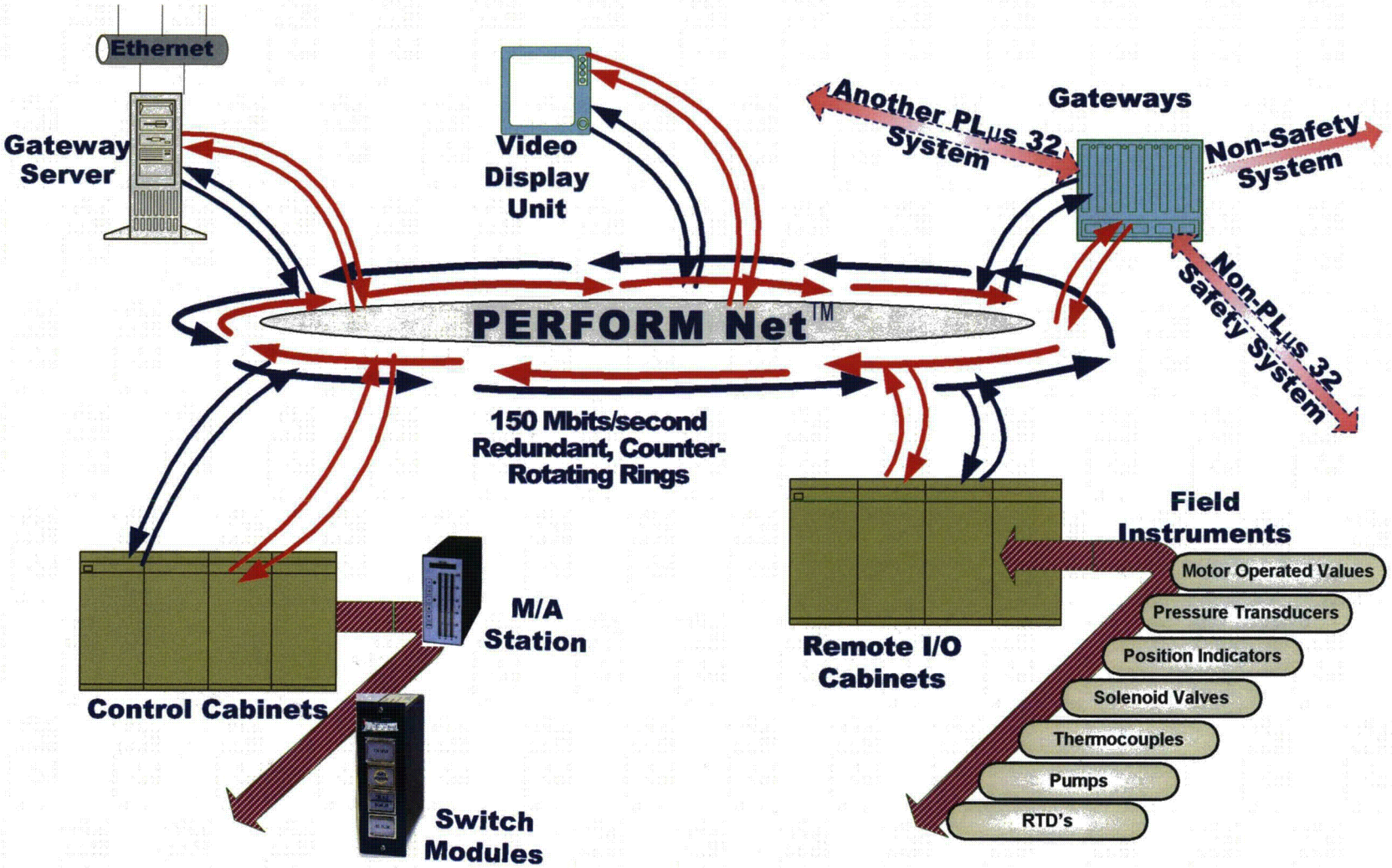
PLµS 32 SYSTEM

Hardware

- Modules
- Card Rack
- Cabinets
- Communications
- Network
- Operator Interfaces

DRS TECHNOLOGIES

GENERIC SYSTEM CONFIGURATION



MODULES

- Control I/O Modules
  - Digital Control Module (DCM)
  - Analog Control Module (ACM)
  - Analog Input Module (AIM)
  - Analog Output Module (AOM)
  - Thermocouple Module (T/CM)
  - RTD/0-2K Ohm Module (RTD)
  - Digital Output Module (DOM)
- Communications
  - Network Interface Module (NIM)
  - Bridge Transfer Module (BTM)
  - Communications Interface Module (CIM)

- Features on Each Module
  - Module Divided Into Three Sections
    - Control (Operator Interface)
    - Logic (Microprocessor and Communications)
    - Field (Field Control Devices)
  - Power Auctioneered On Each Module
    - Separate Power Supplies for Each Section
    - Hot Swappable
  - Each Module Has Control Capability With Some Input And/or Output Capability
    - 4-20 mA In/Out, TC, RTD (All with Auto-Calibration)
    - Digital Modules with On-board Ground Fault Detection on FSR Inputs

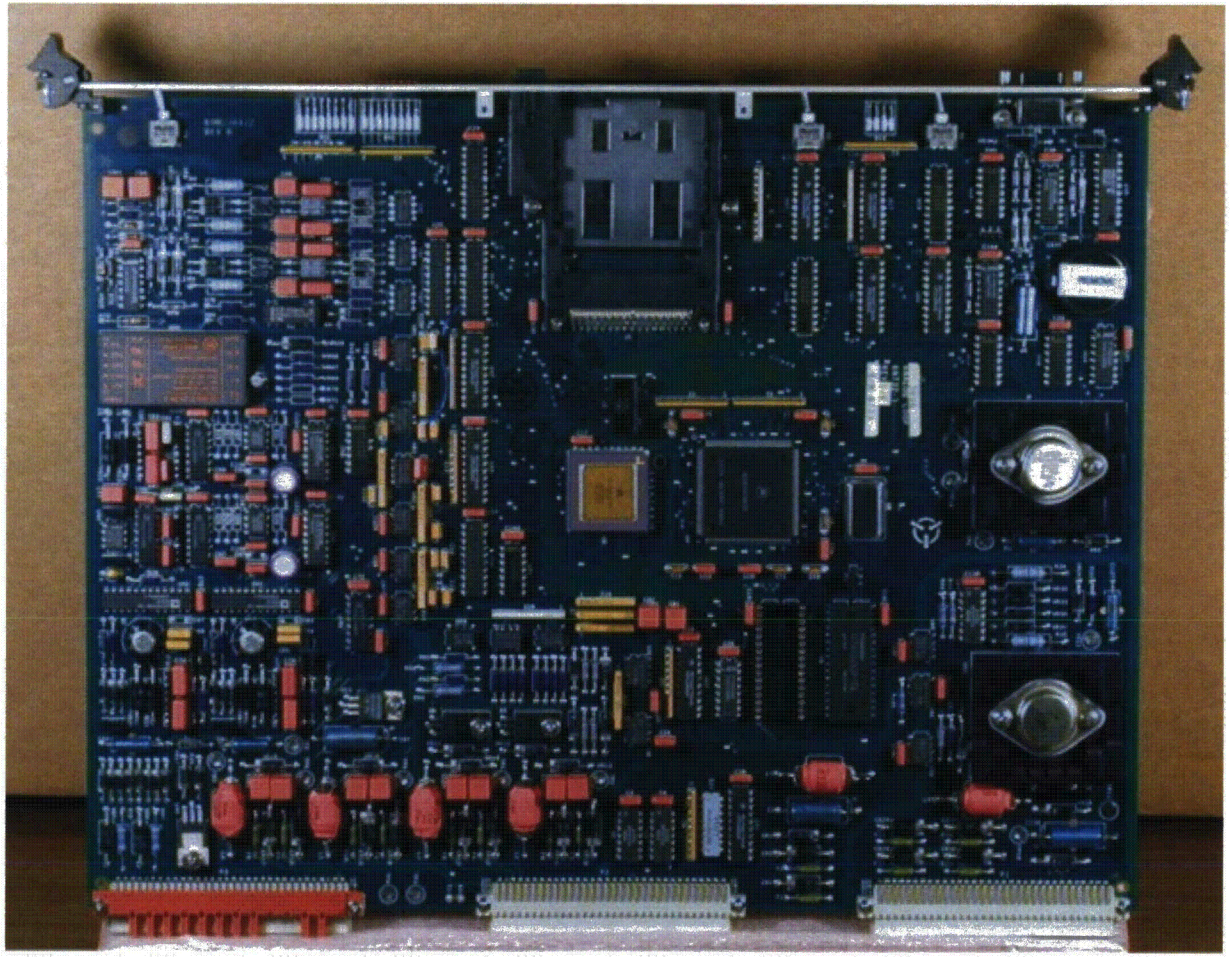
MODULES

- Features on Each Module
  - All Software is Stored on Module in Dedicated EPROM
  - Every Module has a Motorola MC68360 Microprocessor
  -
  -
    -
  - Designed for a 40 Year Product Life

MODULES

- DIAGNOSTIC CAPABILITIES
  - Continuous On-Line Diagnostics Performed on All Modules
  -
  - Levels
    -
    -

MODULES

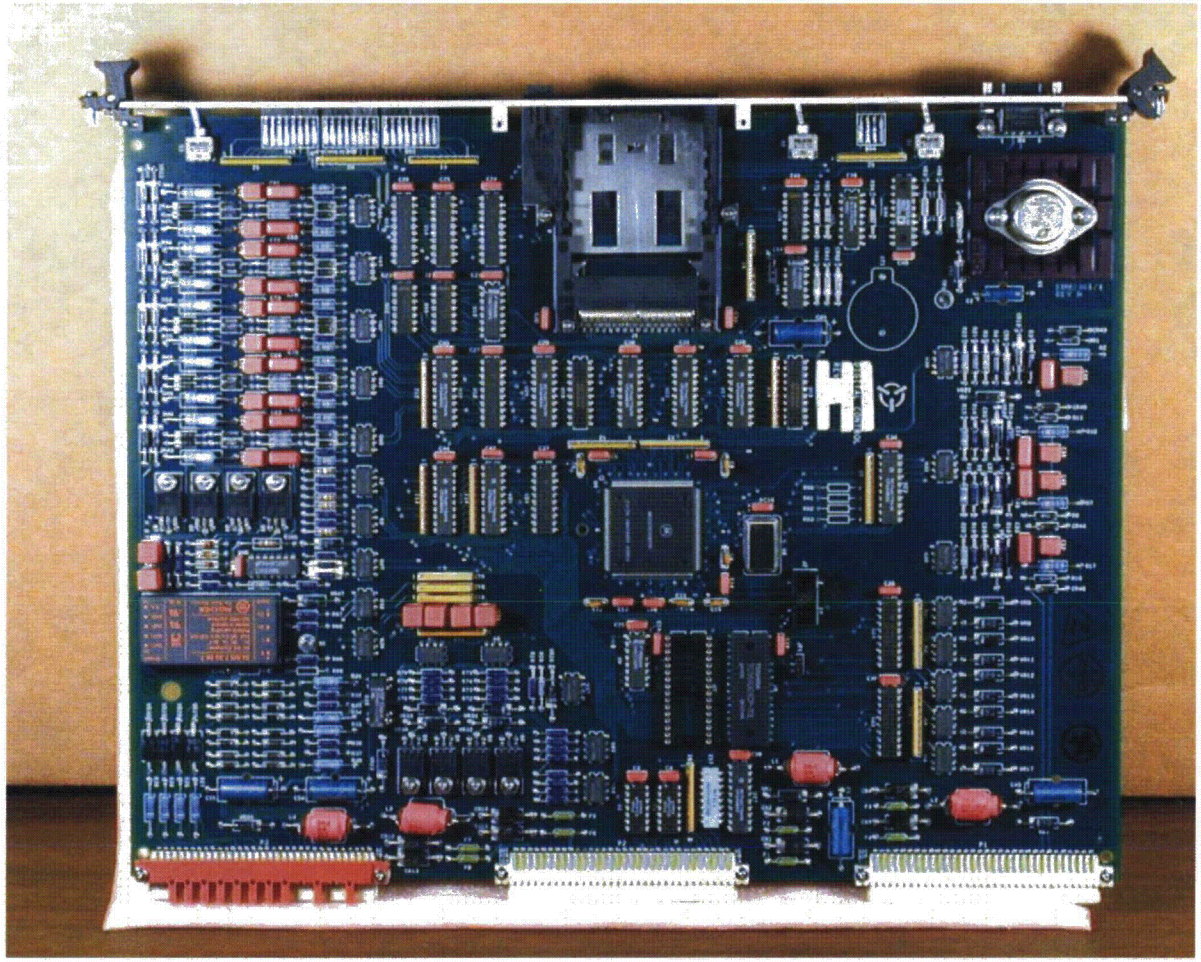


ANALOG CONTROL MODULE

MODULES

- FAULT TOLERANT
  -
  - Redundant Communication Paths
  -
  - Dedicated A/D for Analog Inputs
    - Failure of an A/D only impacts a single input
  - Dedicated D/A for Analog Outputs
    - Failure of a D/A only impacts a single output
  - Each Module Determines the Network Used
    -
    -
  - Redundant Module and I/O Capability

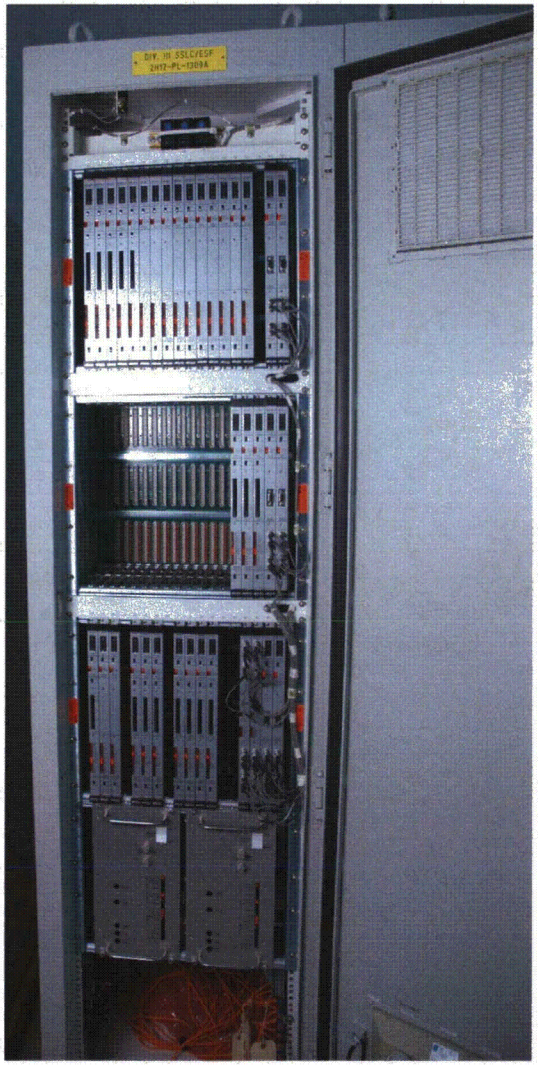
MODULES



DIGITAL CONTROL MODULE

CARD RACKS

- Each Rack Holds 16 Modules Plus 2 NIMs
- Redundant DC Power Feeds Per Section
- Designed as Modular Building Blocks
  - Any Module Function in Any Slot
- Redundant Backplane Communications
  - RS 485 Serial Communication
  - 1.5 Mbit/second HDLC Full Duplex Communication
- Identification
  - Slot Number
  - Rack Number
  - Rack to Module Keying



CABINETS

- Two Basic Cabinet Types
- Logic Cabinets
  - 3 Logic Racks for 48 Modules
    - 2 Network Modules per Cabinet
  - Power Supply Rack
    - Redundant Supplies
    - Independent Power Sources
  - EMI Filters for Each Power Feed
  - Cooling Fans and Controls
- Termination Cabinet
  - Separate Cabinet for EMI Control
  - Termination Assemblies for Field Wiring and Relay Mounting
    - Analog and Digital Designs
  - Modular Design
    - Plug Connector Interface Cables Between Termination Assemblies and Racks
    - Relays and Fusing all on Termination Assembly

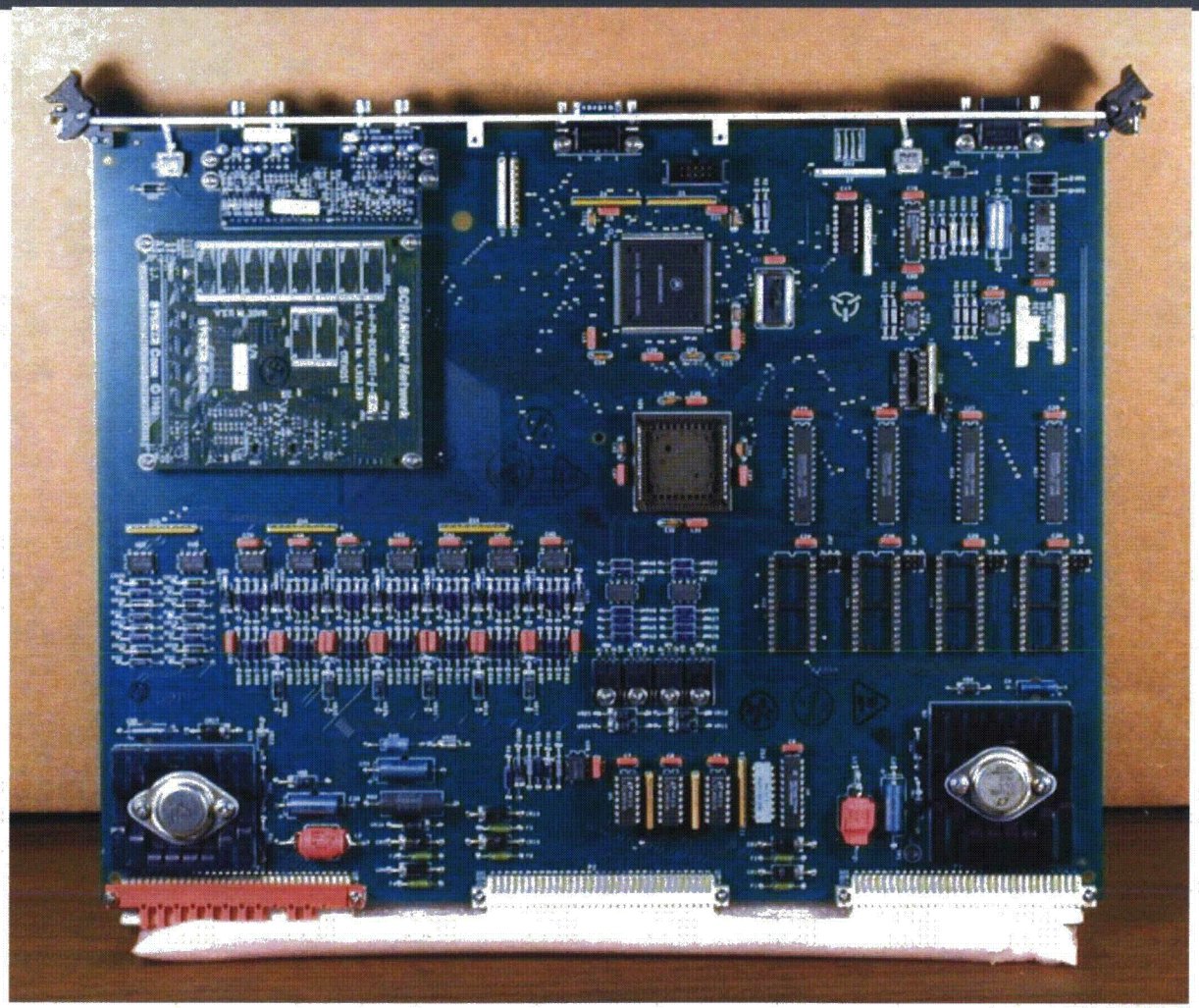
COMMUNICATION

- Network Interface Module (NIM)
  - Communication Link From Cabinet To Cabinet
  - Communication Link Network To Module
  - Communication Link Module To Module
- Communication Interface Module (CIM)
  - Low Data Volume Transfer Network to Network
  - Gateway Interface
    - Device Net
    - Ethernet
    - MODBUS
    - Serial (RS232/RS422/RS485)
    - ATM
    - Profibus
  - 3 Separate and Independent Communication Paths
- Bridge Transfer Module (BTM)
  - High Speed High Data Volume Transfer From Network to Network

COMMUNICATION

- One Module for each Network
- Two Modules for Each Cabinet
- Cabinet Identification/Node Number
  - Hardware Based
  - 128 Maximum Nodes on Network
- Communication
  - Serial RS485 Cabinet Internal (NIM/CIM)
  - Fiber Optic External
- Software Features
  - Cabinet Start-up Node Verification
  - Heart Beat Generation and Validation
  - Network Data Storage and Distribution
  - Cabinet Cooling and High Temperature Alarm (NIM)
  - Cabinet Alarm/Status Reporting (NIM)

COMMUNICATION

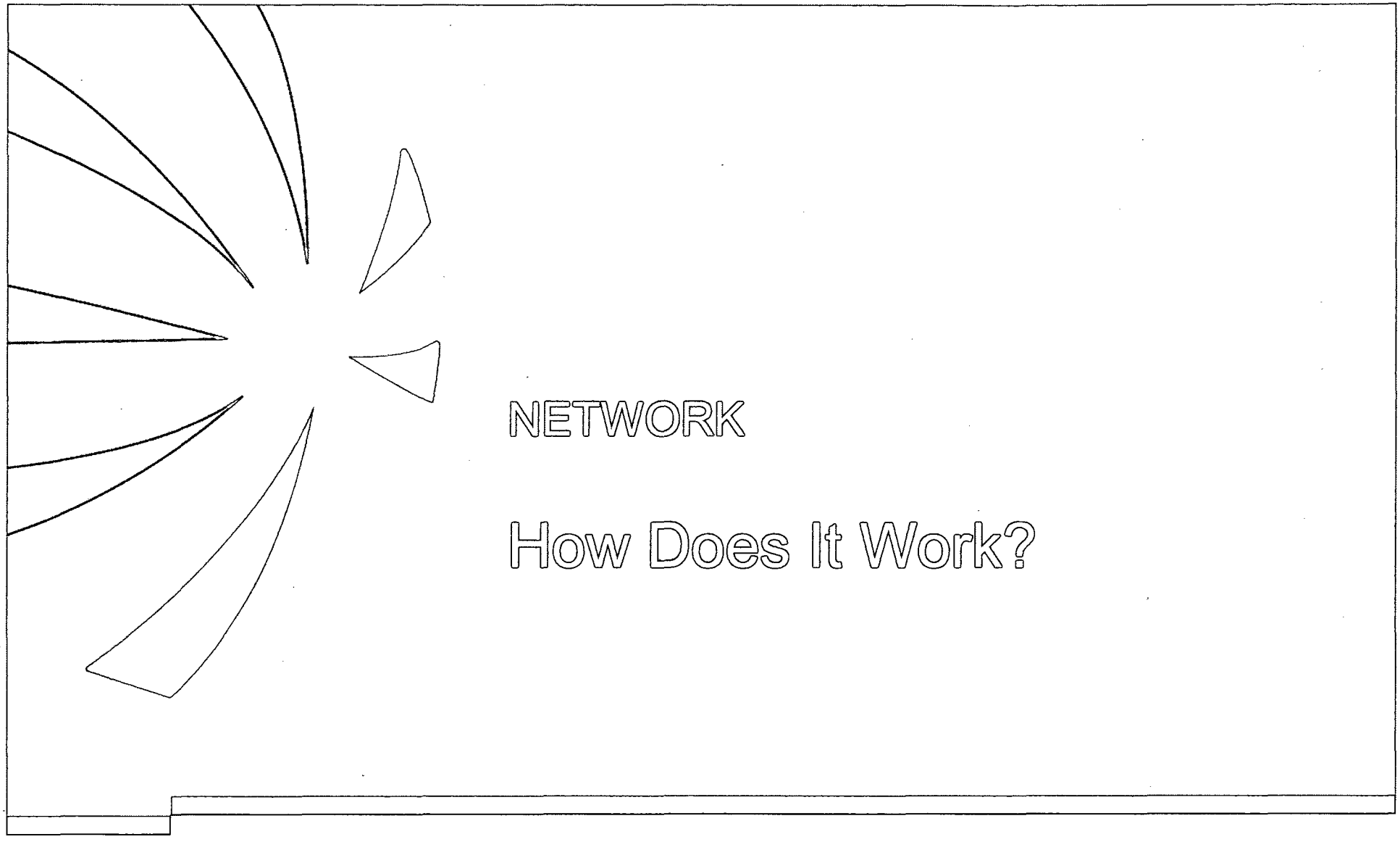


NETWORK INTERFACE MODULE

NETWORK

- PERFORM Net
  - Performance Enhanced Redundant Fiber Optic Replicated Memory Network
- FEATURES
  - Fiber Optic Cabling for Noise Immunity and Electrical Isolation
  - Hardware Based, No Software
  - 150 Mbits/second Data Transmission
  - Redundant Counter Rotating Ring Topology
  - Both Networks Active at All Times (No Failover Delay)
  - All Data Transmitted All The Time

- FEATURES
  - Deterministic Time Response
    - 50 Milliseconds
      - Input - Control - Output on a single module.
    - 100 Milliseconds
      - Input on one module, Control - Output on a second module anywhere in the system.
    - 150 Milliseconds
      - Input on one module, Control on a second module, Output on a third module. Module locations anywhere in the system.
  - Flexible System Configurations
    - Remote or Local I/O
    - Remote or Local Control



NETWORK

How Does It Work?

DRS TECHNOLOGIES

NETWORK

- Concept
  -
  -
  -
  -
  -

- Concept
  -
  -
  -
    -
    -
    -

- Independence
  - Per IEEE 7-4.3.2 1993 Appendix G
  - NIM Provides Data Control For All Data Passed to the Modules
  - Only Data Requested by the FID is Passed From the NIM to the Module
  - Separate Communications Drivers And Receivers on the Module and NIM

NETWORK

DRS TECHNOLOGIES

NETWORK

DRS TECHNOLOGIES

NETWORK

DRS TECHNOLOGIES

DRS TECHNOLOGIES

- Memory
  -
  -
  -
    -
  -

NETWORK

DRS TECHNOLOGIES

NETWORK

NETWORK

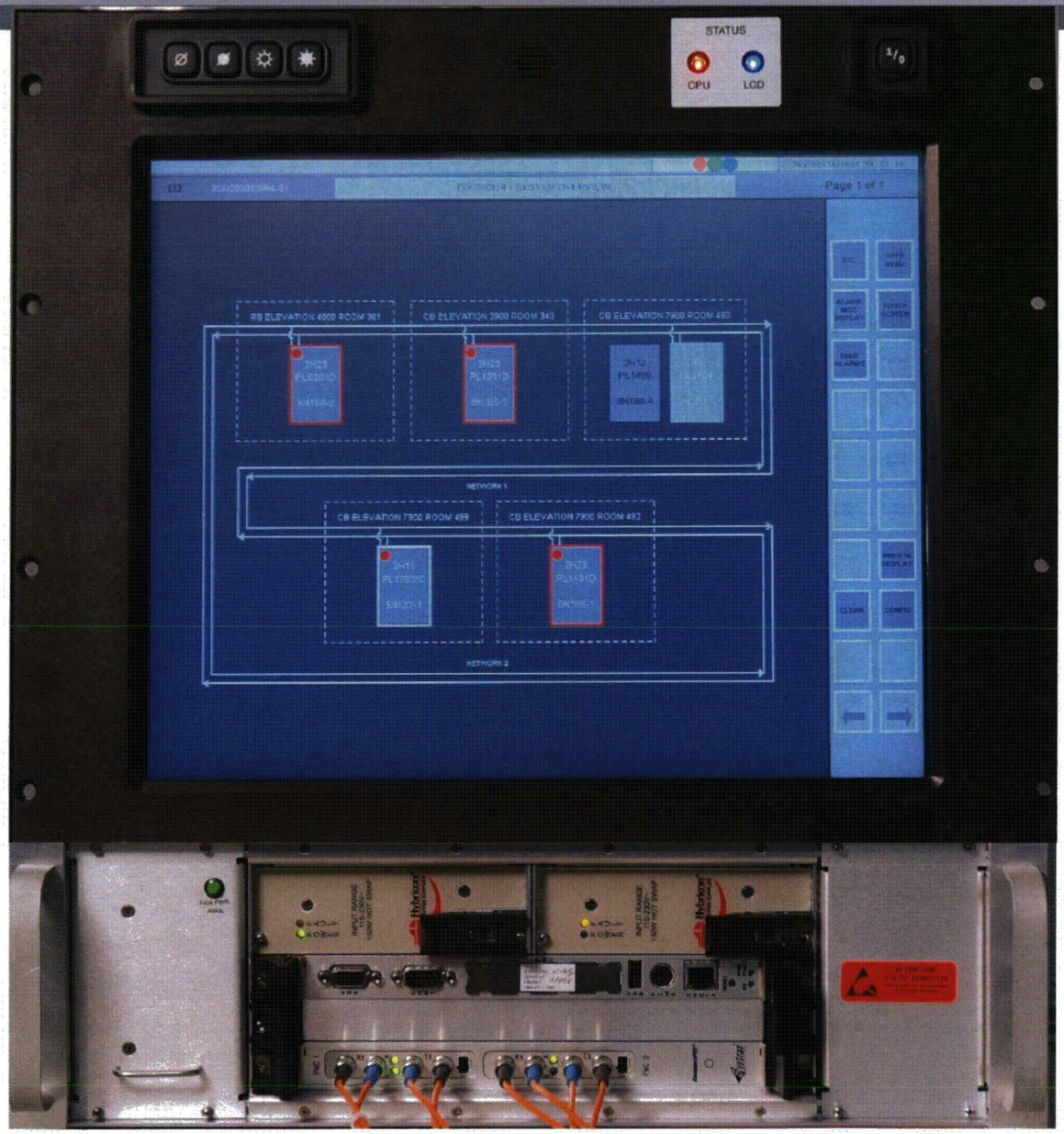
OPERATOR INTERFACES

- Hardwired or Soft Control
  - Control Board Mounted Switches and Indicator Lights
  - M/A Stations for PID Control Loops
  - Operator Interface Subsystem (OIS)
    - Non-safety Class
    - Monitoring and Diagnostics Only
    - Windows Based Operating System
  - Video Display System (VDU)
    - Safety Class
    - Control, Monitoring and Diagnostics
    - Once Through Operating System

OPERATOR INTERFACES

OPERATOR INTERFACES

OPERATOR INTERFACES



RETURN

DRS Consolidated Controls

PLµS 32 SYSTEM

SOFTWARE DEVELOPMENT

DRS TECHNOLOGIES

DEVELOPMENT PHILOSOPHY

- Keep It Simple Stupid (KISS) Philosophy
- Minimal interrupts
  - Interrupts used only for communications
- No recursion, No multi-tasking, No self-modifying code
- No commercial software in the safety operating equipment
  - VDU has a small commercial software package that DRS has qualified
- Independence of software test group
  - Involvement from cradle to grave
- Abnormal Conditions & Events (ACE) analysis

SPECS/REG GUIDES

- Development processes in accordance with IEEE standards and NRC Reg. Guides
  - Software development plan / SQAP - IEEE 730.1
  - Software V&V plan written and enforced by independent NQA group - IEEE 1012, 1028, RG 1.168
  - Configuration Management - IEEE 828, RG 1.169

SOFTWARE MODULES

- NIM - Network Interface Module
- CIM - Communications Interface Module
- Control & I/O Modules
  - –
  - –
  - –
- FIDC - Functional Interconnect Diagram Compiler
- VDU - Video Display Unit

SOFTWARE MODULES
NIM & CIM Components

NETWORK INTERFACE MODULE (NIM)

-
-
  -
-
  -
-
  -

- Two per cabinet for redundancy
- Performance of Cabinet Diagnostics
  - Power Supply Status, Fan Control, Module Status

NETWORK INTERFACE MODULE (NIM)

Operating Cycle

COMMUNICATIONS INTERFACE MODULE (CIM)

- The CIM provides serial buffering between 1E safety systems per IEEE 7-4.3.2
- The CIM software is based on the NIM software
- Operates on a 20 ms operating cycle
-
-

SOFTWARE MODULES
Control & I/O Components

CONTROL & I/O MODULES

- Software Startup Checks
  - Module Type
  - Rack Location
  - Cabinet/Node
- Network Data Validated on each Module before Being Used

CONTROL OPERATING SYSTEM (COS)

- Simple main operating loop (MOL)
  - See diagram next slide

COS OPERATING CYCLE

UNIQUE COS

- Interface to hardware devices - control and field
-
-
  -
  -
-

CONTROL ALGORITHMS (CA)

- Library of more than 100 control algorithms
-
-
-

FUNCTIONAL INTERCONNECT DIAGRAM COMPILER (FIDC)

-
-
-
-

- Processes Information from OrCAD
- Validates the Data from OrCAD
-

FUNCTIONAL INTERCONNECT DIAGRAM COMPILER – What does it do?

FUNCTIONAL INTERCONNECT DIAGRAM COMPILER (FIDC)

- OrCAD to Binary File Manager

FUNCTIONAL INTERCONNECT DIAGRAM COMPILER (FIDC)

DRS TECHNOLOGIES

- Binary Processing

FUNCTIONAL INTERCONNECT DIAGRAM COMPILER (FIDC)

DRS TECHNOLOGIES

- Binary Creation

SOFTWARE MODULES
VDU Components

Video Display Unit (VDU)

- The VDU includes the Display Controller and Flat Panel Display Assembly
  - Display Controller – Intel Pentium III based Single Board Computer and two SCRAMNet cards in a Compact-PCI case
  - Flat Panel Display Assembly – 18.1" display, touch screen, Analog Interface board, speaker
- The VDU software provides soft controls of the equipment via a flat panel display / touch-screen
- The VDU provides the interface between a human and the PLµS 32 Control System
- The VDU incorporates requirements based on NUREG 0700

Video Display Unit (VDU)

- VDU Display Controller Software Components:
  - Custom Operating System Software
  - Application Software
- Custom Operating System Software
  -
  - VDU Control Operating System (VCOS)
    -
    -
    -
    -
      -
      -

Video Display Unit (VDU)

- Application Software Components
  - Developed in cooperation with the end user
    - Screen layout, operation, navigation are developed to meet end user specifications
  - Configuration / Setup Screens
    - Configuration Entry Screen, Touch Screen Calibration Screen, Clean Screen
  - Diagnostic Screens
    -
      -
        »
    -

Video Display Unit (VDU)

- Application Software Components (cont.)
  - Process Display Executive
    -
    -
    -
    -
  - Process Screens (Automatically Generated)
    - Provide monitoring & control of individual systems within division

RETURN

DRS Consolidated Controls

PLµS 32 SYSTEM

Application Software

DRS TECHNOLOGIES

FUNCTIONAL INTERCONNECTION DIAGRAMS – FID

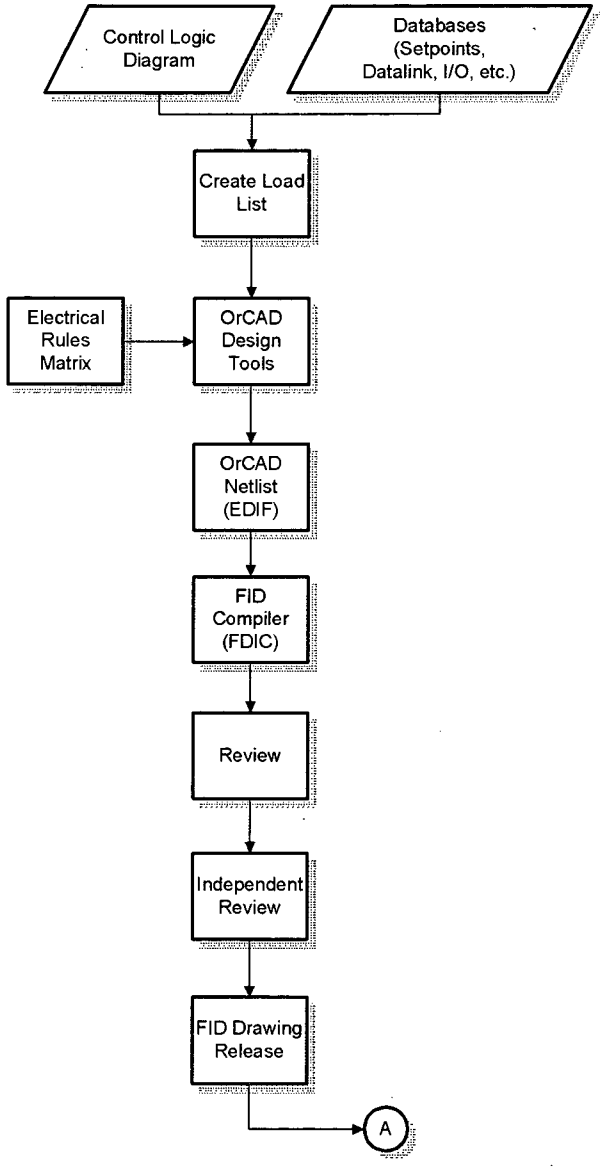
- Graphical Representation of Logic
- Hardware and Network Representation
  - No Connectivity Database Required
- Easy Modification to Control Application
  - Original FID Done by OEM
  - Modifications Made by End-User
    - Configuration Management Responsibility

FIDs

- Provides Configuration Control
  - Documents Each Module
    - Control Logic
    - Network Connectivity
    - Field Terminations
    - Cabinet Wiring
- Control Logic
  - Standard SAMA Logic Symbols
  - Library of Over 100+ Intelligent Symbols

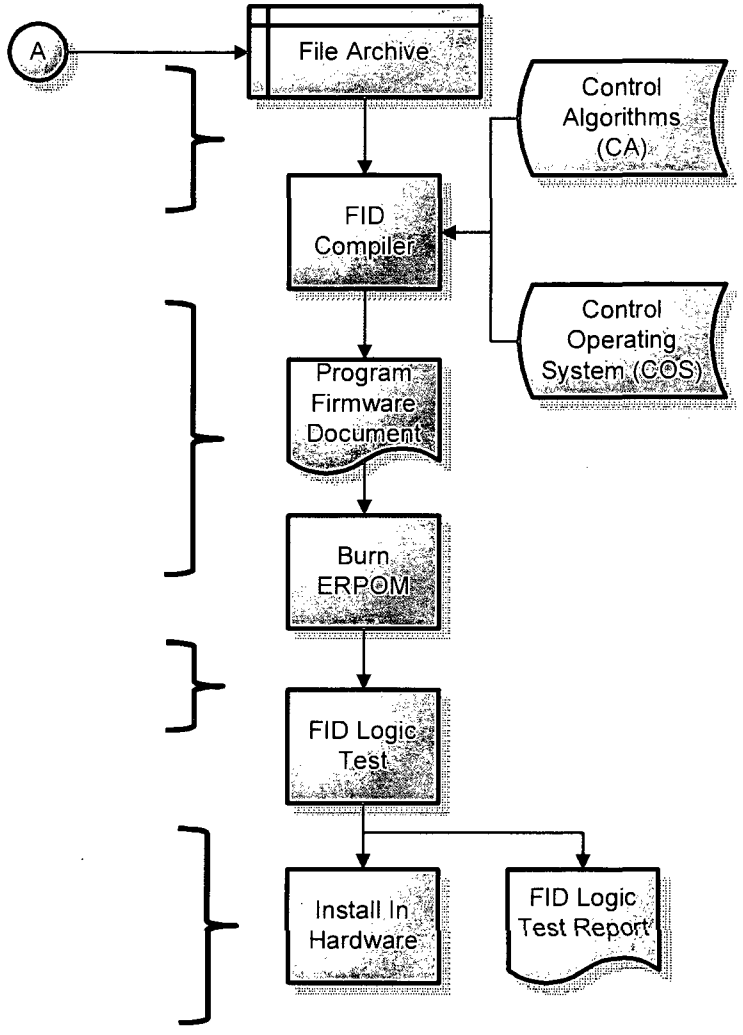
FID PROCESS

- Design
  - Customer I/O Database
    - Load Lists
  - Control Logic Diagrams (CLDs)
    - Typical FIDs
    - Unique FIDs
  - Peer Review
  - Independent Review
  - Release FID



FID PROCESS

- Archive Electronic Files
  - –
- Compile to Binary Files
  - –
  - –
  - –
- Burn EPROM
  - –
- Testing
  - –
  - –



DRS TECHNOLOGIES

FIDs

- Programs Hardware Functionality
  -
  -
  -
    -
    -
  -

TITLE BLOCKS

CONTROL SECTION

- Operator Input / Output
  - –
  - –
  - –

FIELD SECTION

DRS TECHNOLOGIES

MISC PARTS

ANALOG FIELD SECTION

NETWORK SECTION

NETWORK SECTION

- Variables With Initial Values (VWIVs)
  -
  -
  -
    -
  -
    -

NETWORK SECTION

- VWIV Modifiers
  -
    -
  -
    -
  -
    -
  -
    -
  -
    -

LOGIC SECTION

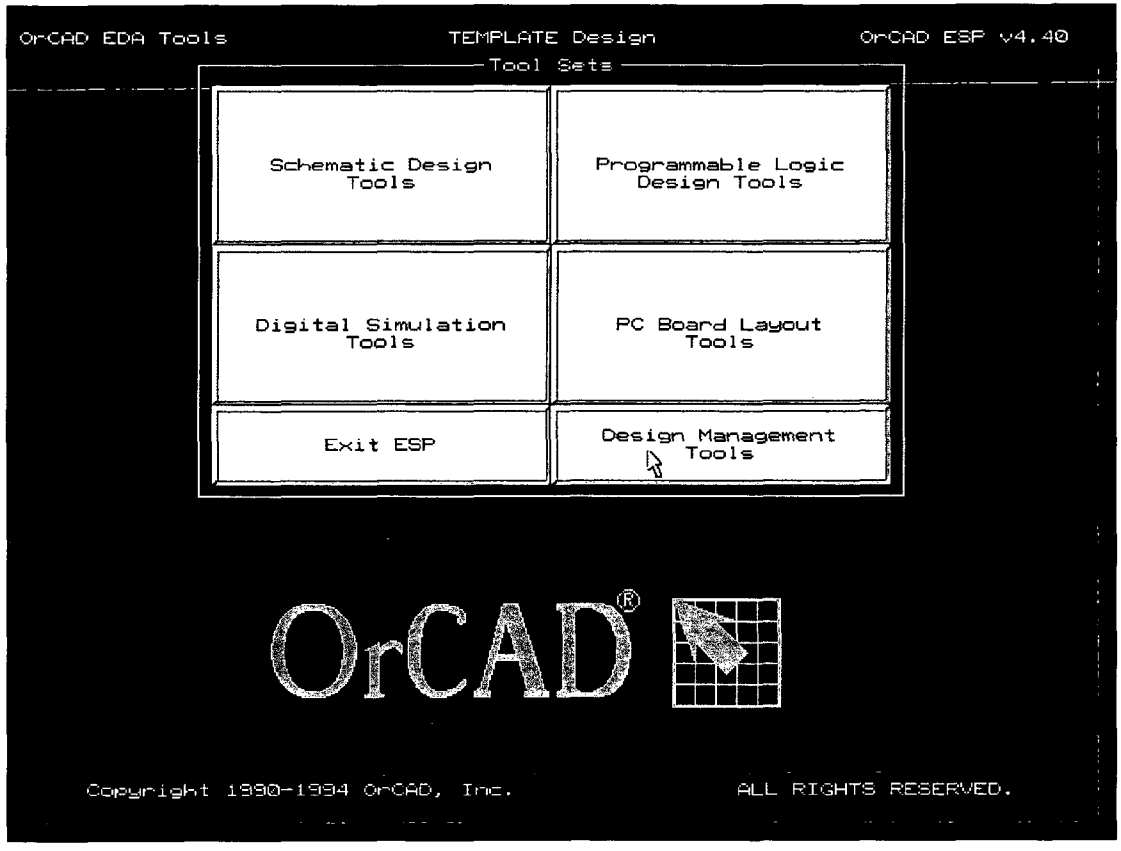
- U? -
  -

LOGIC SECTION

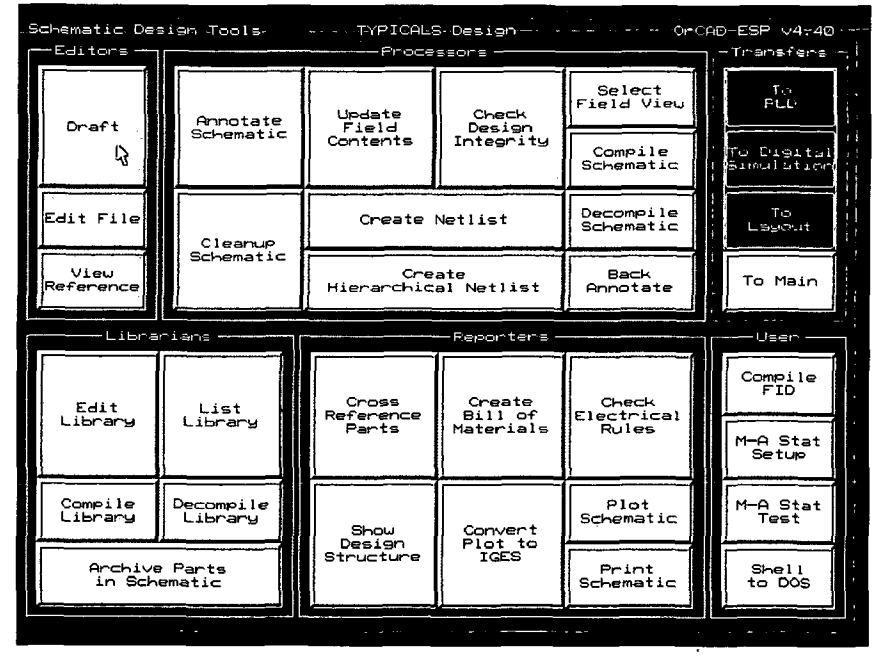
DESIGN TOOLS

- OrCAD
  - Schematic Capture Program
- FID Compiler
  - Netlist to Binary Converter
- EPROM Programmer
  - Program Module EPROMs or Memory Cards

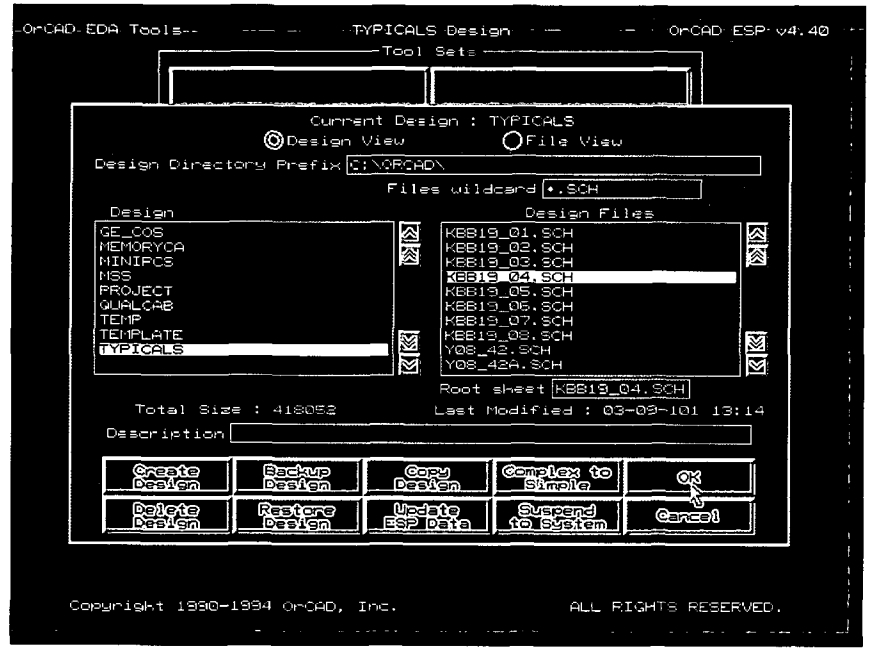
- OrCAD, Schematic Capture Program



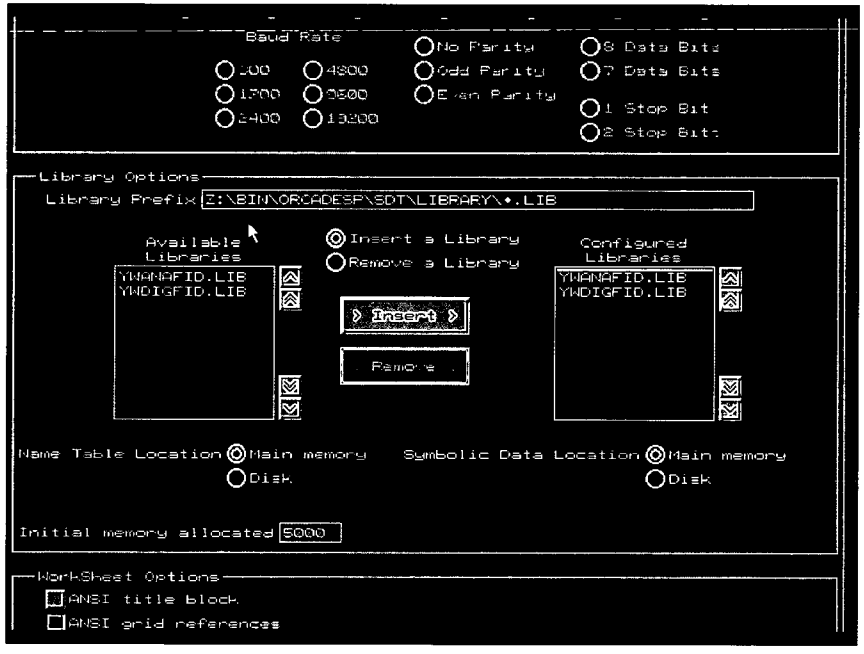
- OrCAD, Schematic Capture Program
  - Design Manager
  - FID Editor
  - Electrical Rules Check (ERC)
  - Netlist Generator
    - Electronic Design Interchange Format (EDIF)



- Design Manager
  - TEMPLATE Design
  - Cabinet Folders
  - Module Selection
    - File Name
    - Date & Time
    - Description
  - Backup Operations



- Library Configuration
  - Analog & Digital
    - Title
    - Hardware
    - Network
    - Logic
  - CDROM Based
    - Z: Drive



- Electrical Rules Check (ERC)
  -
    -
    -
    -
    -

- Electrical Rules Check Continued
  -
  -
  -
  -

FID SUMMARY

- Design Manager
- FID Editor
- Electrical Rules Check (ERC)
- FID Compiler
- EPROM Programmer
- FID Process
- > 5000 Successful Online Installations
  - 5000 More in the Installation Phase

RETURN

DRS Consolidated Controls
PLμS 32 SYSTEM

- Independence
- Redundancy
- Diversity
- Plant Applications
  - Single Loop Control
  - Redundant Loop Control
  - Diesel Generator Sequencer
  - Engineering Safeguards Features

DRS TECHNOLOGIES

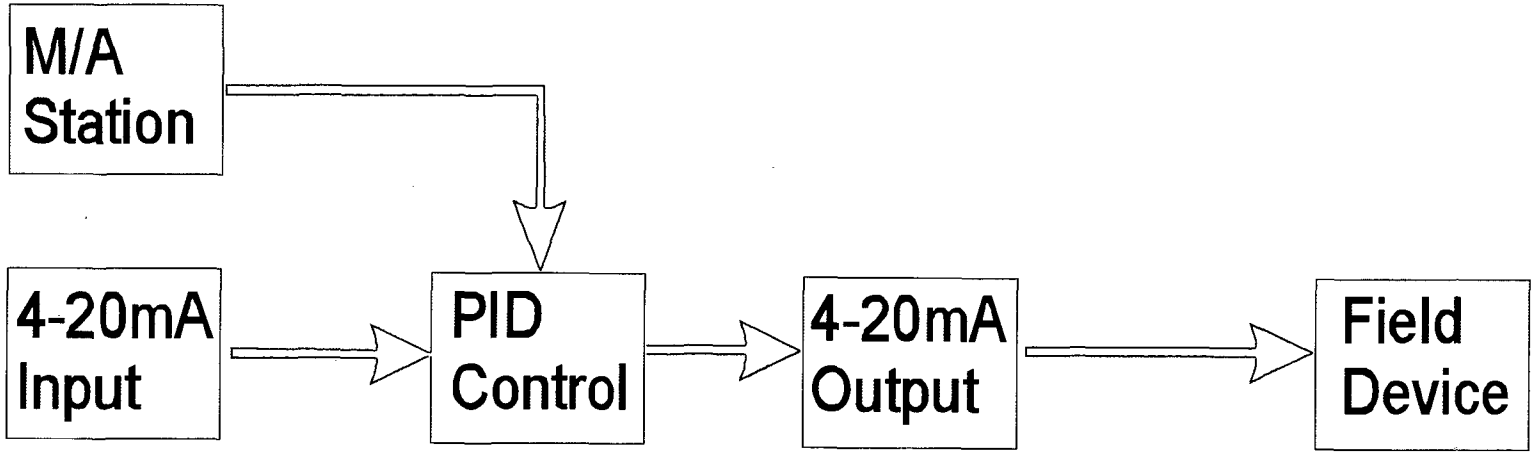
INDEPENDENCE

- Redundant Portions Are Independent
  - Design Of Application Will Influence
  - Redundant Communication Of
    - Network
    - With in Cabinets
- Isolated Signal Paths
  - Fiber Optics Are Used Between Cabinets And Channels
- Separate And Isolated Power Supplies For Sections Of Control Module
- Single Failure In Most Cases Will Not Prevent A Division For Performing It Safety Function

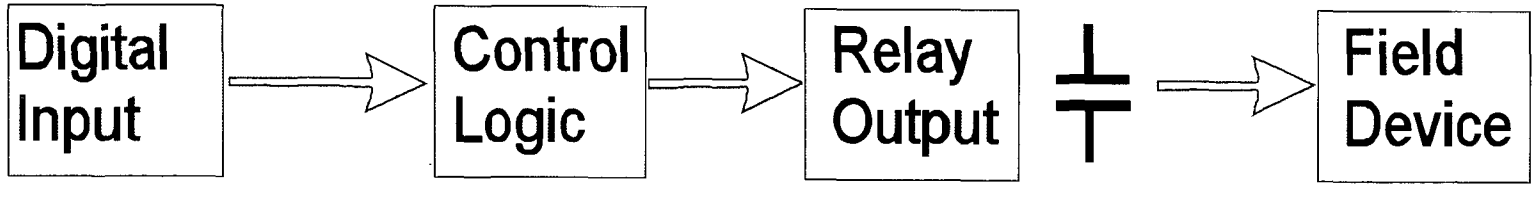
DIVERSITY AND DEFENCE IN DEPTH

- Implemented by Echelons of Defense
  - Each Level has Different Hardware Vendor
    - Insuring Different HW and SW Design Teams
  - High Quality Software and Hardware
    - Reduces Failure Probability
- Evaluated on a Plant by Plant Basis
- Each Level is Independent and Isolated
- DRS has Experience Working with Various Hardware Vendor to Implement
  - Working Alliance With RTP

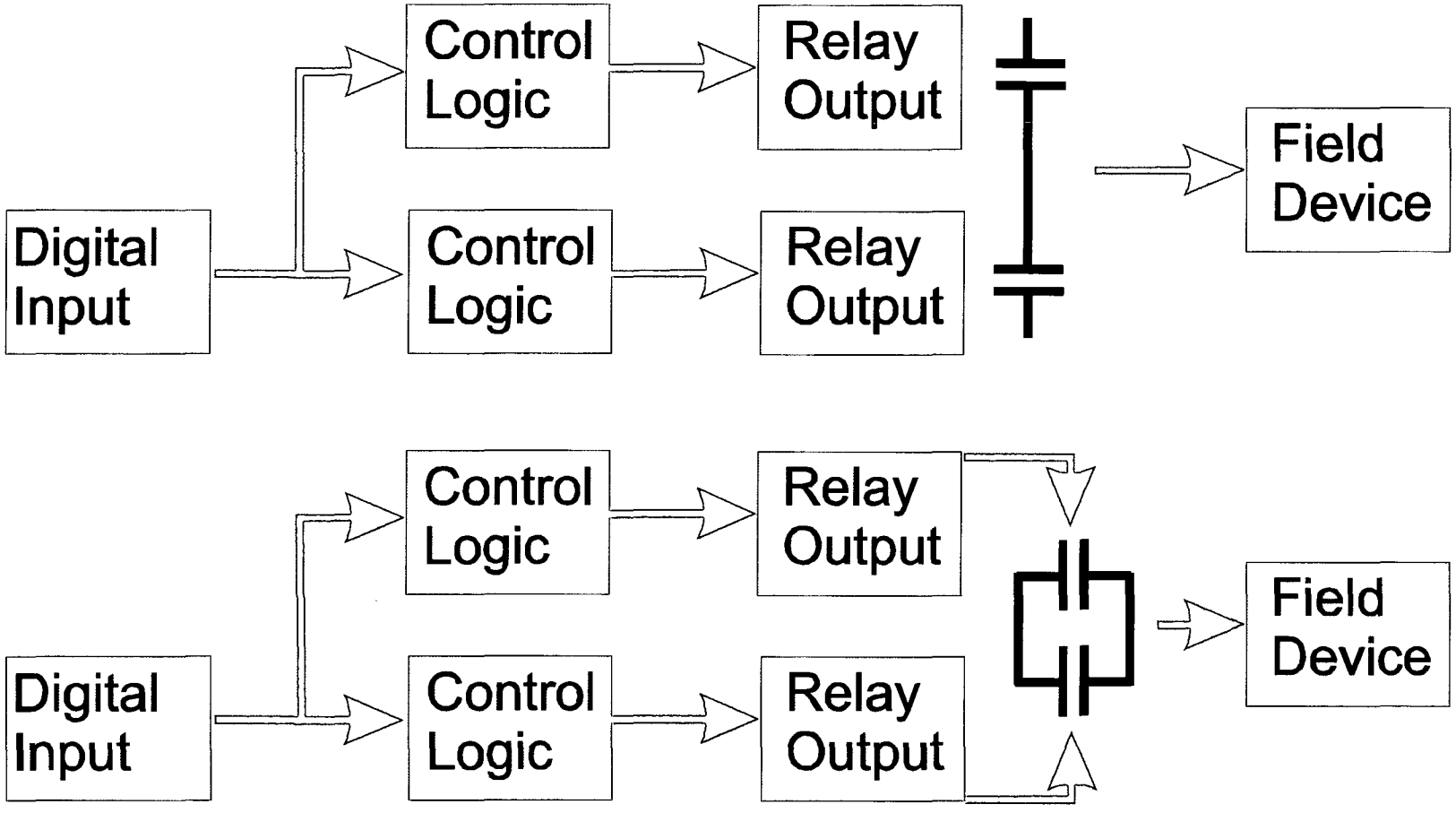
Analog Control Module



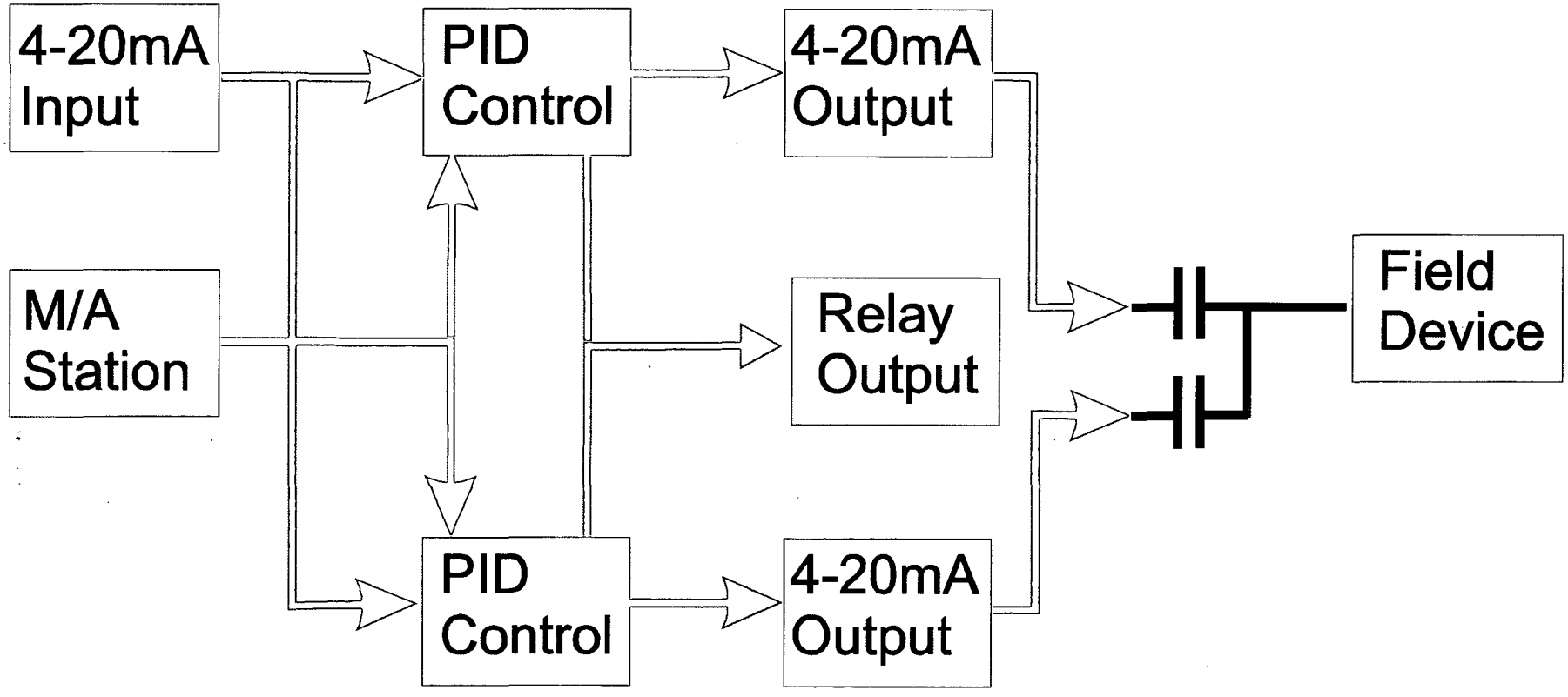
Digital Control Module



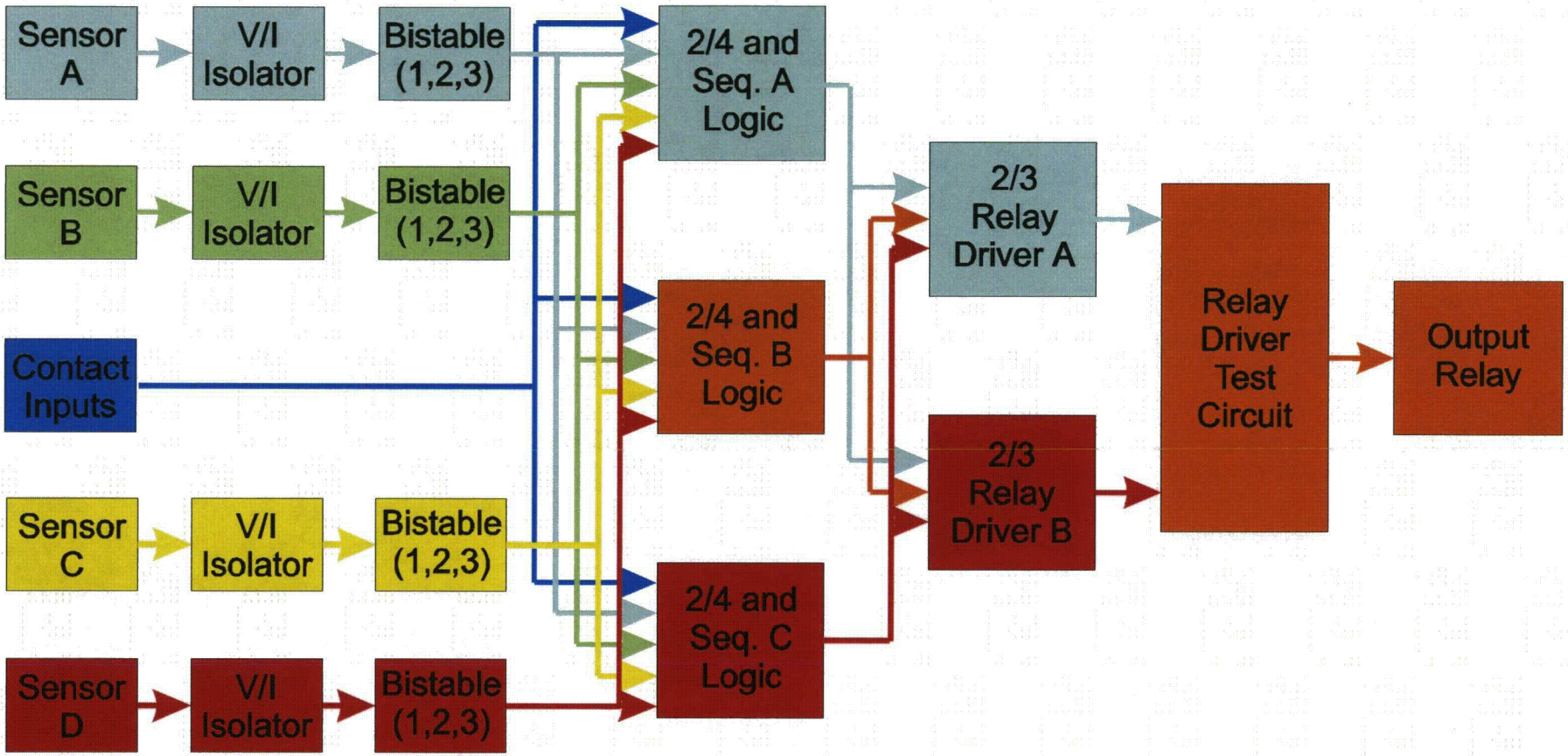
Redundant Digital Control Module



Redundant Analog Control Module



DIESEL GENERATOR SEQUENCER



DRS TECHNOLOGIES

System Overview

DRS TECHNOLOGIES

Typical Communication Interface

ENGINEERING SAFEGUARDS FEATURES

DRS TECHNOLOGIES

ESF Inputs

ENGINEERING SAFEGUARDS FEATURES

ESF Logic and Outputs

ENGINEERING SAFEGUARDS FEATURES

DRS TECHNOLOGIES

ESF Trip Logic

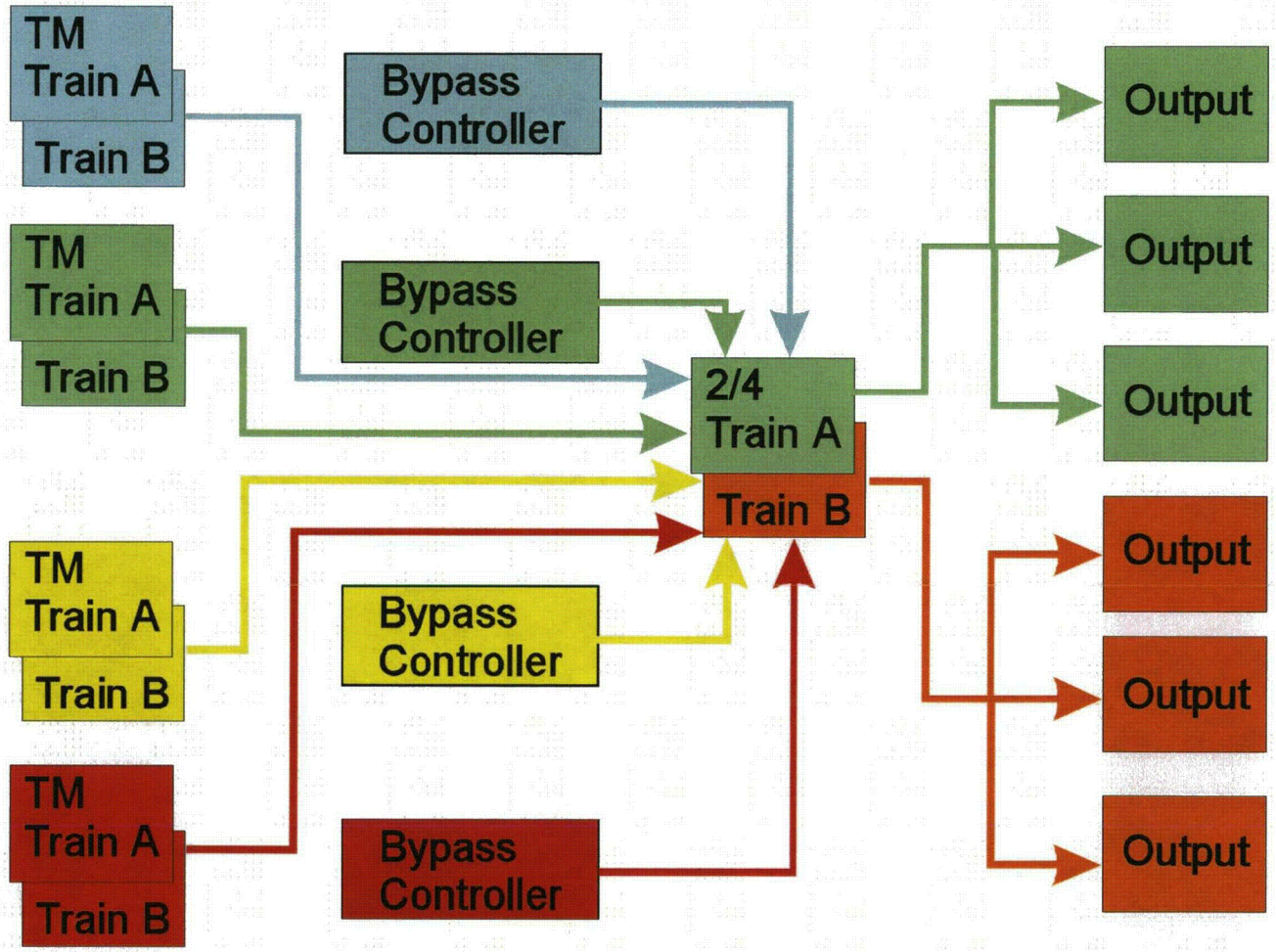
ENGINEERING SAFEGUARDS FEATURES

ESF Channels

ENGINEERING SAFEGUARDS FEATURES

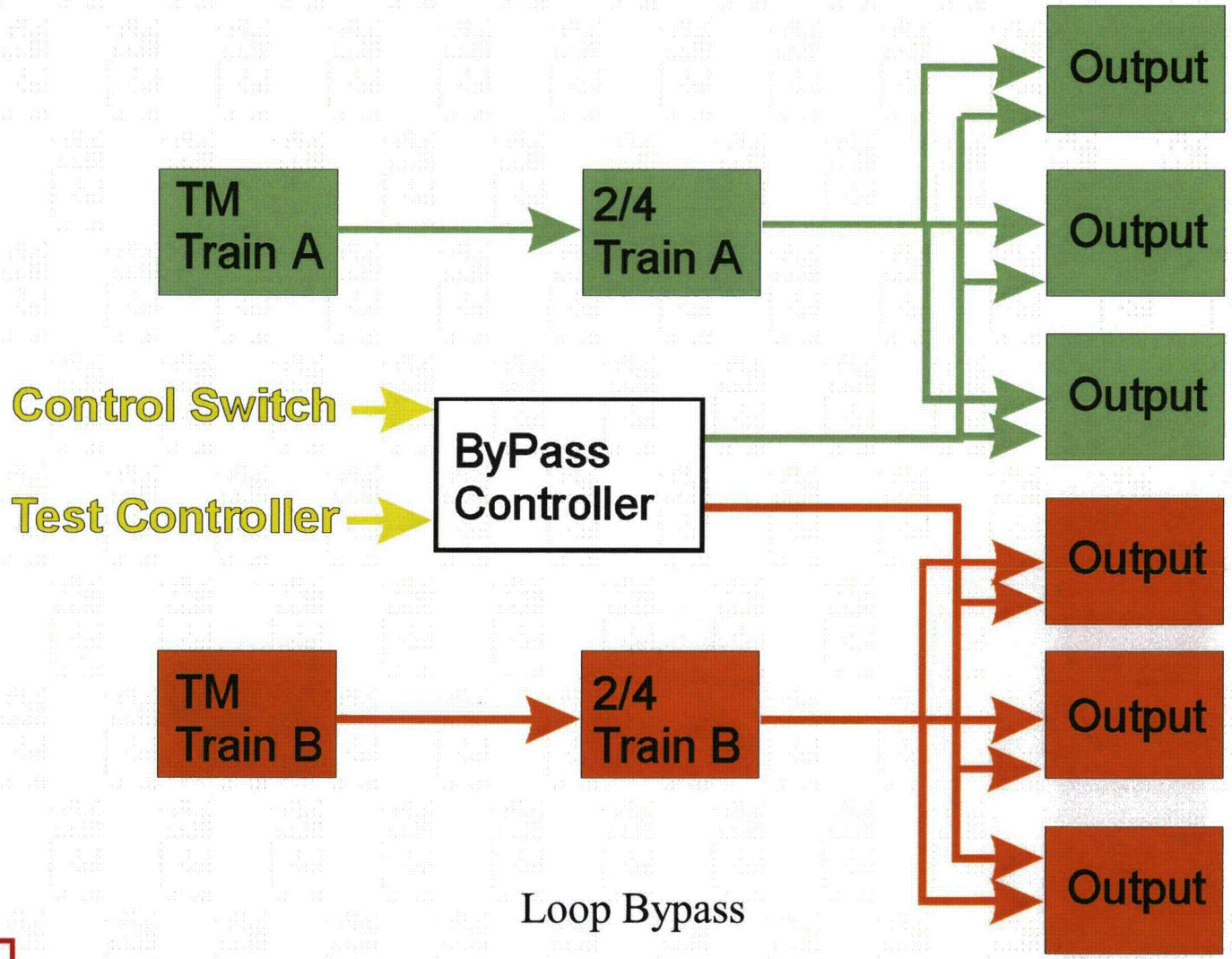
ESF Inter-Connections

ENGINEERING SAFEGUARDS FEATURES



Sensors Bypass

ENGINEERING SAFEGUARDS FEATURES



Loop Bypass

RETURN

DRS Consolidated Controls

PLμS 32 SYSTEM

Class 1E Qualification Program

DRS TECHNOLOGIES

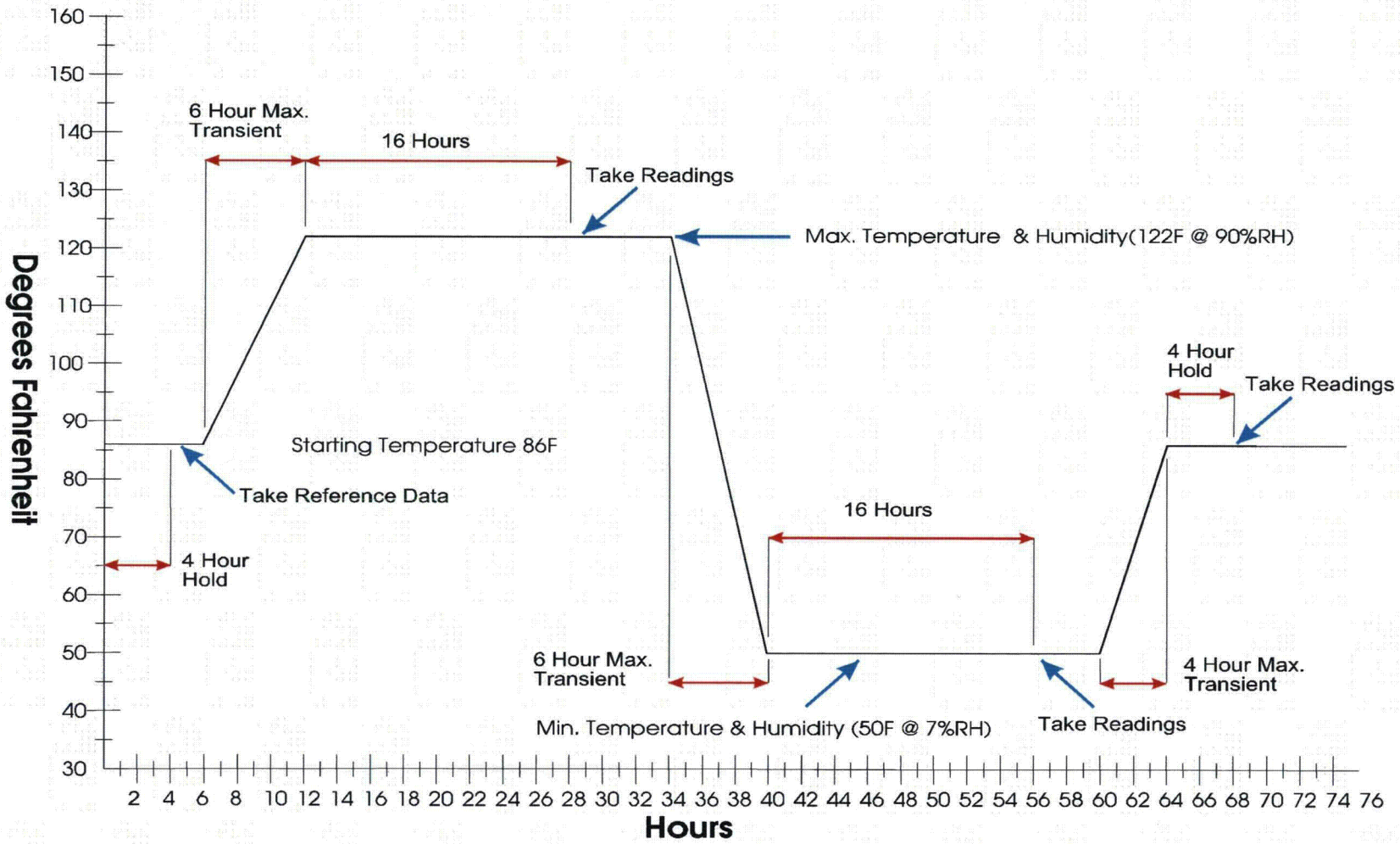
ENVIRONMENTAL QUALIFICATION

- The Unit Under Test (UUT) consisted of an RMU cabinet, an SSLC/TEST cabinet and a VDU
- At all times the UUT was energized and monitored while subjected to the following:
  - ENVIRONMENTAL QUALIFICATION - MILD IEEE-323
  - SEISMIC QUALIFICATION - IEEE-344
  - EMI/RFI QUALIFICATION:
    - TEST METHODS: MIL-STD-461D
    - ACCEPTANCE METHODS: EPRI-TR102323 R1

ENVIRONMENTAL QUALIFICATION

- UUT Installed inside Walk - In Chamber
- UUT Powered & Functionally Tested
- Installed T/C in 20 Selected Locations to Monitor Temperatures
- Walk - In Chamber's Computer Programmed For the Environmental Profile Soaks
- UUT Monitored During Entire 76 Hour Profile by Automated Data Log Recording, and by DRS & Lab Personnel at the start/end of each Temperature/ Humidity Transition
- Performed Baseline Functional Test
- UUT Subjected to Environmental Soak - Profile
- Increase and/or Decrease in the Environmental Profile Was Linear Over a Duration of Time
- Performed Post Functional Test

ENVIRONMENTAL QUALIFICATION PROFILE



SEISMIC QUALIFICATION

- Performed Inspection & Baseline Functional Test
- UUT Mounted on Tri-Axial Shaker Table
  - Placed Tri-Axial Accelerometers in Selected Locations
  - UUT Energized & Monitored at all times
- Resonant Frequency Search Test
- Visual Inspection (After Each Test)
- Steam Relief Valve (SRV) Dynamic Loads (40)
- Operational Basis Earthquake (OBE) (5)
- Safe Shutdown Earthquake (SSE) (1)
- Chugging Vibration (LOCA) Load (40)
- Final Inspection & Functional Test
- Performed Inspection & Baseline Functional Test

SEISMIC QUALIFICATION

- VDU Mounted on Tri-Axial Shaker Table
  - Placed Tri-Axial Accelerometers in Selected Locations
  - UUT Energized & Monitored at all times
- Resonant Frequency Search Test - Non Seismic
- Visual Inspection (After Each Test)
- Operational Basis Earthquake (OBE) (5)
- Safe Shutdown Earthquake (SSE) (1)
- Final Inspection & Functional Test

EMI / RFI Qualification

- Test Methods are In accordance with MIL-STD-461D
- Acceptance Methods are in accordance with EPRI TR102323 R1
- As Applicable; Test Levels, EPRI Levels, v. MIL-STD Levels Are Shown in The Same PLOT
- Performed Functional Test After Each of the Following Tests:
  - Test Method CE101: Conducted Emissions (Power Leads, 30Hz to 50kHz)
  - Test Method CE102: Conducted Emissions (Power Leads, 50kHz to 400 MHz)
  - Test Method RE101: 30 Hz to 100 kHz Radiated Emissions, Magnetic Fields
  - Test Method RE102: 10kHz to 1GHz, Radiated Emissions, Electric Field

EMI / RFI QUALIFICATION

- Test Method CS101: 30kHz to 50kHz, Conducted Susceptibility, Power Leads
- Test Method CS114: 50kHz to 400MHz, Conducted Susceptibility, Cables
- Test Method RS101: 30kHz to 100kHz, Radiated Susceptibility Magnetic Field
- Test Method RS103: 10kHz to 1GHz, Radiated Susceptibility, Electric Field
- Test Method IEC 801-2: Electrostatic Discharge
- Test Method IEC 801-4: Electrical Fast Transient/Burst
- Test Method IEC 801-5: Surge Immunity Test

RETURN

DRS Consolidated Controls

PLµS 32 SYSTEM

Cyber Security

DRS TECHNOLOGIES

Cyber Security

DRS TECHNOLOGIES

Development Cyber Security

Development Cyber Security
Wide Area Access

Development Cyber Security
Local Access

Development Cyber Security
Development Share Access

Development Cyber Security Release Repository Access

-
-
  -
  -
-
  -
-

Product Cyber Security

DRS TECHNOLOGIES

RETURN