UNITED STATES
NUCLEAR REGULATORY COMMISSION
TECHNICAL TRAINING DIVISION

DIGITAL INSTRUMENTATION & CONTROL TRAINING

E-114

UNITED STATES
NUCLEAR REGULATORY COMMISSION
TECHNICAL TRAINING DIVISION

COURSE MANUAL DIGITAL I&C TRAINING (E-114)

This manual is a text and reference document for the Digital Instrumentation & Control course. It should be used by students as a study guide during attendance at this course. This manual was compiled by Altran Solutions under USNRC Technical Training Center contract NRC-38-07-390.

The information in this manual was developed or compiled for NRC personnel in support of internal training and qualification programs. No assumptions should be made as to its applicability for any other purpose. Information or statements contained in this manual should not be interpreted as setting official NRC policy. The data provided are not necessarily specific to any particular nuclear power plant, but can be considered to be representative of the vendor design.

LIST OF EFFECTIVE REVISIONS

Module	Revision
1.0	20070905
2.0	20070905
3.0	20070905
4.0	20070905
5.0	20070905

TABLE OF CONTENTS

LIST OF FIGURES

1.0 COURSE INTRODUCTION

Welcome to the Digital and Microprocessor Control Systems Course!

This course addresses the latest developments on the use of software based equipment on nuclear plant applications. This has become increasingly important as plants move into license renewal, and in consideration of obsolete equipment replacement upgrades. This course will provide a perspective on the guidelines and requirements of the Nuclear Regulatory Commission, Electric Power Research Institute as well as industry, consensus standards organizations and plant specific experience.

Upon completion of this lesson the student will have acquired the knowledge level necessary to understand the technical and regulatory fundamentals of digital system design, installation, licensing and operations and the key differences between digital and analog equipment/systems in terms of their complexity, failure modes, assessment methods, and licensing issues and how they apply to nuclear power plant operation.

The course is divided into five modules or course sections that encompass approximately one day each, although some are longer or shorted based on the amount of information that needs to be addressed. The five modules are:

- MODULE 1 – Introduction and Overview
- MODULE 2 – Architecture Overview
- MODULE 3 – Regulatory Concerns
- MODULE 4 – Qualification
- MODULE 5 – Software/Firmware Lifecycle Concepts

Each of these modules will be covered with a detailed review of the major elements in both slides and review of text references, where applicable. A full outline of these is included in Figure 1-1, Figure 1-2, Figure 1-3, Figure 1-4 and Figure 1-5

At the end of each day, a review of the day and Q&A session will be conducted to address concerns and additional information needed by the students. If the instructors don't have the information handy, an assignment to follow-up and provide the students with the information will be taken and provided sometime during the week.

Module 1 Introduction & Overview:

Module 1 is the first of five modules in the Digital Instrumentation & Control Training Course. The purpose of this module is to assist the trainee in understanding the subjects to be covered this week in each of the five modules and to address the reasons why digital systems are being introduced in nuclear power plants and to see some examples of actual upgrades.

Learning Objectives

After completing this module, you should be able to:

1. Explain the importance of instrumentation issues to safety analysis
2. Be able to state what are the major issues in digital safety system analysis and approval by NRC
3. Explain, in general terms, the general format for NRC review of digital systems using the SRP and all associated guidelines and standards from NRC and industry.
4. Be able to provide an overview of digital system failures that have occurred and the root cause of their failure.

5. Explain the process for digital I&C upgrade following the roadmap developed by NRC and industry
6. Provide an overview of the various stages of the modification process followed for both hardware and software in completing the upgrades to new digital systems.
7. Provide an overview of the regulatory delta between existing and new reactor licensing and the details of requirements to be reviewed in any new reactor licensing for instrumentation and controls.

1.1 Introduction and Overview

The purpose of this module is to provide an overview of the course and to describe why instrumentation issues are important to safety analysis for nuclear power plants. The objectives of this module are to address the main issues of:

- Importance of Instrumentation Issues to Safety Analysis
- Digital Safety System Issues
- NRC SRP Update Process
- EPRI I&C Programs
- References

The basis of the defense in depth design philosophy is addressed from 10 CFR 50, including explicit definition of the three barriers. Figure 1-4 shows the impact of the safety analyses on plant operations and documented in the Technical Specifications.

10 CFR 50 defines the technical basis for instrumentation and control acceptance criteria in the following sections:

- General Design Criteria (GDC) in Appendix A of the Code of Federal Regulations (CFR), Title 10 , Part 50
  - establish high level minimum requirements and principal design criteria which
  - address design, implementation, construction, testing, and performance requirements
  - apply to structures, systems, and components important to safety
- 10 CFR 50.55a (h)
  - addresses the design of I&C systems performing safety functions
  - incorporates IEEE 603/IEEE 279
  - involves design bases, redundancy, independence, single failures, qualification, bypasses, status indication, and testing
- Appendix B of 10 CFR 50 establishes Quality Assurance (QA) requirements

Plants are converting from analog to digital for a variety of reasons including the following:

- Analog systems are experiencing excessive drift because of aging
- Vendors are discontinuing analog product lines
- Difficulty in obtaining product support for existing systems
- Some plants want to take advantage of digital system flexibility

We show examples of older and now newer designs of plant control rooms – provide different challenges to the reviewer in that much more emphasis on digital platforms is required.

We have learned by example from other safety critical industries such as:

- Federal Railroad Administration

- Federal Aviation Administration
- Power grids
- Foreign nuclear power agencies
- Chemical industry
- NASA

The major I&C systems subject to review by the NRC are listed below, based on sections in the NRC Standard Review Plan:

- Protection Systems
- Engineered Safety Features Actuation Systems (ESFAS)
- Safe Shutdown Systems
- Information Systems Important To Safety
- Interlock Systems Important To Safety
- Control Systems
- Diverse I&C Systems (e.g., Anticipated Transient Without Scram [ATWS] mitigation system)
- Data Communications Systems
- Essential Auxiliary Supporting Systems (e.g., heating ventilation, and air conditioning [HVAC] systems)

A number of plants have attempted digital modifications under 10 CFR 59 over the past number of years. These include:

- Haddam Neck – Full RPS/ESFAS changeout
- D.C. Cook - Signal conditioning portion of RPS/ESF
- Zion – Signal conditioning/process sense portion of RPS/ESF

Also, a number of plants have requested prior staff review as follows – just as examples:

- Watts Bar – RTD bypass
- Sequoyah – RPS/ESF signal conditioning/process sense
- Diablo Canyon Power Plant– RPS/ESF signal conditioning/process sense
- Turkey Point – EDG sequencer
- Haddam Neck – AFW control
- South Texas – QSPDS
- ANO2 – Core Protection Calculator

The key issues in the early plant upgrades include:

- Licensing was seen as problematic
- Concern about new characteristics and failure modes
- Utilities and Regulators were adjusting processes to accommodate digital issues
- Work was needed to establish a consensus approach

In 1995, based on ACRS recommendations, the NRC staff undertook a task to update NUREG 0800 Standard Review Plan (SRP) Chapter 7 (completed in 1997) to address lessons learned in digital upgrades to date. The SRP was updated again in 2007. The objectives of this update included:

- Maintain Regulatory Basis
- Incorporate lessons learned – ALWR reviews
- Incorporate lessons learned – Retrofits
- Incorporate operating experience
- Describe criteria for Retrofits and ALWRs
- Update for latest standards referencec

This set of changes, basically involved no fundamental changes to the SRP but format changes to support additional guidance as follows:

- General Requirements and Guidance in Section 7.1
- Adds References to new Regulatory Guides and BTPs on Digital Issues
- Highlight Review Areas, Acceptance Criteria, and Review Process for Digital Systems
- Add discussion of Standard Plant Reviews
- Add References to digital systems guidance

Three new SRP Sections were added and three appendices were revised in 1997 as follows:

- 7.0 – Introduction
- 7.8 – Diverse Actuation (ATWS and Diverse Backup)
- 7.9 – Data Communication
- 7.0-A – Describes process for Digital Reviews
- 7.1-C – Describes IEEE 603 review
- 7.1-A – Addresses Part 52, Revision to Part 50 and new Regulatory Guides

A number of new Branch Technical Positions on specific areas of focus were developed and included in the SRP, as follows:

- Software Reviews – BTP-14
- Defense in Depth and Diversity – BTP-19
- Real Time Performance – BTP-21
- On-Line and Periodic Testing – BTP-17
- Design Certification – BTP-16
- PLCs – BTP-18
- Non-Digital Topics – BTP 10,11,12 & 13

Figure 1-6 provides a comparison of the criteria that the SRP Chapter 7 provides on the major focus areas in digital upgrades.

Also, six new NRC Regulatory Guides were established as follows:

- R.G. 1.168 – Verification, Validation Reviews and Audits (IEEE 1012 & 1028)
- R.G. 1.169 – Software Config. Mgmt (IEEE 828 & 1042)
- R.G. 1.172 – Software Requirements Spec. (IEEE 830)
- R.G. 1.170 – Software Test Documentation (IEEE 829)
- R.G. 1.173 – Software Life Cycle (IEEE 1074)
- R.G. 1.171 – Software Unit Test (IEEE 1008)

Figure 1-7 provides an overview of an example of the new Regulatory Guide 1.173 and the associated IEEE 1074, and how they address the basic framework for life cycle processes.

The SRP was again updated in 2007 with the following changes:

- Added Section 7.1-D – IEEE 7-4.3.2-2003
- Updated to conform with latest standards referenced (IEEE 7-4.3.2,
- Used new terminology for “auxiliary supporting features” per IEEE 603-1991
- Deleted reference to Reg Guide 1.153 - now covered by 1999 version 10 CFR 50.55a(h)
- Updated for EMI/RFI – Reg. Guide 1.180
- Added reference to Reg. Guide 1.204
- Added ITAAC/DAC criteria and Reg Guide 1.206

The revised SRP provides significant benefit to both the industry and the NRC as follows:

- No impact on existing systems
- SRP and Regulatory Guides are Guidance Only

- Developers will benefit from known acceptance approaches to designing digital systems

For license amendment applications, the following guidance is provided in the SRP update:

- Selected portions will be used
- Depth of review depends on safety significance and complexity
- Only review differences from previously approved designs
- Defense in Depth and Diversity applicable to RPS and ESFAS only

An example is provided in Figure 1-8 through Figure 1-16 to address the NRC document requests for Oconee License Application Request (LAR) vs. normal document availability (all submitted at one time). These figures cover all of the life cycle phases from project definition to operations and maintenance.

There are significant areas of interest in NRC Research to address the major focus areas that are needed to address all aspects of licensing digital upgrades.

An example listing of the main focus areas receiving attention in NRC Research today are included in the following:

- EMI/RFI Qual.
- Environmental Qual.
- Lightning Protection Guidelines
- Requirements Assessment
- Diagnostic and Fault Tolerance
- Operating Systems

A complete review of the ongoing work in NRC Research will be covered in Module 3 – Regulatory Concerns.

The Electric Power Research Institute (EPRI) is also heavily involved in developing guidelines as a standard roadmap for digital upgrades. The utility goals for digital upgrades include the following:

- Maximize plant capacity/output levels
- Achieve and maintain high reliability
- Achieve and maintain high availability
- Maintain high levels of safety
- Maintain high levels of operator awareness of plant and equipment states
- Minimize the likelihood of human errors
- Integrate fault tolerance and fault recovery into systems (from both human and equipment errors/failures)
- Use commercially available products

The utility goals for digital upgrades are also based on the expanded use of digital technology capabilities, which include:

- Process large data volumes
- Data validation techniques
- Extensive diagnostic capabilities
- Integrated diagnostic and predictive algorithms
- System based early fault detection
- Intelligent displays, e.g. alarm filtering
- Operations/maintenance/engineering advisory systems
- Automated processes
- Electronic procedures with information and control
- Multi-media capabilities

The implementation using digital systems will introduce a set of secondary issues as follows:

- Radiation sensitivities
- Reliability and availability concerns

- Materials issues
- Maintenance issues
- Learning curve for people

Next, we will review a few digital failures that have occurred over the past number of years in the non-nuclear and nuclear arena. They are addressed in the slides in Section 1.1 as well as in the handouts at the back of the section.

For nuclear related implementation, the set of documented failures, noted by the NRC is shown in Figure 1-17 and Figure 1-18**.** These provide the categories and quantities of failures documented in LER's reviewed by the NRC from licensees from 1990 to 1993, as an example.

Additional new failure data is provided in Section 1.2 of this course.

Next, we review a set of references from EPRI, NRC and industry to address all aspects of digital upgrades. Many of these references will be addressed in detail during the course.

Finally, we review the need for digital upgrades, with a quote from Amir Shahkarami, Exelon Senior Vice President, in Figure 1-19 and the organization of the NRC-Industry Technical Working Groups (TWG) and their progress to date.

1.2 Lessons Learned

The purpose of this section is to review a number of nuclear power plant digital upgrades that have been installed and have not performed as expected.

First, a review of the failure data from various sources is reviewed. Then examples from Licensee Events Reports that addressed digital system failures are analyzed. These involved both hardware and software failures. Recent examples include the Palo Verde Core Protection Calculation (CPC) event in Figure 1-20 and Figure 1-21and the TVA Browns Ferry Unit 3 data storm in Figure 1-22 through Figure 1-24.

The following systems are reviewed in the slides included in Section 1.2:

- Digital Radiation Monitoring Upgrade
- Digital Feedwater System Upgrade
- Digital Annunciator System Upgrade
- Digital Turbine Control System Upgrade

The moral of these stories is as follows:

- Even a Watchdog Can Bite Its Owner
- Just Because They Installed It Before You Doesn't Mean They Looked First
- Just Because Their System Hasn't Crashed Doesn't Mean Your System Won't
- If You Look Before You Leap, You Can Save Yourself a World Of Hurt

1.3 Digital I&C Upgrade Process

1.3.1 Digital I&C Upgrade Process

The purpose of this section is as follows:

- Provide background and a brief history of digital I&C upgrades and associated regulatory issues
- Explain the importance of "process" when implementing digital upgrades
- Show that any modification involves development, evaluation and control processes

The objectives for the student that we will address as part of this section are to:

- Understand why processes are important for digital upgrades
- Discuss the types of processes involved in a digital I&C modification
- Explain how computer and software related processes relate to traditional processes in nuclear plant modifications

This section provides a review of the history of digital system upgrades, from a regulatory perspective, since the late 1980's: The digital I&C upgrade process guideline from EPRI was developed to provide a roadmap, following the issue of the NRC Standard Review Plan (SRP).

The major issues identified in the digital I&C upgrade process are:

- Use of software and potential for software common cause failure
- Effects of electromagnetic interference (EMI)
- Use and control of equipment for configuring computer-based systems
- Commercial dedication of digital equipment that includes software

Figure 1-25 provides an overview of the digital upgrade process from the proposal stage thru the operations stage.

The NRC has been very active in support of development of the roadmap for digital upgrades including the following:

- Worked with ALWR Program and vendors to approve ALWR designs
- Commissioned U.S. National Research Council Study on Use of Digital I&C
- Prepared Regulatory Guides endorsing IEEE Standards
- Revised Standard Review Plan
- Developed Revision 4 to NUREG-0800, Standard Review Plan, Chapter 7 (I&C)
- Performed research and developed NUREG reports
  - Use of high-level languages NUREG/CR-6463
  - Adequacy of digital sampling rate and other performance concerns NUREG-1709

Figure 1-26 provides and overview of the influences on digital upgrade process that relate to the development of and consensus with the roadmap applied to the digital process. While the incorporation of the separate elements seems complex and intensive process – it is really common sense and what we are already doing today.

Figure 1-27, Figure 1-28, Figure 1-29, Figure 1-30 and Figure 1-31 provide an overview of the IEEE 1012 life cycle process for software as it is incorporated with TR-102348. The fundamental conclusions of this entire discussion on process is that, while complex in the incorporation into digital upgrades, the process has been defined and followed in many cases, successfully by licensees with NRC oversight.

Lastly, we review the organization and progress made by the NRC TWGs related to the modification and design review process in Figure 1-32 through Figure 1-34.

1.3.2 Digital Modification Process

The purpose of this section is to focus on the major elements in the development process for digital upgrades, from the overall modification process to

development of the digital system, platform, hardware and software.

The objectives of this section are as follows:

- Identify the basic design and development processes used in a digital I&C modification
- Explain the relationship between the various processes

Figure 1-35 provides an overview of the digital modification process as regards the platform vs. application. The platform is assembled based on hardware, software and human-machine interface functions all combined.

Figure 1-36 provides an overview of various options in completing the upgrade process as regards digital systems. There are many options for the integration of platforms with plant specific features.

1.3.3 Digital Delta

The purpose of this section is to define the important differences between analog and digital I&C systems. The objectives are as follows:

- Identify some key differences between analog and digital equipment
- Identify personnel skills needed to understand, evaluate and apply digital equipment

It is important to define "digital equipment" as follows:

- For the purpose of this course (and the EPRI source documents), "digital equipment" means equipment involving a computer of some kind
  - Typically microprocessor based
  - Often referred to as "programmable digital" to distinguish from fixed logic

The wide range of equipment that is comprised by digital equipment is:

- Digital relay
- Digital meter
- Smart transmitter
- Recorder
- Embedded controller
- Standalone single-loop controller
- Programmable logic controller (PLC)
- PC
- Data acquisition and monitoring system
- Distributed control system (DCS)

There are some key differences between digital and analog systems and how they perform safety functions as follows:

- How signals are processed
- Internal complexity including software
- Human-machine interfaces
- Types of reviews and materials to be reviewed when:
  - Evaluating acceptability of the equipment
  - Troubleshooting problems
  - Making changes

There are also important differences in how the systems operate in regards to operation:

- Testing by itself is not enough
- Development process is important
- Failure modes are different
  - Subtle and unexpected behaviors and failure modes

- More severe, difficult to predict consequences

In summary, for comparison of analog and digital systems for upgrades:

- Digital can be a very good solution
  - Only solution for long-term improvements
- Isn't always the right solution
- Needs to be evaluated properly and costs well understood
- Will become less costly to implement as it is more widely used and accepted

1.4 Applications[1]

The objective of this lesson is to discuss real-world examples of how microprocessor devices are already finding their way into nuclear power plants. The applications that will be explored are:

- Reactor Protection & Engineered Safeguards
  - Siemens/Framatome Teleperm XS Platform
  - Typical for Oconee
- Main Turbine Control
  - Main turbine control system upgrade at Diablo Canyon
- Feedwater Pump Speed Control
  - Feedwater pump speed control system upgrade at Diablo Canyon
- Protective Relays
  - General discussion
- Power Converters
  - General Discussion
- Variable Speed Drives
  - General discussion

1.4.1 Reactor Protection & Engineered Safeguards

Three digital I&C systems have received Safety Evaluation Reports (SER) from the USNRC documenting their acceptability for use in Reactor Protection systems (RPS) and Engineered Safety Feature Actuation Systems (ESFAS) applications in US nuclear power plants. These systems are:

- Invensys Triconex TRICON
- Framatome ANP Teleperm XS
- Westinghouse Common Qualified (Common Q) Platform

This lesson will provide a brief overview of the Framatome ANP Teleperm XS (TXS) platform. The TRICON platform will be discussed later. The TXS platform platform was selected for discussion because it is already widely used in Europe for nuclear safety-related applications and appears to be the closest to being applied for RPS/ESFAS applications in the United States. At this time, the Oconee plant has a specific contract for the RPS/ESFAS. The Oconee RPS/ESFAS license amendment was submitted, then subsequently withdrawn, primarily due to submittal quality issues. The license amendment is scheduled to be resubmitted in Fall, 2007. Other US nuclear plants have commitments for the non-safety related Teleperm XP platform.

1.4.1.1 Teleperm XS Platform

The Teleperm XS (TXS) platform was developed specifically for European nuclear safety applications. The platform contains modules that were taken from a commercially available programmable controller

[1] Discussions of vendor systems and existing plant applications are strictly for educational purposes and are not intended to convey any proprietary, technical or licensing information. Altran Solutions Corp, its personnel or its subsidiaries are not responsible nor liable for the accuracy or lack of accuracy of any of these discussions.

(PLC) platform and qualified for the nuclear application. The system software and configuration tools were specifically developed for nuclear safety-related I&C applications. Teleperm XS cabinets are shown in Figure 1-37.

Siemens/Framatome ANP designed the TXS as a solution for upgrading safety I&C systems at nuclear power generating stations. Functional reliability is based on a philosophy of combining failsafe design and fault tolerance. Process-related functions are separated from safety systems. A malfunction or accident in a process system will not affect the safety system.

The system supports distributed multiple computer systems with almost any degree of redundancy. It is scalable to permit development of technical and economically optimized solutions. It provides ability to perform Class 1E analog tasks as well as load shed/sequencing, reactor trip and ESFAS coincidence logic and other discrete functions.

Framatome ANP provides system platforms for all I&C tasks to be implemented in a nuclear power plant. Use of the TXS platform for safety applications and the TXP platform for operational functions is illustrated in Figure 1-38.

The TXP platform is oriented to automation of non-safety related I&C functions. These include open and closed loop control of NSS, BOP, Main Turbine as well as the human machine interface (HMI). The TXS is designed for safety related applications; typically, the Reactor Protection System and Engineered Safety Features Actuation System.

As shown in Figure 1-38, there are two interfaces between the safety and non-safety systems:

1. Data Transfer

Data transfer is handled by gateway computers that provide a communication bridge that implements a TXS interface on the safety side and a third party interface on the non-safety side. Gateways are available for a variety of commercial platforms and operating systems. The gateways are part of the Monitoring and Service Interface (MSI) shown in Figure 1-39. This view is expanded in Figure 1-40 to show how the safety functions implemented into the TXS platform fit into the plant data hierarchy and also how redundant channels of TXS hardware can be used to implement major safety functions. Figure 1-41 provides a much more detailed view of the TXS architecture, but from a hardware viewpoint, rather than the functional view shown in Figure 1-40.

2. Device Actuation

Actuation of safety-related actuators and devices is handled by special Priority Logic Modules (also known as AV-42 modules) (1E devices) or by relay-based interlocks, shown in Figure 1-38 and Figure 1-39. For these interfaces, the safety command will override the non-safety command.

1.4.1.2 Four-Set, Two Train RPS Architecture

A typical application for the TXS platform in the US market (for Westinghouse PWR reactors) consists of four reactor protection sets and two actuation trains. This is illustrated in Figure 1-42, which expands on a portion of the architecture shown in Figure 1-41.

1.4.1.3 Signal Acquisition, Distribution and Online Validation

Signals acquired by each of the four redundant protection sets are conditioned, and then distributed among the protection sets via fiber optic data links. Thus, the complete set of input data is available to

each of the four protection sets. The Signal Online Validation (SOV) function in each set compares all available data values then defines one representative value to be used for processing in that set.

1.4.1.4 Relay Voting

The four redundant reactor trip signals coming from the four protection sets are connected to relay logic that performs a "2-out-of-four" coincidence function. The voting matrix output is wired directly to the Reactor Trip Breaker (RTB). A relay matrix is provided for the two redundant RTBs.

1.4.1.5 TXS Voter

For ESF actuation, one TXS voter is provided for each ESF train. This arrangement consists of two independent pairs of masters/checkers. Each pair is in a separate subrack with a separate power supply. With this arrangement, random signal failures will only affect half of a voter. The second half of a voter takes control in the event of such a failure. Both master/checker pairs function in synchronous cycles. A single failure will not result in either loss of function or spurious actuation. This functionality is illustrated in Figure 1-44.

1.4.1.6 Monitoring & Service Interface (MSI)

The TXS architecture contains two Monitoring & Service Interface computers, shown in Figure 1-45. These computers provide:

- Information interface to the Main Control Board
- Information interface to the non-1E systems via gateway computers
- Service interface to the complete TXS I&C system (Protection Sets, Voters, MSIs, Gateways).

1.4.1.7 Human Machine Interface

The TXS platform provides the following HMI interface functions:

- Loop controllers

  Analog loop controllers are included for NSSS functions:
  - Reactor Coolant Temperature
  - Neutron Flux
  - Power Distribution
  - Rod Position
- Setpoint Adjustment

  Safety function setpoints usually are not subject to change. Setpoints may be adjusted through the MSI as needed
- Manual Actuation

  Manual actuation is a plant-specific function. The TXS platform can be designed to allow and to detect manual actuations. As needed, automatic safety actions can override manual actions. The AV-42 "Priority Logic Module" used to perform this function is illustrated in Figure 1-46.
- Display of Status and Values

  The TXS platform can provide analog and discrete information to status indicators, recorders and analog meters.
- Data Transfer

  The TXS platform provides an interface for third-party non-1E data processing and archiving functions via the gateway computers. This interface also is used to transfer information from the TXS to the TXP platform.

In addition to the third party interface, data is transferred between the Service Unit and the TXS computers. This data is used for diagnostics, surveillance test and failure tracking rather than permanent operational use.

1.4.2 Main Turbine Control

This lesson will review the Diablo Canyon Main Turbine Control System upgrade. This upgrade replaced the original non-safety Diablo Canyon Digital Electro hydraulic Control (DEHC) computers with a triple-mode redundant control system made by Triconex. The original Westinghouse P2000 computers are shown in Figure 1-47.

The P2000 equipment was replaced due to obsolescence, reliability and maintenance issues. Although the old system was working well, replacement parts were becoming scarce. In addition, the old system had single-failure vulnerabilities that detracted from the needed reliability.

The new system uses Triconex hardware and Wonderware InTouch software for the Human Machine Interface. Wonderware InTouch is a commercial product that runs on a variety of hardware platforms. For the Diablo Canyon Application, Wonderware uses a CompactPCI PC-based platform running under Microsoft Windows 2000 Professional.

Serious consideration was given to design improvements that would address several operation and reliability issues Diablo Canyon experienced with the old DEHC system since plant startup in 1985.

These new features included:

1. Dual position sensors on the Governor valves. The position sensors provide feedback to the control system to ensure that the valves move to their commanded position. A failed or erratic sensor can cause unstable operation of the turbine (See Figure 1-50).

2. Triple Redundant Control System. The old system had a single set of I/O hardware and a single processor. A single failure could cause the control system to fail, with a unit trip soon to follow. The new system has triple redundant I/O and processors. A single failure (now called “fault” not “failure”) will not cause any loss of function, whether it is an I/O leg or a processor. The system will alarm the fault and continue operation. This arrangement has been in use in the process industry since about 1985 and has logged millions of hours of operation without a single failure to a non-safe condition (See Figure 1-54).

3. Programmed ramps to automate response of the control system to loss of equipment. In the old system, operator action was required to attempt avoiding a trip when certain equipment failed.

4. Three (3) speed probes + 1 spare. The original system had 2 speed probes with one spare. With a single failed speed probe, determining which probe had failed was problematic. With three probes, a single failed probe is much easier to detect. The installed spare allows a failed probe to be swapped into service with the control system on-line, thus retaining three active probes (See Figure 1-48 and Figure 1-49).

5. Dual Servo Position Controllers for each Governor Valve. The old system had one partial arc card per valve. The Moog valve

coils were wired in series, so there was no redundancy (See Figure 1-51).

6. Dual Redundant Network for Human Machine Interface and Maintenance Terminal (See Figure 1-52).

7. Modbus connection to the Woodward Feedwater pump speed controller to get information for each feedwater pump (Not shown in Figure 1-52).

8. Improved Hot Zero adjustment for valve testing. In the old system, the governor valve had to be less than 0.15% open to allow the stop valve to shut. In the new system, the stop valve can shut with the governor valve less than 1% open with other conditions met.

9. Redundant 500 kV breaker position to indicate that the generator has been paralled to the grid.

10. Improved diagnostics. During testing, a shorted lead in the field blew a fuse on a digital input card and was easily located using the Tricon diagnostics panel.

11. Error files record all events even if they are not significant enough to cause an alarm. This helps locate problems before they become problems.

12. The exact Tricon code is being run in the plant training simulator for operations training. No fidelity issues.

The above features eliminated as many single points of failure as possible to increase reliability. As discussed, programmed runbacks and ramps were implemented to automate response to specific equipment failures:

1. Runbacks (Same functions; enhanced features).

- Loss of Stator Water cooling (480 MW/min 10 seconds ON; 50 seconds OFF)
  - Activation on low flow or high conductivity with time delay.
  - Software enhancement to prevent undershoot and turbine trip
  - OTDT and OPDT (480 MW/min, 10 sec ON, 50 sec OFF).

2. Programmed Ramps (New)

- Circulating Water Pump Trip (ramp rate based on Tref – Tavg)
  - Armed with generator paralled, > 650 MW and Bypass off
  - Tref – Tavg indicates steam dump demand (prevents loss of condenser vacuum)
- Feedwater pump trip (225 MW/min until , 650 MW, then 25 MW/min until < 550 MW)
  - Armed with generator paralleled, > 550 MW, and Bypass off
  - Confirmed by both feedwater discharge pressures < 750 psi
- Heater Drip Pump trip (40 MW/min, > 770 MW
  - Armed with generator paralleled, > 770 MW, and Bypass off.

Figure 1-53, taken during construction, shows the new equipment being installed in the racks.

Figure 1-56 through Figure 1-59 illustrates some of the custom screens that are part of the new HMI.

Finally, Figure 1-60 illustrates some of the standard diagnostics that are available to troubleshoot the Tricon system.

Since its installation in 2005, no plant downtime or transient behavior have ve been attributed to the new MTCS. The system has performed as intended in response to plant transients that have occurred.

1.4.3 Protective Relays

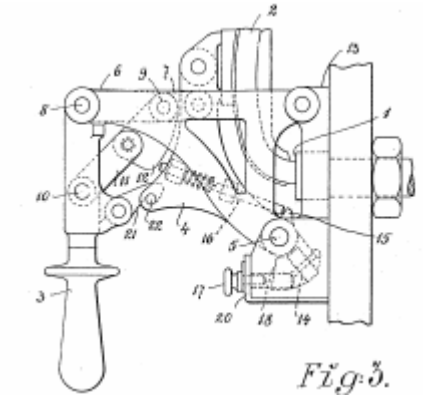
Development of electrical protective relays has taken place in three stages:

- Electromechanical, introduced around 1900
- Static (electronic), 1960's
- Microprocessor, early 1980s

A comparison of the technological history in Protection and Station Automation can be seen in Figure 1-61, which compares the space requirements of old and modern equipment. One numerical terminal can replace up to five panels with electromechanical relays or two panels with static relays. Self-supervision and communication are additional features of numerical terminals

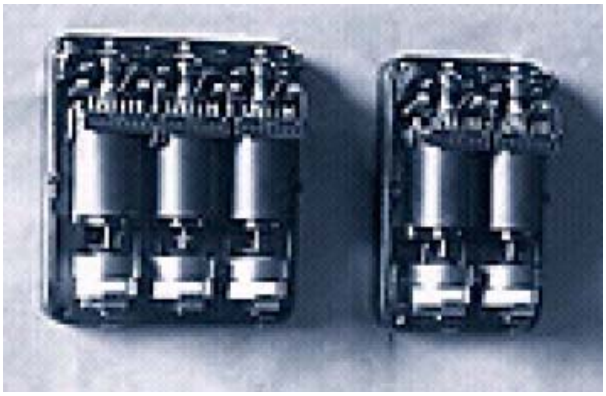
Electromechanical Protective Relays

The first protective relays were integrated into circuit breaker designs and were used to provide the overcurrent trip function. The design shown in the figure below illustrates an integrated overcurrent trip mechanism in hydroelectric power stations around the end of the 19th century.



Overcurrent Trip Mechanism 1900

The first standalone electromechanical relay was designed in 1904 and introduced commercially in 1905. The relay had a bellows made of impregnated balloon cloth that, together with an air valve that attenuated motion of the solenoid, provided the delay required to implement the time overcurrent function. Aging of the cloth bellows was a problem in this design.



Time Overcurrent Relays 1905

Thermal relays using a bimetallic strip were developed for overcurrent protection of three-phase motors. The first ABB thermal relays were delivered in 1912.

Thermal Overcurrent Relay, 1912

The ABB RI relay was designed in 1918 and delivered worldwide from 1920 to 1985, when the last RI relays were replaced by microprocessor based numerical relays. This relay is still used in many countries. In order for numerical relays to be coordinated with these old relays, modern ABB numerical relays still implement the time overcurrent curves of the RI relay.

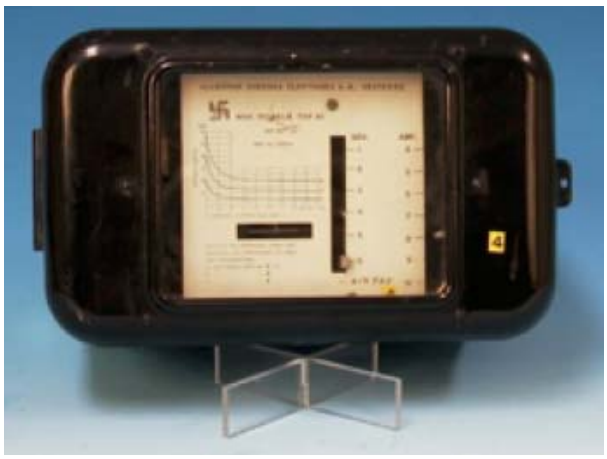


ABB Induction Type Time Overcurrent Relay 1920 – 1985

Modular plug-in relays began to be introduced around 1925 – 1930. The modular design enabled these relays to be replaced without rewiring.

In the 1960's, static relays were introduced. The first static relays were timers, time delays, time overcurrent, voltage, etc.

Microprocessor based relays started to replace static relays in the early 1980's. At first, these relays were "hybrid" solutions, where the time-critical filtering was performed with analog electronics.

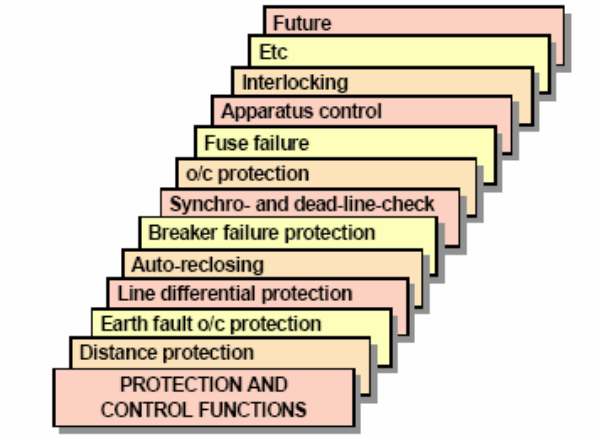
Around 1986, the first fully numerical relays were introduced. These relays now integrated a number of functions:

- Full scheme line distance relay with 5 zones
- Load compensated operation
- Phase selector
- Power swing blocking
- Disturbance recorder - 1 ms resolution
- Event recorder
- Over-current
- Fault locator
- Built-in protection communication schemes
- Serial data communication with two ports for monitoring and control

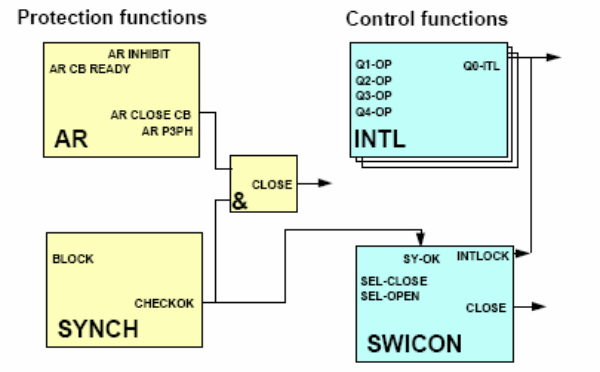
Electromechanical relays had achieved a very high level of accuracy and safety as long as regular adjustments and maintenance were carried out. The first static relays to be introduced were not able to match the high stability and reliability of the electromechanical relays. However, they did offer more functionality. When the static relays were replaced later with digital electronics and still later by microprocessors, the steady improvement of digital electronics and use of self-supervision and diagnostic routines have resulted in modern relays becoming even more reliable than the conventional electromechanical relays.

In the mid 1990s, numerical protective relaying took on a platform concept. The platform consists of a number of hardware modules for analog inputs and A/D conversion, a main processing module, dc/dc supply module, communication modules and a number of flexible input and output modules.

The platform incorporates an extensive library of protection and control software functions, monitoring functions and communication functions. Thus, it is technically possible to integrate the protection and control functions. The different control and protection functions use the same information from the primary equipment and have many similarities, including some redundant functions.



By coordinating these main functions and integrating them when possible, the functionality and performance of the control and protection system can be increased. The integration can both decrease the required wiring and space and increase the overall reliability and availability together with reduced investment and operation cost. This allows the design engineer to concentrate on achieving the basic power system requirements on dependability, security, fault tolerance and availability.



Integration of protection and Control Functions

Use of numerical protective relays allows most functions to be performed by means of software modules running on the same computer-based device. These multi-functional units can be used for control as well as for protection and other secondary functions. It is possible to group and combine different functions using just software tools.

While conventional relay equipment was developed for one specific application, modern digital devices are able to handle a multitude of functions in parallel.

Advantages of the modern technology are:

- A substantial reduction in the number of components used to perform the same functions.
- The hardware required for control, protection and measuring functions can be built into the local control cubicle. An additional room for this equipment is no longer needed.
- Reduction or elimination of wiring due to the use of fiber optic communication buses. Project engineering is simplified and EMC problems are less severe.
- Increased availability through self-supervision and self-checking of the electronics for the remaining hardwired connections as well as checking the function of the protective circuits.

Figure 1-62 shows a substation bay with an integrated control cubicle. If conventional technology were used rather than integrated protection and control with microprocessor-based technology, at least one and possibly two more cubicles would be required.

1.4.4 Energy Conversion – Static Inverters

A static inverter or Uninterruptible Power System (UPS) is designed to be the prime source of power to a critical load. A UPS not only provides uninterruptible power to a critical load, but also isolation from voltage variations and various forms of voltage transients present on the utility line.

Many problems experienced in the areas of data processing, communication, closed loop instrumentation and on-fine computers are the result of power related problems such as temporary outages, momentary interruptions, surges, sags or noise. Electric motors, welders, switches or fuse clearing may be causing the problem. Surges, sags or noise problems can be partially remedied through the use of line conditioners. However, if temporary outages or momentary interruptions are a major part of the problem, the solution is an Uninterruptible Power System (UPS).

Single Unit Float Configuration

There are several configurations of UPS used in industry. However, the single unit Float configuration shown in Figure 1-63 is the most common because it contains the fewest number of major components. This configuration is also the typical UPS used in nuclear power plant applications.

This system converts utility AC power to DC through the battery charger. The regulated DC power is supplied to both a bank of batteries and to the inverter. The inverter "inverts" the DC back into regulated, noise-free AC power and passes it along to the static switch. The static switch, under normal conditions, passes this AC power through to a manual switch and on to the load. If AC power to the battery charger is lost, the batteries automatically begin supplying the required DC power to the inverter.

If the inverter fails, or a fault on the load overloads the inverter, the static switch will automatically transfer the load to the alternate source of power. The manual bypass switch is a mechanical, make-before-break switch that is used to bypass the UPS for maintenance purposes.

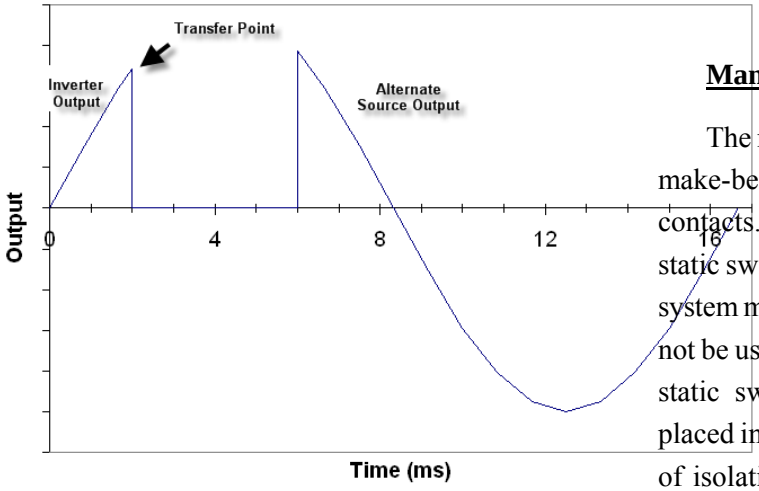
Static Switch

The static switch provides an automatic transfer from the output of the inverter to the alternate source in the event of an overload on the UPS output. An overcurrent transfer circuit in the static switch automatically transfers the load to the alternate source due to inrushes from the load or faults on the load.

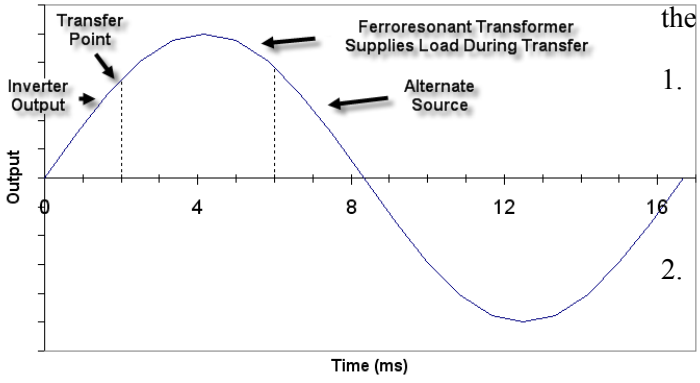
Without this feature, the inverter could be driven into current limit prior to clearing a fault. This would most likely cause all the loads to be lost. The static switch, therefore, transfers to the alternate source at 110% to 125% (depending on manufacturer) of rated load, where fault clearing capabilities should exist. Because this circuit cannot differentiate between an inrush and a fault, it is common for the initial energization of a load to cause a transfer and be energized from the alternate source for a short time.

The static switch also provides an automatic transfer from the inverter output to the alternate source in the event of an inverter failure. The typical static switch has a maximum transfer time of four milliseconds.

In the following illustration, a static switch transfers load upon loss of voltage being supplied to the switch from the inverter. The static switch senses the loss of voltage and initiates a transfer. The sense-to-transfer initiation time is approximately four milliseconds.



Some critical applications may not be able to tolerate a loss of voltage, even for 4 ms. If this is the case, a zero-break static switch is also available using a ferroresonant type inverter. In this inverter, the output transformer is ferroresonant, that is, the transformer magnetic circuit is resonant at the line frequency and energy is stored in its magnetic field. The zero-break static switch on the ferroresonant inverter monitors the output of the inverter, prior to the ferroresonant transformer. If the square wave deteriorates, indicating an inverter failure; the static switch sensing circuit will initiate a transfer to the alternate source, with the stored energy in the ferroresonant transformer used to accomplish the zero-break transfer. The zero-break transfer is illustrated in the following figure:



Manual Bypass Switch

The manual bypass switch is usually a mechanical make-before-break type of switch with overlapping contacts. Its purpose is to bypass the output of the static switch and tie directly to the alternate source for system maintenance. The manual bypass switch should not be used to remove alternate source power from the static switch. Instead, a circuit breaker should be placed in series with the alternate source. This method of isolation permits testing of the static switch with power applied to both poles while in the bypass mode.

Rectifier/Battery Charger

The battery charger provides a regulated source of DC power to the battery system and inverter and also isolates the UPS from the AC line through an isolation transformer. The output of the charger must be regulated and have current limiting capabilities. The current limit function provides protection for both the batteries and the charger. The battery charger must be sized large enough to supply the inverter and simultaneously recharge a fully discharge battery bank within a specified time. Output voltage regulation is important since the battery requires a precise charging voltage for maximum life and minimum maintenance.

Inverter

The inverter provides three primary functions in the UPS:

1. Inversion - the changing of the DC power to AC power composed of a sine wave free from harmful harmonic distortion; typically 5% total harmonic distortion (THD) or less.
2. Regulation - the regulation of the AC voltage to a tolerance level acceptable to the load, typically +2% of the nominal voltage.

3. Limiting Capability - provides for the current limiting capability as a means of self-protection.

Several components of the UPS are used in the Variable Speed Drives discussed in the next section.

[Credit: Solidstate Controls, Inc]

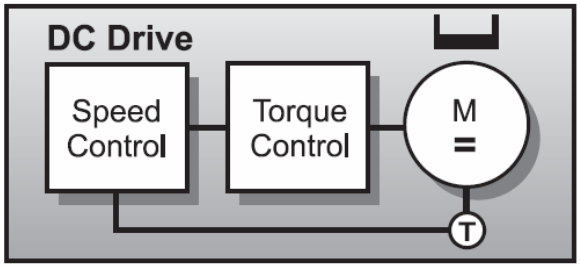
1.4.5 Variable Speed Drives

The objective of this lesson is to understand the basic function of a variable speed drive (VSD) and how microprocessor technology is being used to enhance performance in VSDs.

The function of a VSD is to control the flow of energy from the electrical power system to the process. Energy is supplied to the process through the motor shaft. Two physical quantities describe the state of the shaft: torque and speed. To control the flow of energy we must therefore, ultimately, control these quantities.

When the VSD operates in torque control mode, the speed is determined by the load. Likewise, when operated in speed control, the torque is determined by the load. Initially, DC motors were used as VSDs because they could easily achieve the required speed and torque without the need for sophisticated electronics. However, the evolution of AC variable speed drive technology has been driven partly by the desire to emulate the excellent performance of the DC motor, such as fast torque response and speed accuracy, while using rugged, inexpensive and maintenance free AC motors.

DC Motor Drive



Control Loop of a DC drive Motor

In a DC motor, the magnetic field is created by the current through the field winding in the stator. This field is always at right angles to the field created by the armature winding. This condition, known as field orientation, is needed to generate maximum torque. The commutator-brush assembly ensures this condition is maintained regardless of the rotor position.

Once field orientation is achieved, the DC motor's torque is easily controlled by varying the armature current and by keeping the magnetizing current constant. The advantage of DC drives is that speed and torque - the two main concerns of the end-user - are controlled directly through armature current. Advantages of the DC drives are:

- Accurate and fast torque control
- High dynamic speed response
- Simple to control

Initially, DC drives were used for variable speed control because they could easily achieve a good torque and speed response with high accuracy. The drive was simple. The commutator controls field orientation and there is no need for a complex electronic control system.

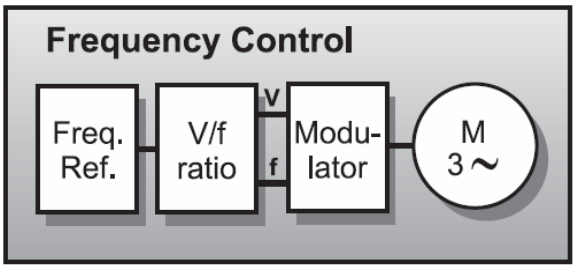
Drawbacks of the DC drive are:

- Reduced motor reliability

- Regular maintenance
- Motor costly to purchase
- Needs encoder for feedback

While a DC drive produces an easily controlled torque from zero to base speed and beyond, the motor's mechanics are more complex and require regular maintenance.

AC Drives – Frequency Control Using Pulse-Width Modulation



Control Loop of an AC Drive with Frequency Control using PWM

The AC drive frequency control technique uses parameters generated outside of the motor as controlling variables, namely voltage and frequency. Both voltage and frequency reference are fed into a modulator which simulates an AC sine wave and feeds this to the motor's stator windings. This technique is called Pulse Width Modulation (PWM) and utilizes a rectifier to convert the AC supply voltage to DC. The intermediate DC voltage is kept constant. The inverter controls the motor in the form of a PWM pulse train dictating both the voltage and frequency. Significantly, this method does not use a feedback device which takes speed or position measurements from the motor's shaft and feeds these back into the control loop. Such an arrangement, without a feedback device, is called an "open-loop drive".

Advantages of this drive are:

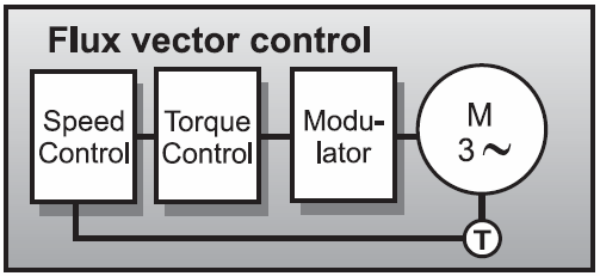
- Low cost
- No feedback device required
- Simple

Because there is no feedback device, this drive offers a low cost and simple solution to controlling economical AC induction motors. It is suitable for applications which do not require high levels of accuracy or precision, such as pumps and fans.

Disadvantages of this drive are:

- Field orientation not used. Voltage and frequency are the control variables.
- Motor status ignored. There is no speed or position feedback.
- Torque is not controlled. Feedback is required to control torque
- Delaying modulator used. The modulator slows down the communication between the incoming voltage and frequency signals and the need for the motor to respond.

AC Drives - Flux Vector Control Using PWM



Control Loop of an AC Drive with Flux Vector Control

- Field-oriented control - simulates DC drive
- Motor electrical characteristics are simulated
- "Motor Model"

- Closed-loop drive
- Torque controlled INDIRECTLY

This drive simulates a DC drive. To emulate the magnetic operating conditions of a DC motor, i.e. to perform the field orientation process, the flux-vector drive needs to know the spatial angular position of the rotor flux inside the AC induction motor.

With flux vector PWM drives, field orientation is achieved by electronic means rather than the mechanical commutator/ brush assembly of the DC motor.

1. Information about the rotor status is obtained by feeding back rotor speed and angular position relative to the stator field by means of a pulse encoder. A drive that uses speed encoders is referred to as a "closed-loop drive".

2. The motor's electrical characteristics are mathematically modeled with microprocessors used to process the data.

The electronic controller of a flux-vector drive creates electrical quantities such as voltage, current and frequency, which are the controlling variables, and feeds these through a modulator to the AC induction motor. Torque, therefore, is controlled INDIRECTLY.

- Good torque response
- Accurate speed control
- Full torque at zero speed
- Performance approaching DC drive

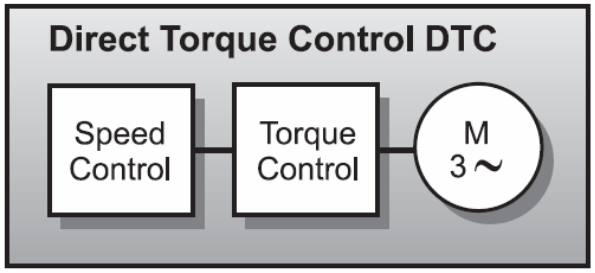
Flux vector control achieves full torque at zero speed, giving it a performance very close to that of a DC drive.

Disadvantages of this drive are:

- Feedback is needed to achieve a high level of torque response and speed accuracy.
- Costly. Feedback device adds complexity to the drive.
- Modulator needed. The modulator slows down the communication between the incoming voltage and frequency signals and the need for the motor to respond.

Although the motor is mechanically simple, the drive is electrically complex.

AC Drives – Direct Torque Control



Control Loop of an AC Motor Using Direct Torque Control

With Direct Torque Control, field orientation is achieved without feedback using advanced motor theory to calculate the motor torque directly and without using modulation.

The controlling variables are motor magnetizing flux and motor torque. With DTC there is no modulator and no requirement for a tachometer or position encoder to feed back the speed or position of the motor shaft.

DTC uses the fastest digital signal processing hardware available and a more advanced mathematical understanding of how a motor works. The result is a drive with a torque response that is typically 10 times faster than any AC or DC drive.

The dynamic speed accuracy of DTC drives will be 8 times better than any open loop AC drives and comparable to a DC drive that is using feedback. DTC produces the first "universal" drive with the capability to perform like either an AC or DC drive.

DRIVE	CONTROL VARIABLES
DC DRIVES	Armature Current, I_A Magnetising Current, I_M
AC DRIVES (PWM)	Output Voltage, U Output Frequency, f
Direct Torque Control	Motor Torque, T Motor Magnetising Flux, Ψ

Comparison of Motor Drive Control Variables

The above table shows that both DC Drives and DTC drives use actual motor parameters to control torque and speed, enabling fast dynamic performance. For most applications using DTC, no tachometer or encoder is needed to feed back a speed or position signal. The main difference between DTC and other AC drive technologies is that no modulator is required with DTC.

Because torque and flux are motor parameters that are being directly controlled, there is no need for a modulator, as used in PWM drives, to control the frequency and voltage. This dramatically speeds up the response of the drive to changes in required torque. DTC also provides precise torque control without the need for a feedback device.

For the purpose of this lesson, it is important to note that microprocessor technology makes advanced motor control possible, whether it is vector control or DTC. Advanced motor controls enable variable speed applications to achieve performance equivalent to that of dc motors, yet using inexpensive squirrel-cage induction motors. Without microprocessor technology, variable speed motor applications would be limited to using those using dc motors or less efficient and less precise (but also less expensive) ac motors.

[Credit: ABB Technical Guide No.1- Direct Torque Control]

1.5 New Plant Licensing Delta

This section will address the following objectives:

- Provide overview of the new reactor designs coming into NRC for COL, ESBWR, ABWR, AP1000, EPR and APWR
- Review regulatory delta
- Review Reg. Guide 1.206 guidance on I&C
  - ITAAC
  - DAC
  - Reviewed new technology applications
  - Summary

First, we will review a summary of the current licensing application listing for new plants as shown in Figure 1-64 and a set of pictures and artists drawings of the new control rooms as anticipated for the 5 major designs, as shown in Figure 1-65 through Figure 1-69:

- AP1000
- ABWR
- ESBWR
- EPR
- US APWR

The elements of the regulatory guidance for new plants includes:

- 10 CFR Part 52 – ESP, DC, COL
- IEEE 603-1991 law(not guidance) per 10 CFR 50.55a(h)

- For COL or construction permit requested After May 13, 1999
- IEEE 7-4.3.2-2003, per Reg. Guide 1.152

Next, we review the regulatory delta between IEEE 279 and IEEE 603, as follows:

- IEEE 279 and 603 do not directly discuss digital computer-based systems. Guidance on digital computer-based systems is in IEEE 7-4.3.2-2003, as endorsed by Reg. Guide 1.152, Rev 2.
- Computer system software integrity should be demonstrated by the applicants software safety analysis activities (BTP 7-14)
- Reg. Guide 1.206 provides a list of expected deliverables or review tasks on new plants

The SRP Chapter 7 provides specific guidance for new plant reviews including:

- ITAAC – for DC and COL reviews, the staff reviews the proposed ITAAC associated with SSCs following SRP Section 14.3. ITAAC review cannot be completed until the rest of this portion of the application has been reviewed.
- COL Action Items and Certification Requirements and Restrictions
  - For a COL applicant referencing a DC, a COL applicant must address COL action items included in the referenced DC (open items, interface items, site parameters, etc)

Reg. Guide 1.206 Section 3:III.5 defines Design Acceptance Criteria (DAC) as follows:

- Per SECY-92-053, DAC are:
  - "A set of prescribed limits, parameters, procedures, and attributes upon which the NRC relies, in a limited number of technical areas, in making a final safety determination to support a design certification."
  - DAC are measurable, testable and subject to analysis using pre-approved methods.
  - Verified as part of the inspections, tests, analyses, and acceptance criteria (ITAAC)

Reg. Guide 1.206 Section C.III.5 also includes the following guidance:

- "The path to successfully satisfying DAC and completing the associated ITAAC may include review of information or procedures that occur early in the construction, fabrication, or development processes that may necessitate early involvement by NRC inspectors and staff, e.g.; in development of reactor protection system software."

Next, a full set of the Reg. Guide 1.206 Section C.III.5 listing of information necessary to verify completion of I&C design is provided in Figure 1-70 through Figure 1-73.

Reg. Guide 1.206 Section C.II.2.2.5 provides an overview of ITAAC for I&C including:

- Major Focus Areas:
- Compliance to 10 CFR 50.55a(h)
- Compliance with GDCs
- Documentation of high quality software design process
  - –Software plans
  - –Report output from life-cycle phases
  - –BTP-14 output documents

A set of expected DAC phases and deliverables is now provided in a set of slides that address example DAC and licensing deliverables to NRC staff for each phase and expected timelines for those deliveries and

reviews by NRC staff as shown in Figure 1-74 through Figure 1-80.

Finally, new technologies are expected to be introduced in new reactor licensing including:

- Gamma Thermometers
- FPGAs
- Simulation assisted design

Two illustrations of how a gamma thermometer (GT) works are included in Figure 1-81 and Figure 1-82.

A picture of what an FPGA looks like and the type of configurations it can replace is included in Figure 1-83

In summary, we have covered the following in this section:

- Provided overview of the new reactor designs coming into NRC for COL, ESBWR, ABWR, AP1000, EPR and APWR
- Reviewed regulatory delta
- Review Reg. Guide 1.206 guidance on I&C
  - ITAAC
  - DAC
- Reviewed new technology applications
- Summary

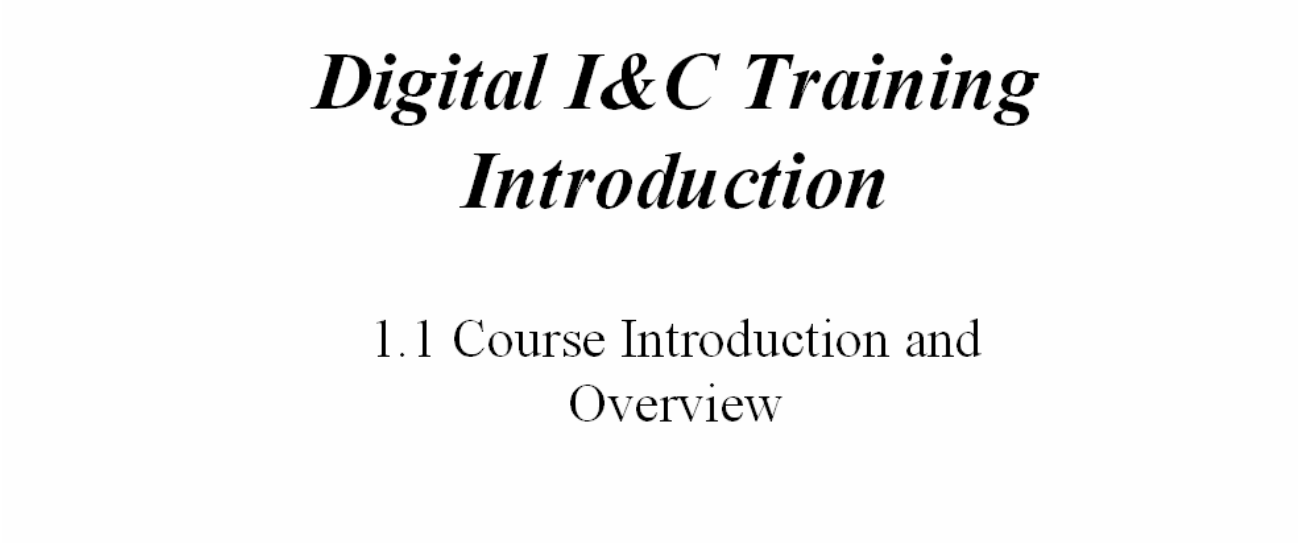


Figure 1-1 Introduction

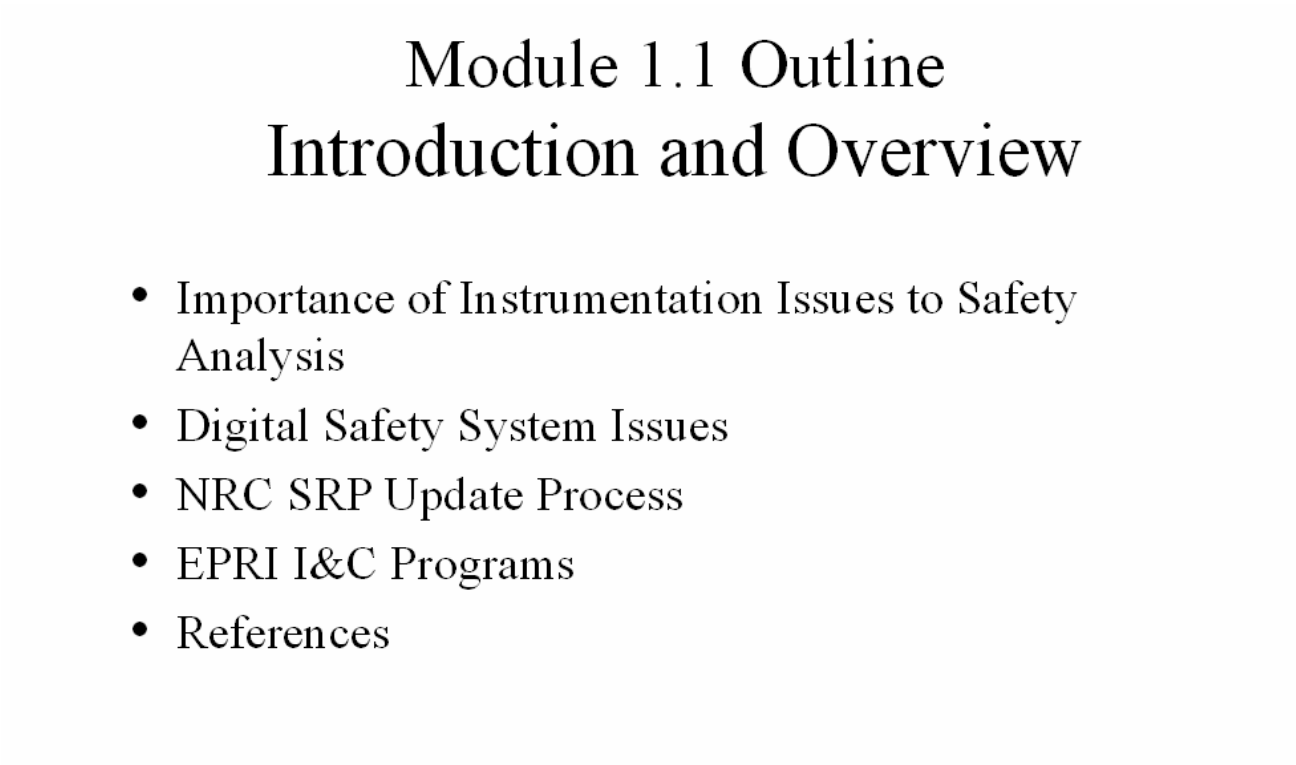


Figure 1-2 Outline

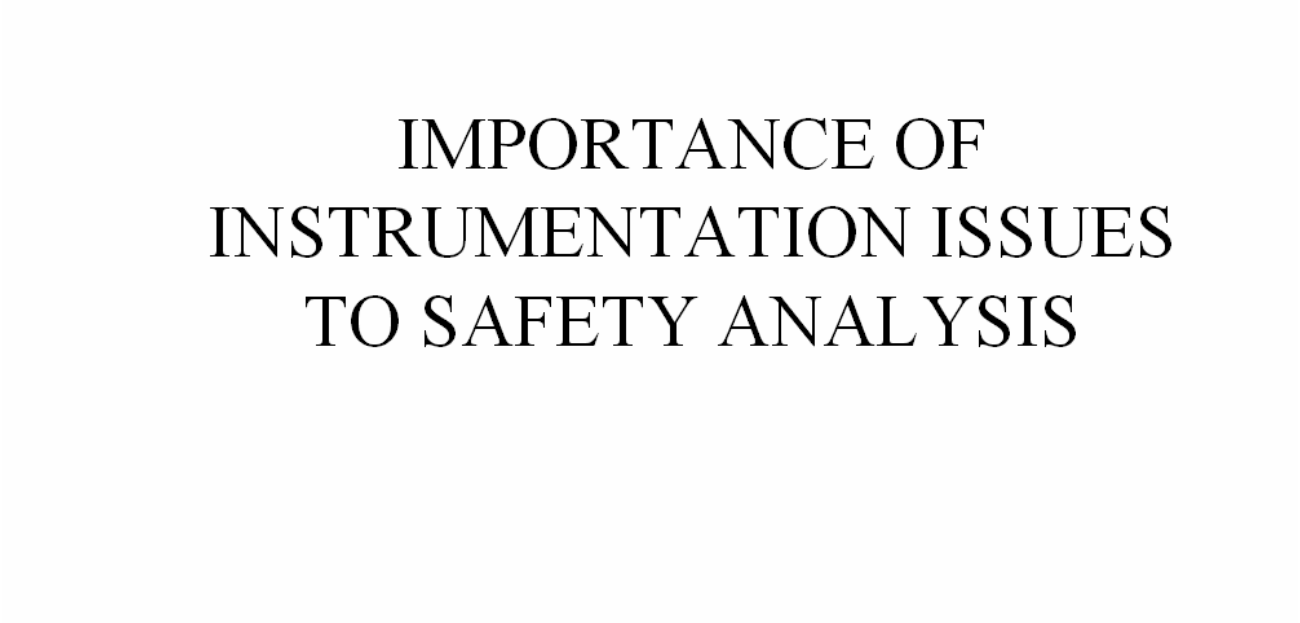


Figure 1-3 Importance of Instrumentation Issues to Safety Analysis

DEFENSE IN DEPTH DESIGN PHILOSOPHY

- Simply stated, the reason for reactor safety requirements is to prevent the release of radioactivity from the fuel.
- Nuclear power plant design is based upon the concept of using multiple, successive barriers to prevent the escape of radioactive material.
- To assure that these barriers are not compromised as a result of abnormal occurrences (e.g., Equipment failure, human error, or natural phenomena) the industry & NRC have adopted the concept of a 3 tiered safety philosophy.
- It is intended that a defense in depth will be achieved for each of the radioactivity barriers.
  - Reactor Coolant System Boundary
  - Fuel Clad
  - Containment Boundary

Figure 1-4 Defense in Depth Design Philosophy

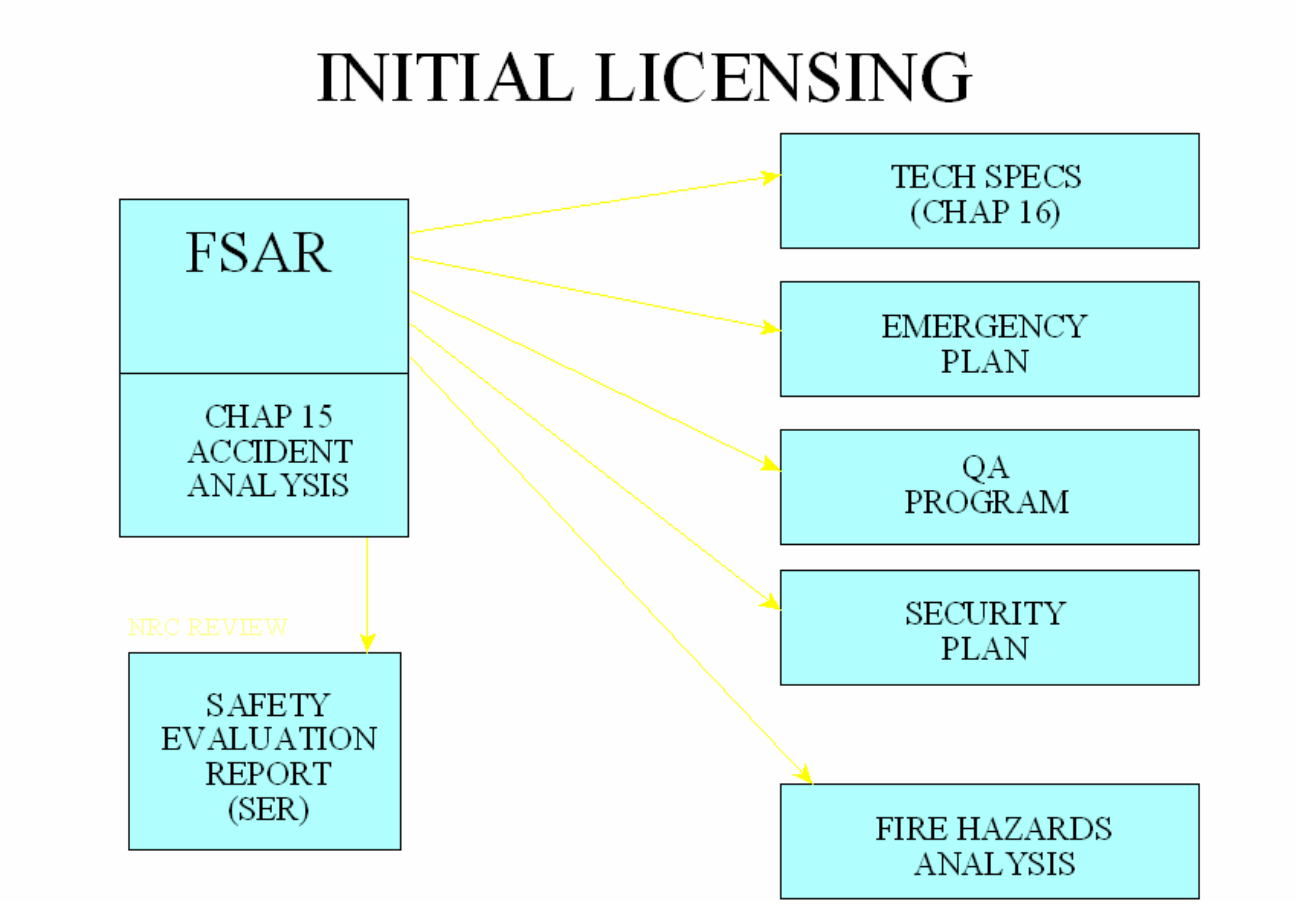


Figure 1-5 Initial Licensing

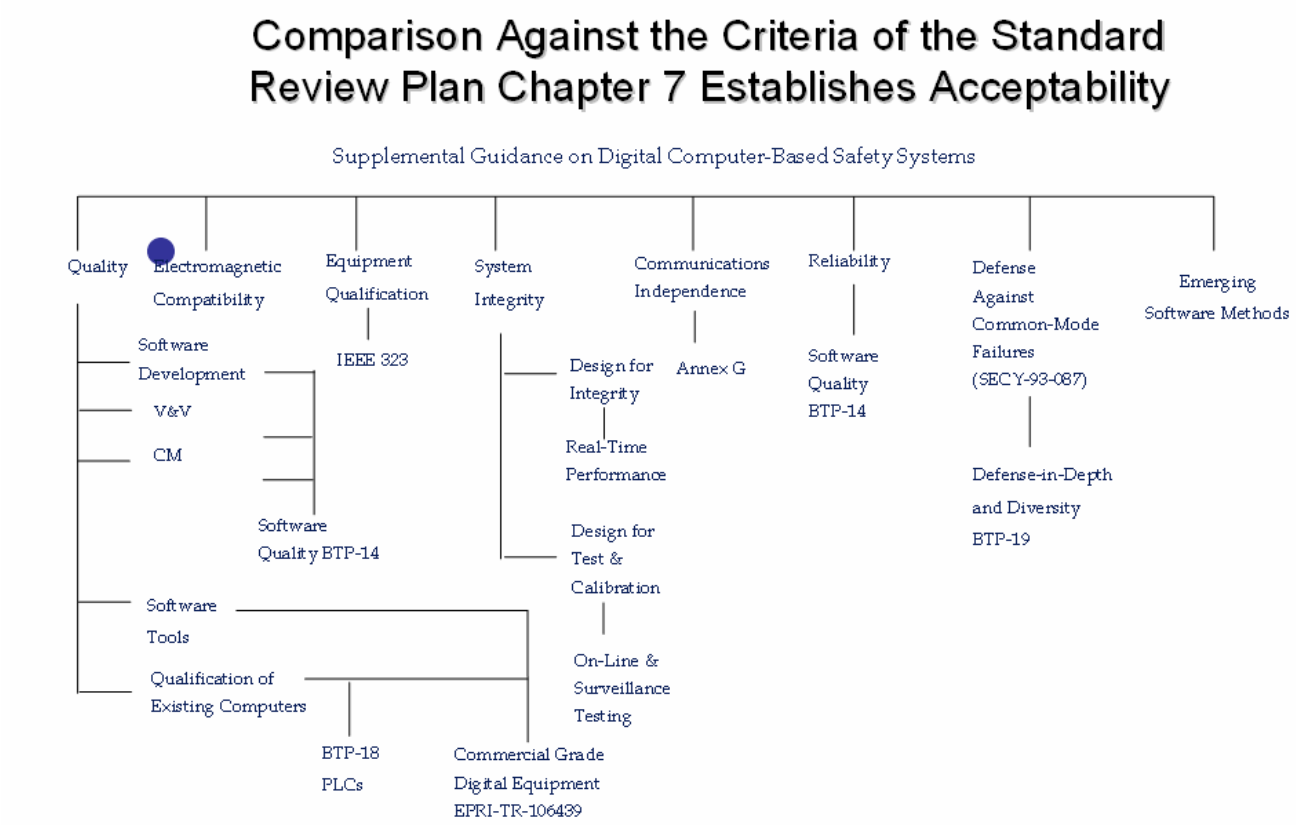


Figure 1-6 Comparison of the Criteria of the Standard Review Plan Chapter 7

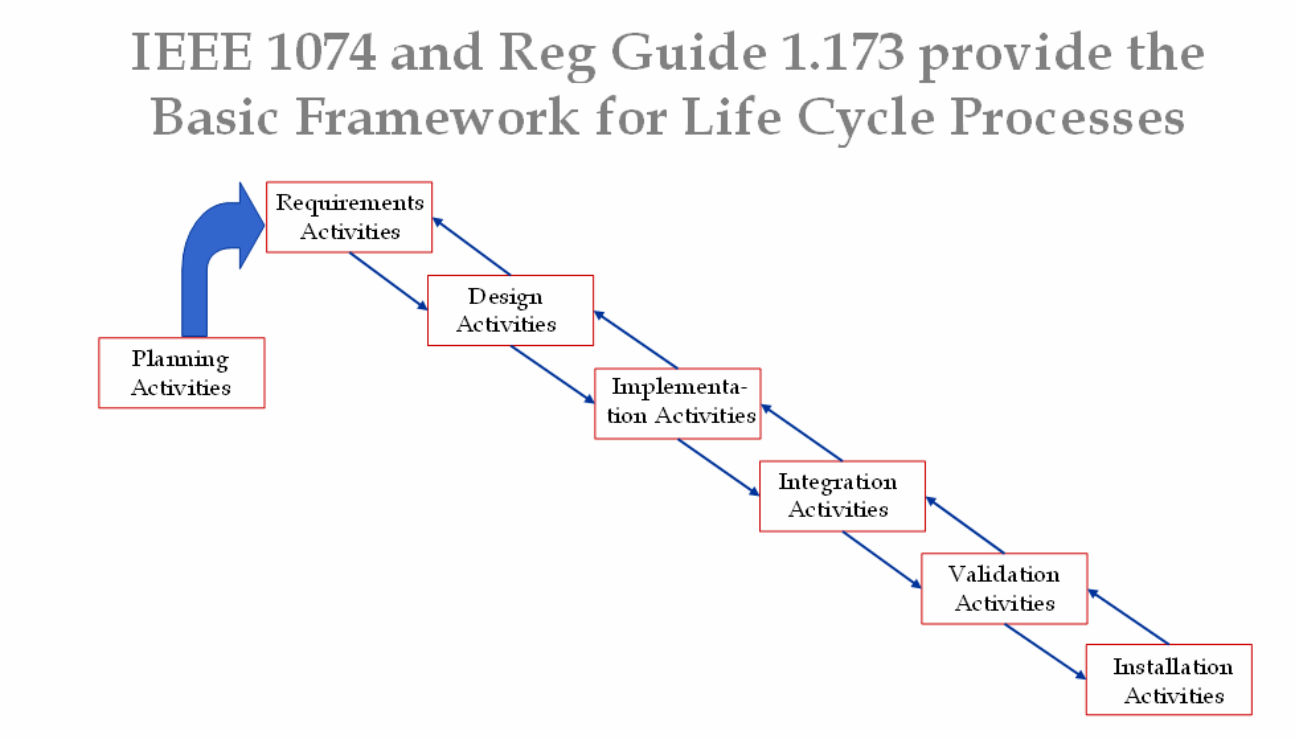


Figure 1-7 Basic Framework for Life Cycle Processes

NRC Document Request for Oconee Digital LAR vs. Normal Document Availability

Life Cycle Phase	Oconee Documents
Documents requested with initial LAR submittal	
1.) Project Definition and Planning	ONS Unit 1 RPS/ESFAS Controls Upgrade Software Requirements Review Report Software and Data Quality Assurance (SDQA) Program ONS Units 1, 2, & 3 RPS/ESFAS Controls Upgrade Software Installation Plan ONS Units 1, 2, & 3 RPS/ESFAS Controls Upgrade Software Safety Plan ONS Units 1, 2, & 3 RPS/ESFAS Controls Upgrade Verification and Validation Plan ONS Unit 1 – RPS & ESFAS Configuration Management Plan

Figure 1-8 Oconee Digital RPS LAR Document Request (1 of 9)

NRC Document Request for Oconee Digital LAR vs. Normal Document Availability

Life Cycle Phase	Oconee Documents
Documents requested with initial LAR submittal	
2. Requirements Phase 3. Design and Implementation Phase	System Description for LAR Input Detailed System Architecture Oconee 1 RPS&ESFAS Requirements Traceability Matrix (FAT Version) Teleperm XS Product Information on Release 3.0.7A of TXS Software Oconee Nuclear Station TXS RPS/ESPS Replacement System Cabinet Design: 1PPSCA0005 Oconee Nuclear Station TXS RPS/ESPS Replacement System Cabinet Design: 1PPSCA0006 FMEA Summary Calc. TXS FMEA ONS 1, 2, & 3 RPS/ESF Controls Upgrade Design Specification for Key Locks and Key Switches Software Requirements Specification,ONS-1 RPS/ESF Software Requirements Specification (QA1)

Figure 1-9 Oconee Digital RPS LAR Document Request (2 of 9)

NRC Document Request for Oconee Digital LAR vs. Normal Document Availability

Life Cycle Phase	Oconee Documents
Documents requested with initial LAR submittal	
2. Requirements Phase 3. Design and Implementation Phase	ONS Unit 1: RPS and ESFAS Replacement Project Open Item Form, "HW Typicals for CRD (Control Rod Drive) UV (under voltage) Test Jacks, Doc Step 3.12 ONS 1, 2, & 3 RPS/ESF Controls Upgrade Hardware Design Solutions Oconee Nuclear Station, Units 1, 2, & 3 RPS/ESF Controls Upgrade ID Coding Concept ONS Unit 1 RPS/ESFAS Controls Upgrade Software Design Description ONS Unit 1 – RPS & ESFAS Factory Acceptance Test Plan Dedication Package for Absopulse Power Supply TXS Supplemental EQ (Equipment Qualification) Summary Test Report ONS RPS/ESFAS Replacement Project EQ Summary Test Report

Figure 1-10 Oconee Digital RPS LAR Document Request (3 of 9)

NRC Document Request for Oconee Digital LAR vs. Normal Document Availability

Life Cycle Phase	Oconee Documents
Documents requested with initial LAR submittal	
2. Requirements Phase 3. Design and Implementation Phase	TUV Certificate on Communication Processor TUV Documentation on SCP2 Testing TUV Certificate on Processing Module FANP (Framatome ANP) Report, "TELEPERM XS Simulation – Concept of Validation and Verification Configuration Management Reactor Building Narrow Range Pressure Instrument Loop Accuracy Calculation (ESFAS) Wide Range RCS Pressure Uncertainty, (ESFAS HPI & LPI setpoints) RPS Flux/Flow Ratio Uncertainty Evaluation RPS RCS Pressure & Temperature Trip Function Uncertainty Analysis and Variable Low Pressure Safety Limit RPS High Flux and Pump/Power Monitor Trip Function Uncertainty Analysis

Figure 1-11 Oconee Digital RPS LAR Document Request (4 of 9)

NRC Document Request for Oconee Digital LAR vs. Normal Document Availability

Life Cycle Phase	Oconee Documents
Documents requested with initial LAR submittal	
2. Requirements Phase 3. Design and Implementation Phase	ONS Unit 1 – RPS & ESFAS System Functional Description Engineered Safeguard Feature Actuation System (ESFAS) Replacement Project Specification Reactor Protection System (RPS) Replacement Project Specification Documentation of Software Requirements and SDQA for RPS/ESFAS System Replacement SIVAT LSELS Specifications, Job 4310002, Outputs: EFHV0037 Teleperm XS Function Blocks, Version 2.60 FB-ADDON, Version 1.2 SIVAT-TXS Simulation Based Validation Tool, Version 1.4.0 (now rev. 1.5.1) U1 Parameter Calc

Figure 1-12 Oconee Digital RPS LAR Document Request (5 of 9)

NRC Document Request for Oconee Digital LAR vs. Normal Document Availability

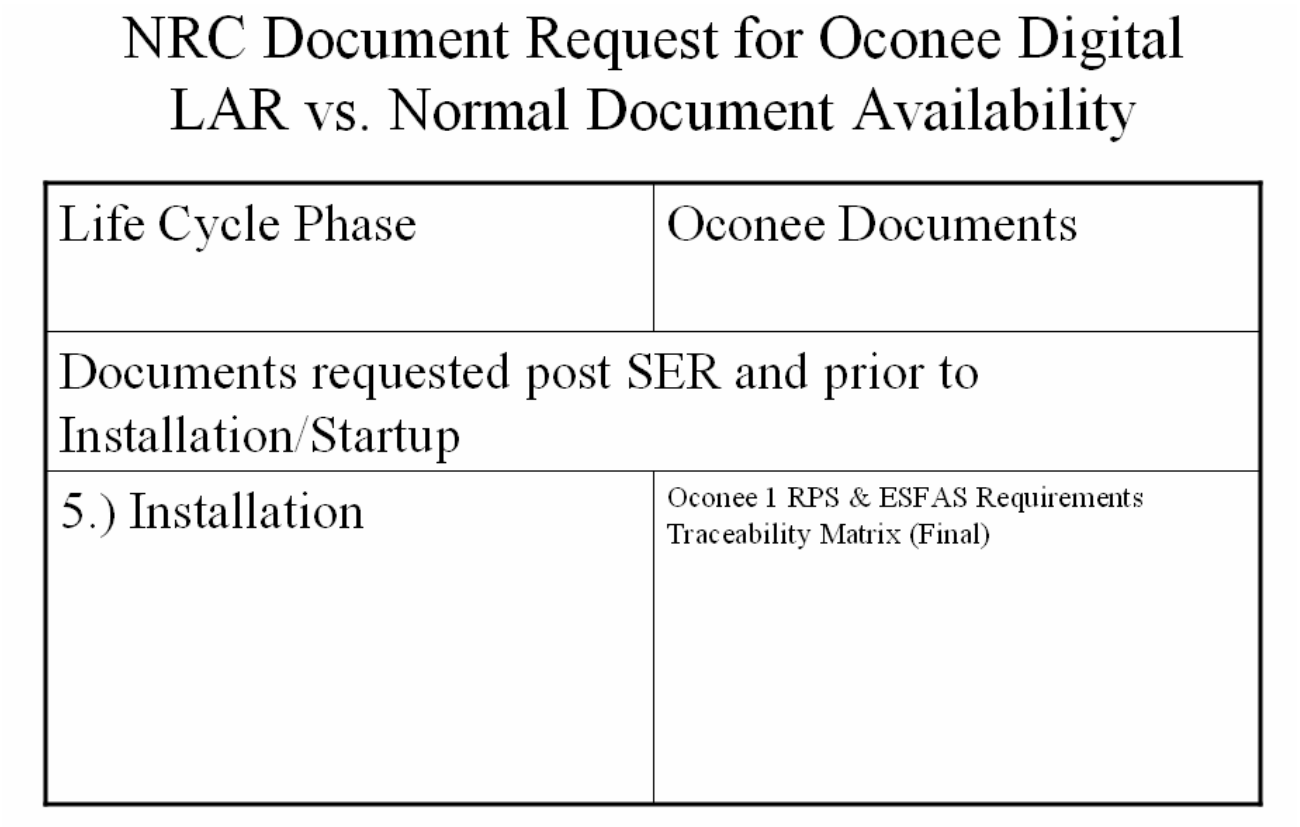
Life Cycle Phase	Oconee Documents
Documents requested post LAR submittal and during staff LAR review (prior to SER)	
3.) Design and Implementation	Site Acceptance Test Plan

Figure 1-13 Oconee Digital RPS LAR Document Request (6 of 9)

NRC Document Request for Oconee Digital LAR vs. Normal Document Availability

Life Cycle Phase	Oconee Documents
Documents requested post SER and prior to Installation/Startup	
4.) Testing (Pre-installation)	ONS Unit 1 – RPS & ESFAS Factory Acceptance Test Procedures ONS Unit 1 – RPS & ESFAS Factory Acceptance Test Results Report Site Acceptance Test Plan Procedures Site Acceptance Test Results Report

Figure 1-14 Oconee Digital RPS LAR Document Request (7 of 9)



NRC Document Request for Oconee Digital
LAR vs. Normal Document Availability

Life Cycle Phase	Oconee Documents
Documents requested post SER and prior to Installation/Startup	
5.) Installation	Oconee 1 RPS & ESFAS Requirements Traceability Matrix (Final)

Figure 1-15 Oconee Digital RPS LAR Document Request (8 of 9)

NRC Document Request for Oconee Digital LAR vs. Normal Document Availability

Life Cycle Phase	Oconee Documents
Documents requested post SER and prior to Installation/Startup	
6.) Operation, Maintenance and Support (prior to Unit operation with digital system installed)	Power-Imbalance Safety Limits and Tech. Spec. Setpoints Using Error-Adjusted Flux/Flow Ratio of 1.094 Duke Power Company, Oconee Nuclear Station, "Nuclear Instrumentation RPS Removal from and Return to Service for Channels A, B, C and D, Rev. 031, ETQS No. RPS-Q-ENTRY

Figure 1-16 Oconee Digital RPS LAR Document Request (9 of 9)

LERs from 1990-1993 Show Digital I&C System Failures

Digital System Failure Events Reported in LERs (1990-1993)

Category	Number of Events
Software Error	30
Human-Machine Interface Error	25
Electromagnetic Interference	15
Random Component Failure	9
Total	79

Figure 1-17 LERs from 1990-1993 Show Digital I&C System Failures

LERs from 1990-1993 Show Digital I&C System Failures (cont)

Digital I&C System Failure Events in U.S. NPPs

Cause	Number of Events			
	Spurious Trips and System Actuations	Loss of Monitoring or Control Function	Incorrect or Incomplete Parameter Evaluation	Others
Hardware	4	5	0	0
Software	2	7	5	15
Human Interaction	6	8	2	10
EMI	10	4	0	1
Total	22	24	7	26

Figure 1-18 LERs from 1990-1993 Show Digital I&C System Failures (cont)

NRC Digital Upgrade Public Hearing
8 November 2006

- **Amir Shahkarami, Exelon Senior Vice President**

"We believe the use of digital technology is absolutely necessary for the future of our nuclear industry. It will enhance safety. It reduces obsolescence, not only from equipment standpoint, but from a knowledge standpoint."

"The New Era Of Nuclear Power"
GE Energy Orbit Magazine
Volume 26 Number 3 2006

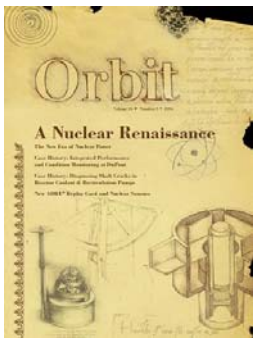


Figure 1-19 Amir Shahkarami Quotation

2005 Software Design Error in Software Upgrade at Palo Verde 2 for 2,736 hrs.

- **Original software design:**
  - **Trip CPC channel if sensor detected to be "Failed – Out of Range"**
- **Software hardware upgrade:**
  - **Use inputs from two sets of instruments and multiplexers (primary and secondary)**
- **Out of Range Sensor Failure:**
  - **Primary detected sensor failure results in switchover to secondary.**
  - **Out of Range Failure on secondary reverts to "last stored good value"**
- **CCF of all sensors of one type could result in continuous use of "last good value" in all 4 CPCS channels rather than *TRIP*.**
- **$P_{CPCS-CCF} = 8 \times P_{Sensor-CCF} \times 2.75 \times 10^{-6}/hr \times 2{,}736\ hr$**
  $= 8 \times 8.4 \times 10^{-4} \times 2.75 \times 10^{-6}/hr \times 2{,}736\ hr = 5.0 \times 10^{-5}$
- **Given CCF of instruments, *no credit for operators*, HEP=1.0**
- **CCDP = $0.289/yr \times 5.0 \times 10^{-5} \times 1.0 = 1.44 \times 10^{-5}$**

Figure 1-20 Palo Verde Core Protection Calculator Event (1 of 2)

2005 Software Design Error in Software Upgrade at Palo Verde 2 for 2,736 hrs.

- Narrative Version:
  - APS project replacement CPC software and hardware – completed on Unit 2 and Unit 1 and 3 not implemented yet
  - Westinghouse discovered during design review for Korea plants
  - On-line software did not match CPC Functional Requirements Specification
  - SRS erroneously included a feature that uses the last valid sensor input signal for the current scan value when a particular sensor fails – while FRS requires use of range limits for failed sensor signal. Use of range limits would result in an automatic CPC channel trip if needed.
  - The flaw in the software could have resulted in the avoidance of an automatic CPC channel trip when needed for certain sensor failures
  - Significant – the operators would have had annunciator indication of the sensor failure and could have manually tripped (or bypassed) the channel if needed.
  - Summary – V&V and Testing Correct – SRS incorrect.

Figure 1-21 Palo Verde Core Protection Calculator Event (2 of 2)

TVA Browns Ferry Unit 3 Data Storm – 2006

- IEN 2007-15
- Aug. 19. 2006, BF3 manually scrammed following loss of both reactor recirculation pumps.
- Initial investigation found that the recirculation pump variable frequency drive (VFD) controllers were nonresponsive. Also, the BF3 condensate demin. Controller had failed simultaneously. Condensate demin. Controller is dual redundant PLC connected to the ethernet-based plant integrated computer system (ICS) network – along with VFDs.
- Both VFD and cond. Demin. Controllers are microprocessor based utilizing proprietary software.

Figure 1-22 Browns Ferry Data Storm (1 of 3)

TVA Browns Ferry Unit 3 Data Storm – 2006

- Root Cause: malfunction of the VFD controller because of excessive traffic on the plant ICS network. Testing confirmed. Can achieve failure on the existing 10-megabit/second netowrk.
- PLC vendor indicated that the PLC failure was a likely symptom of the excessive network traffic.
- Licensee corrective actions:
  - Develop network firewall device that limits connections and traffic to any potentially susceptible devices on the plant ICS network
  - Installing network firewall device on each unit's VFD controller and condensate demin. controller.

Figure 1-23 Browns Ferry Data Storm (2 of 3)

TVA Browns Ferry Unit 3 Data Storm – 2006

- Summary:
- Ethernet used extensively for LAN
- Data packet is a basic unit – to function properly, a device must be able to effectively handle the broadcast packets it receives.
- Key point – all network devices must allocate time and resources to read and interpret each broadcasted data packet, even if the packet is not intended for that particular device.
- Excessive data packet traffic on the network may cause connected devices to have a delayed response to new commands or even lockup.
- Excessive network traffic also called *broadcast (or data) storm.*

Figure 1-24 Browns Ferry Data Storm (3 of 3)

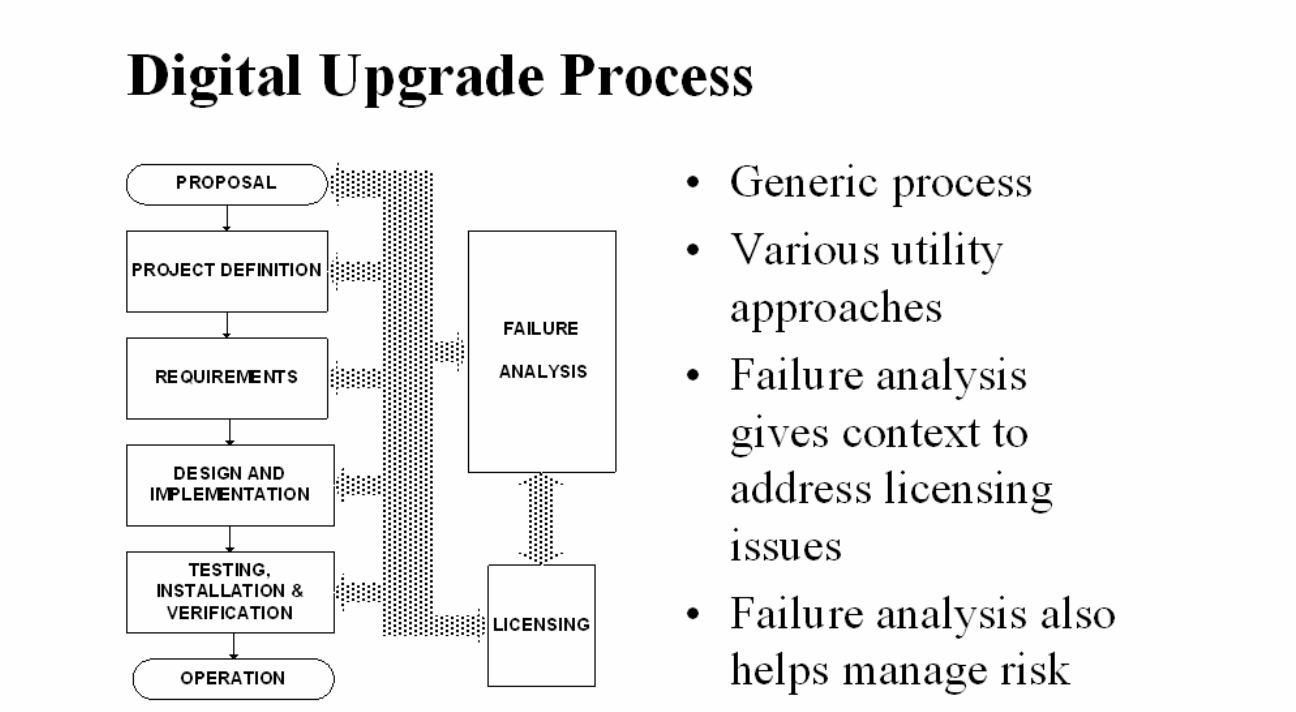


Figure 1-25 Digital Upgrade Process

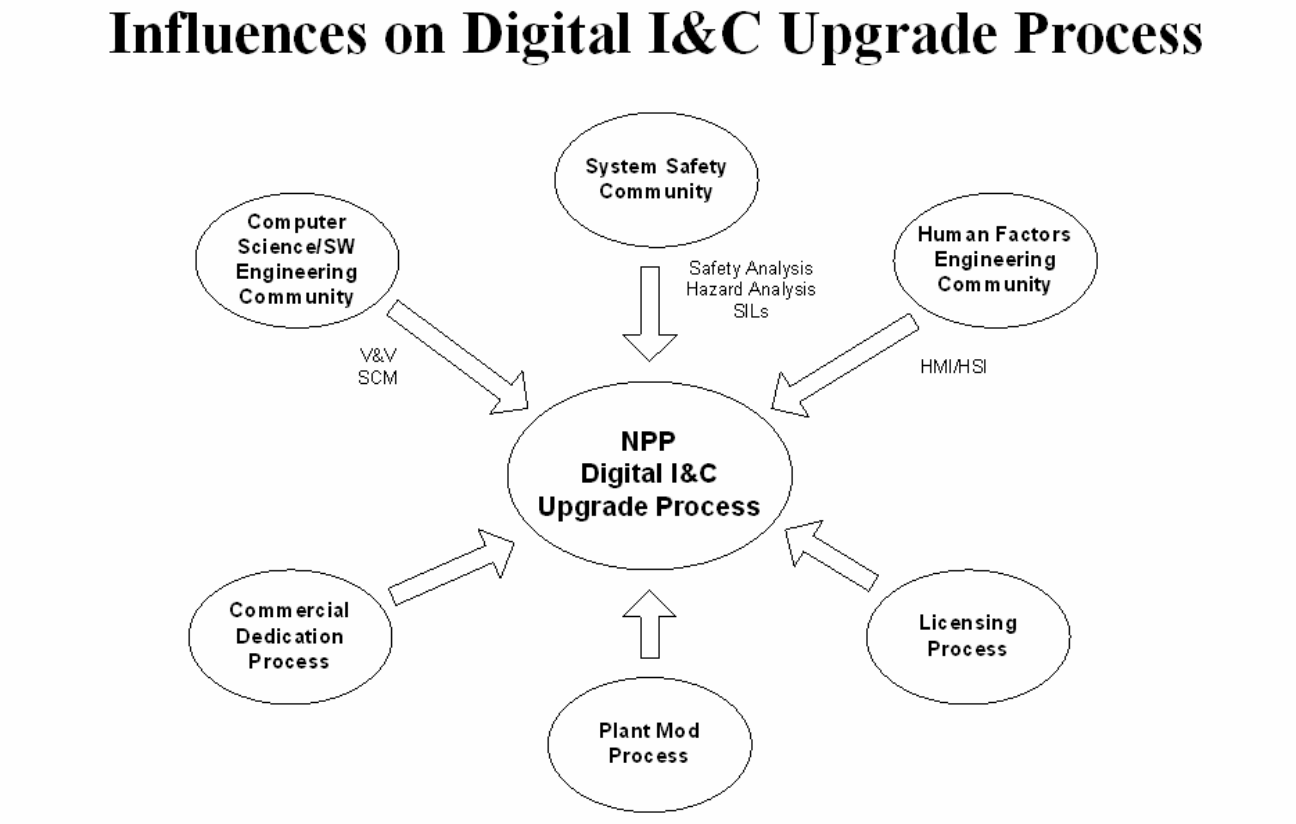


Figure 1-26 Influences on Digital I&C Upgrade Process

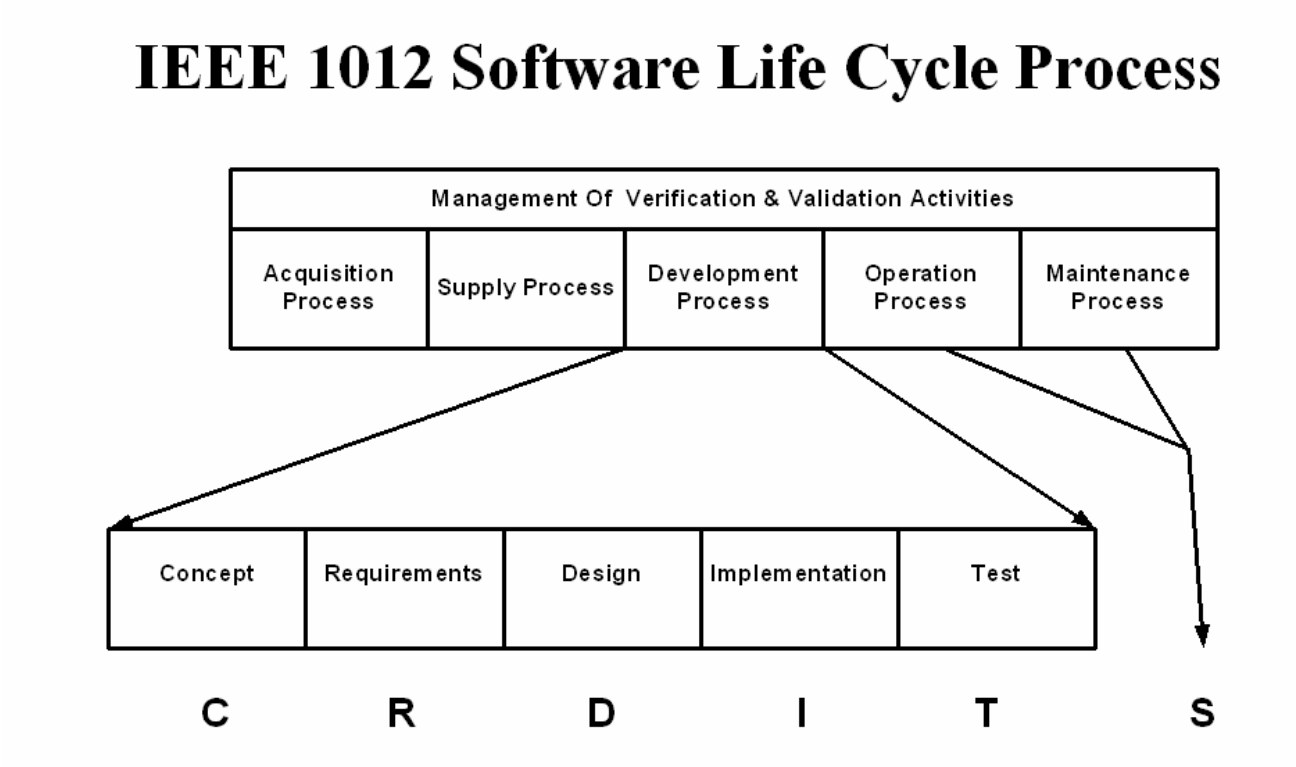


Figure 1-27 IEEE 1012 Software Life Cycle Process

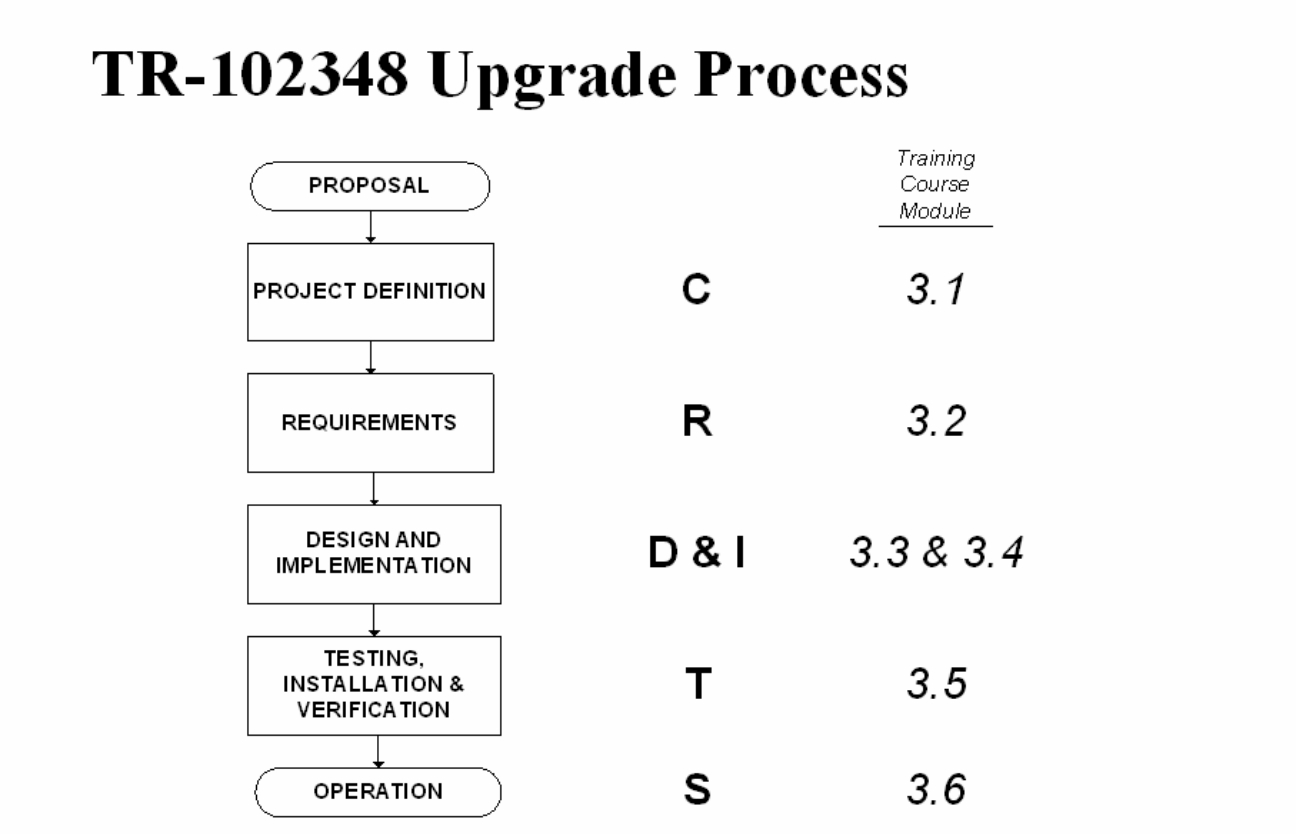


Figure 1-28 TR-102348 Upgrade Process

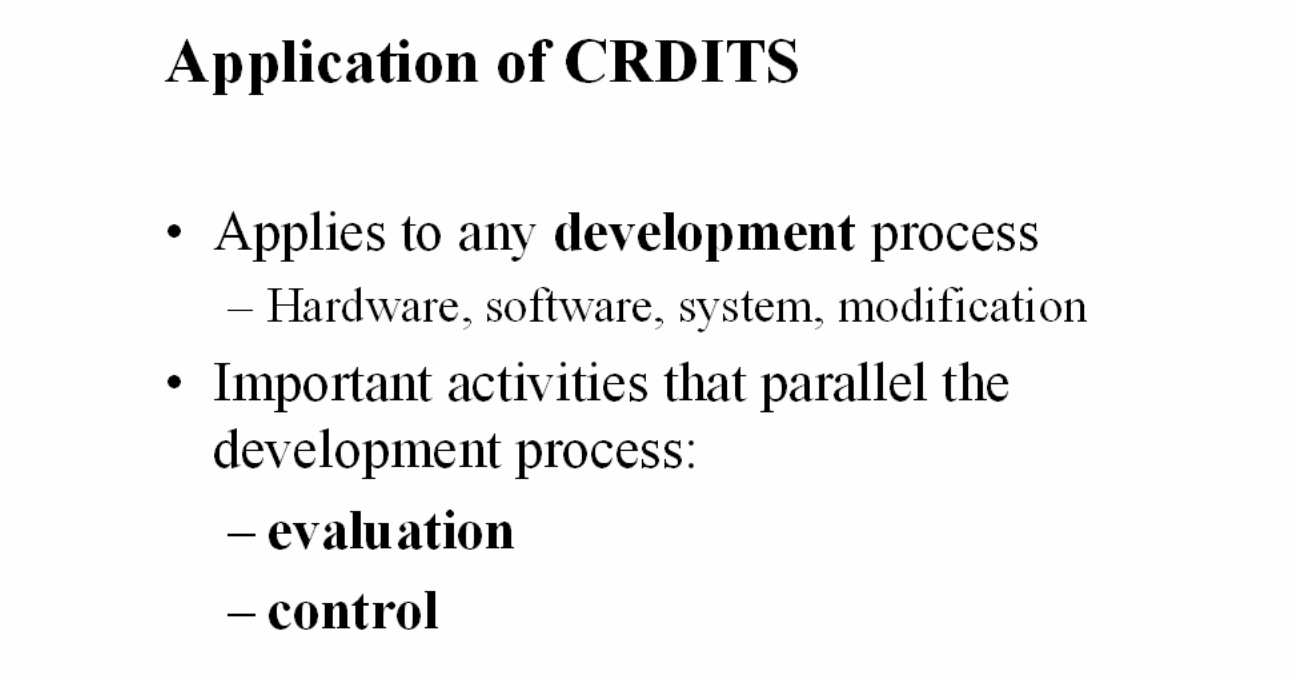


Figure 1-29 Application of CRDITS

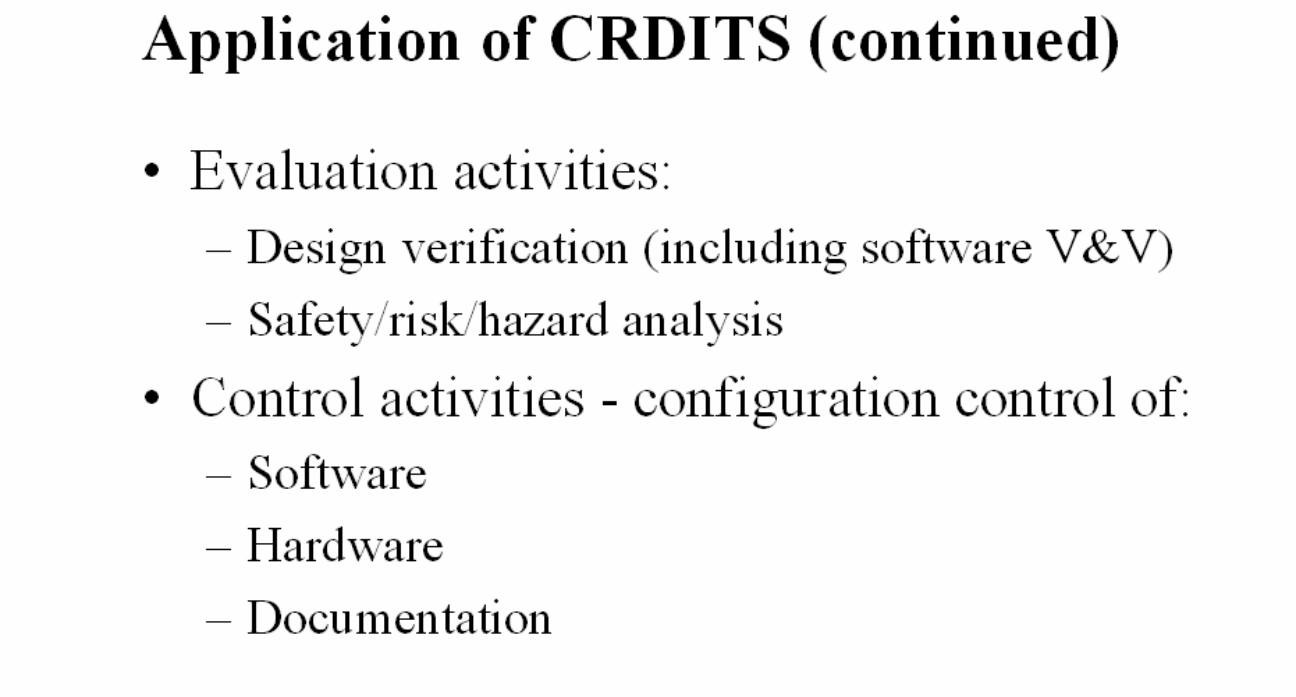


Figure 1-30 Application of CRDITS (continued)

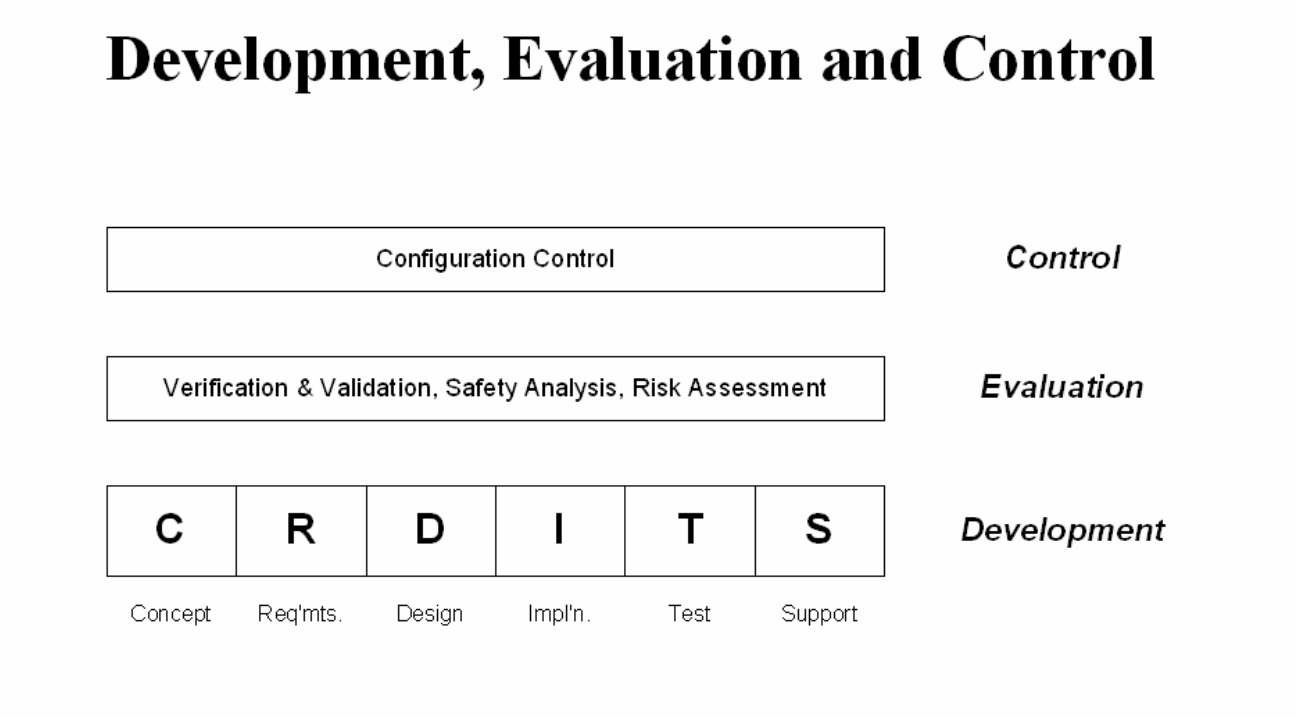


Figure 1-31 Development, Evaluation and Control

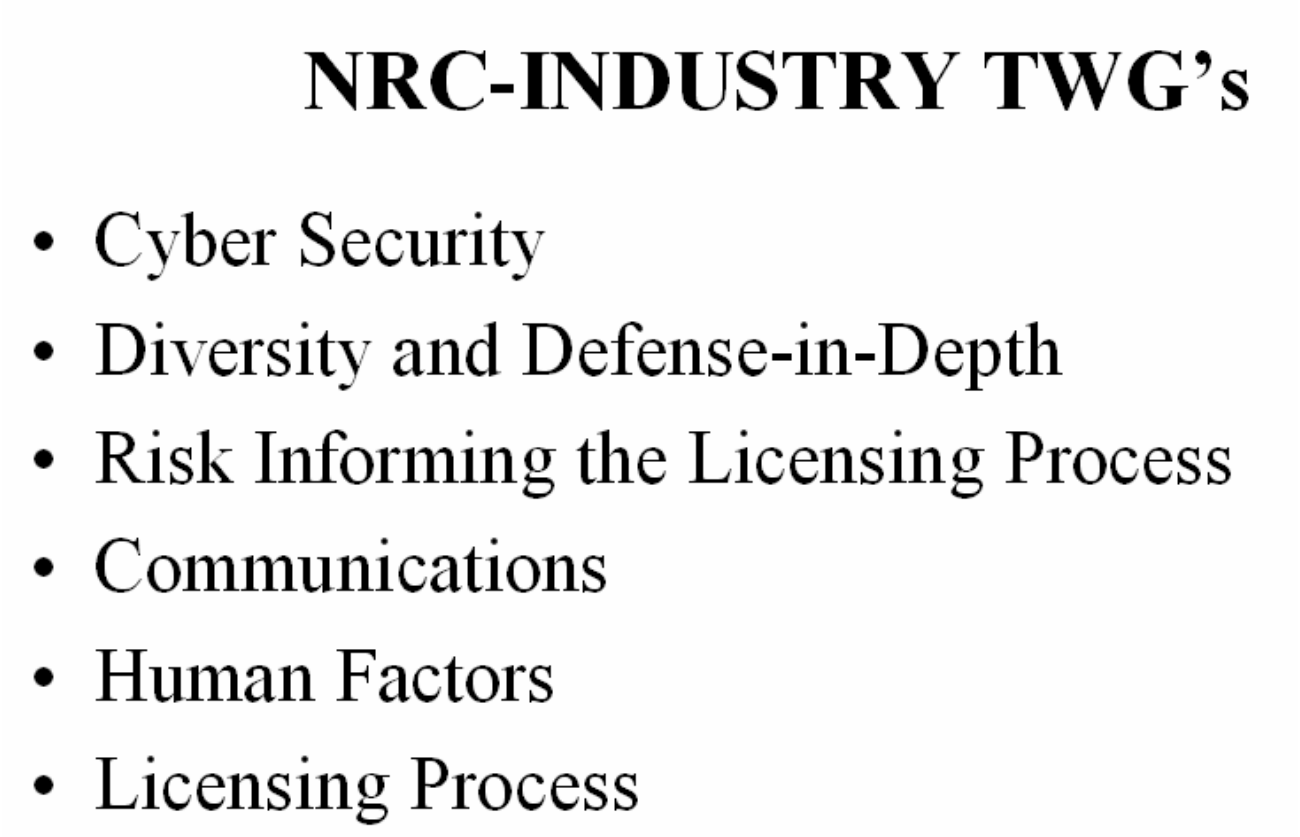


Figure 1-32 NRC-Industry TRG's

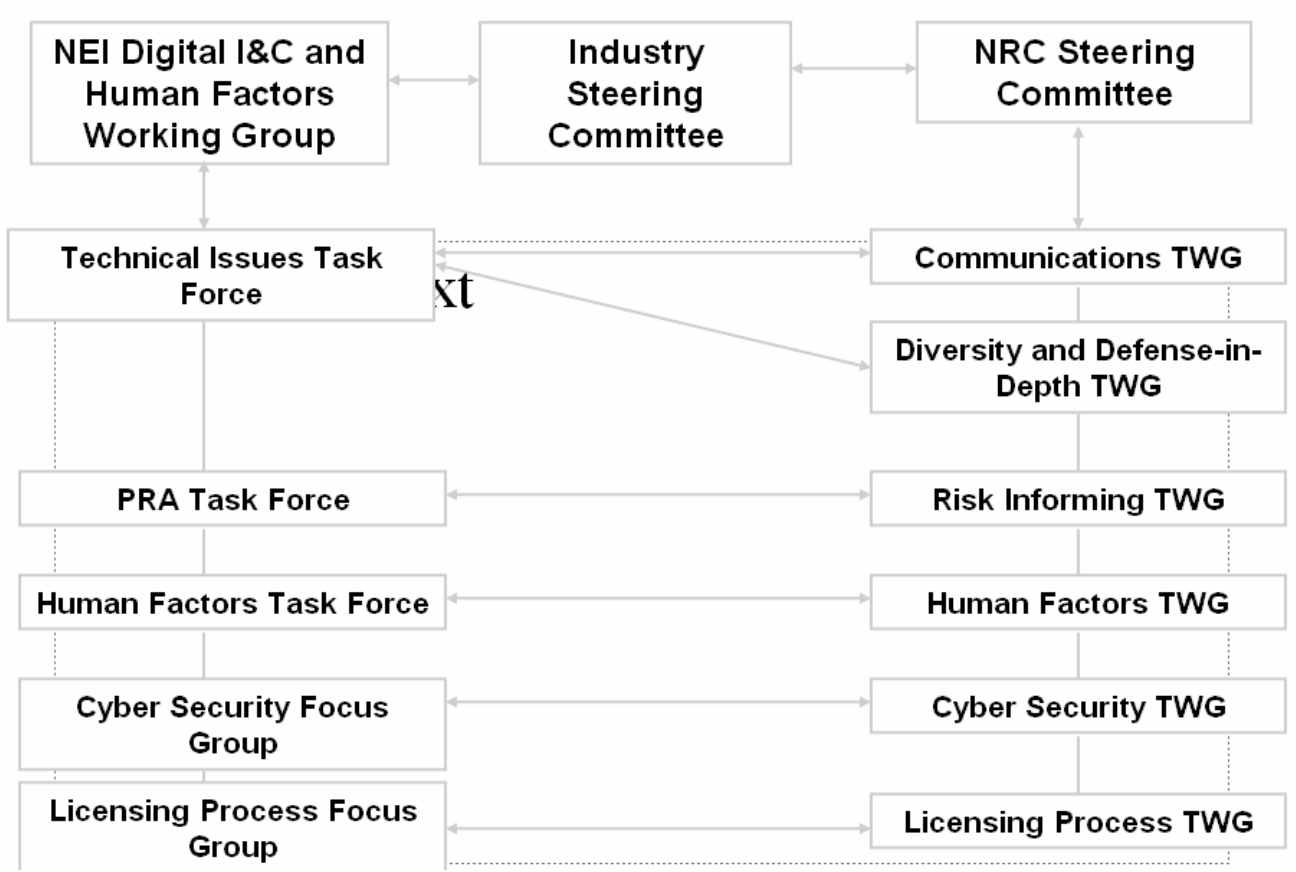


Figure 1-33 TWG Structure

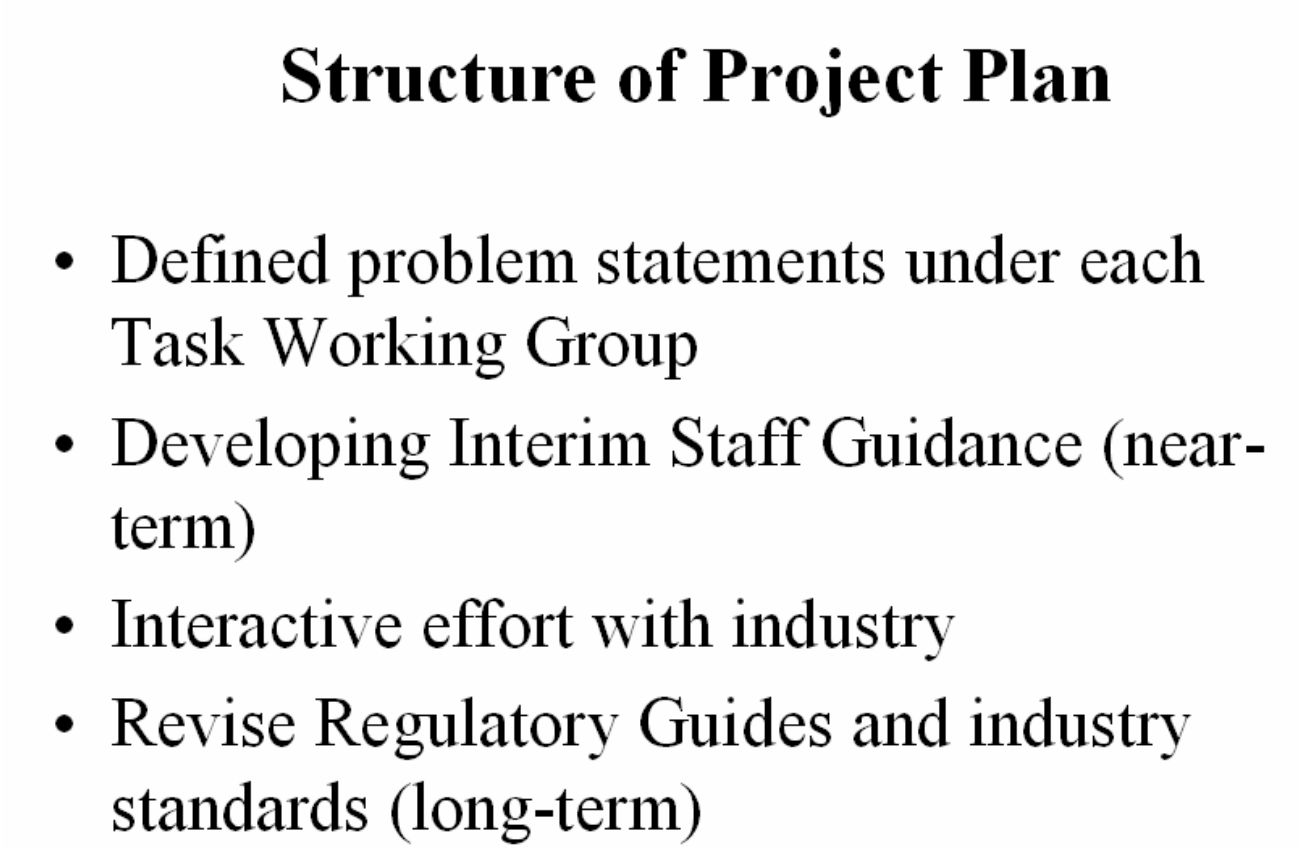


Figure 1-34 Project Plan Structure

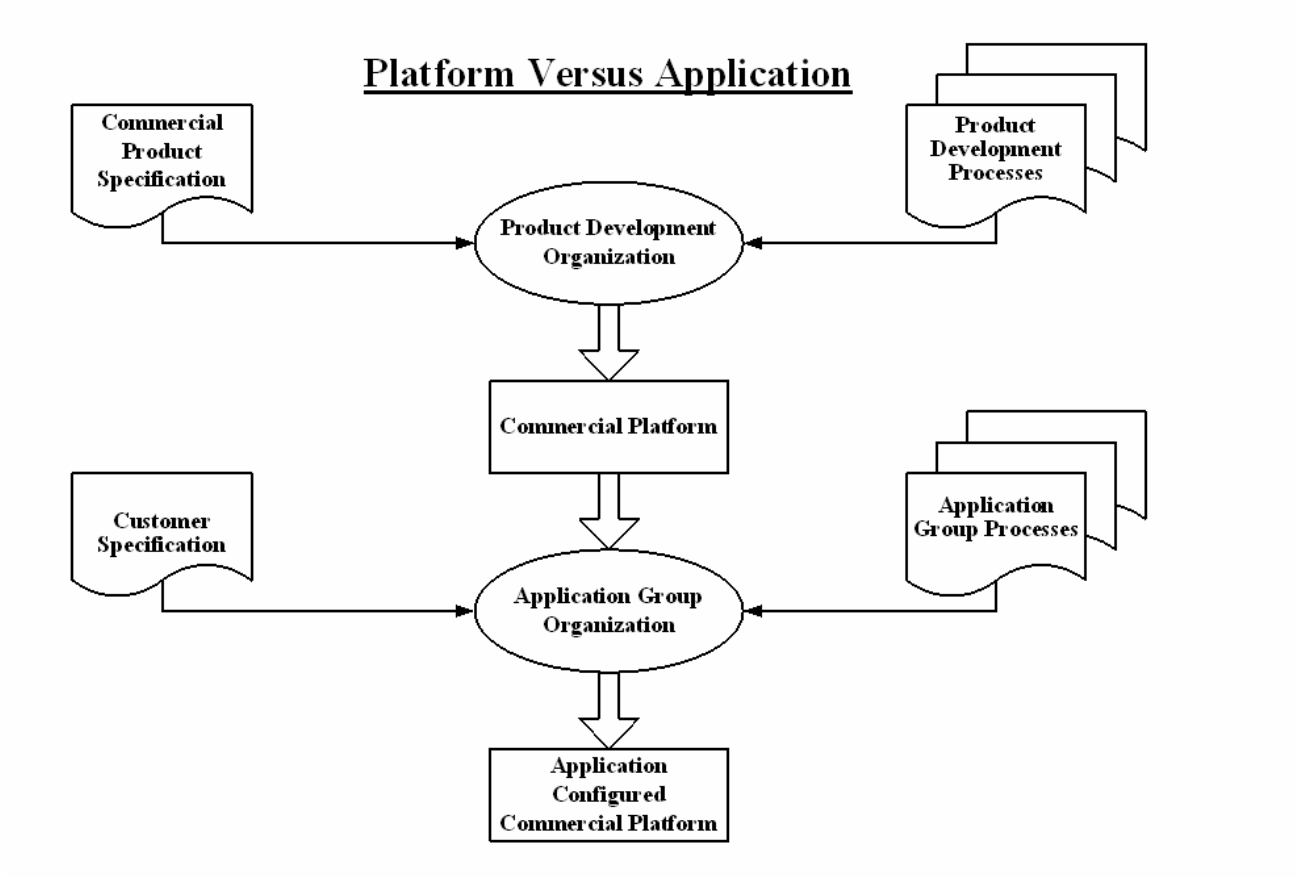


Figure 1-35 Platform versus Application

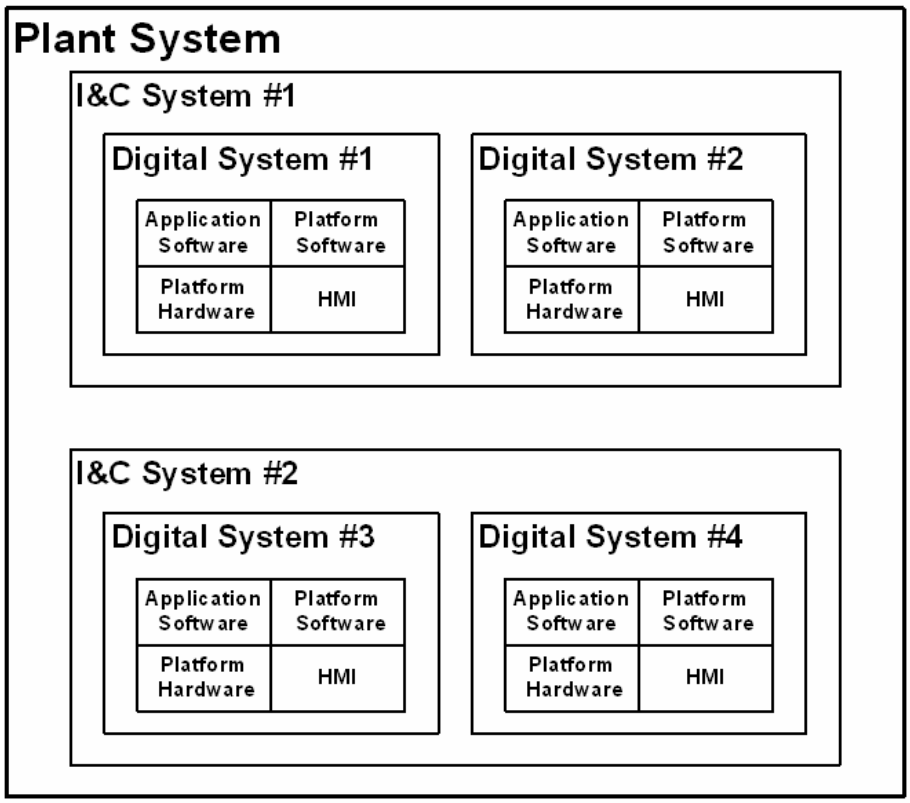


Figure 1-36 Plant System

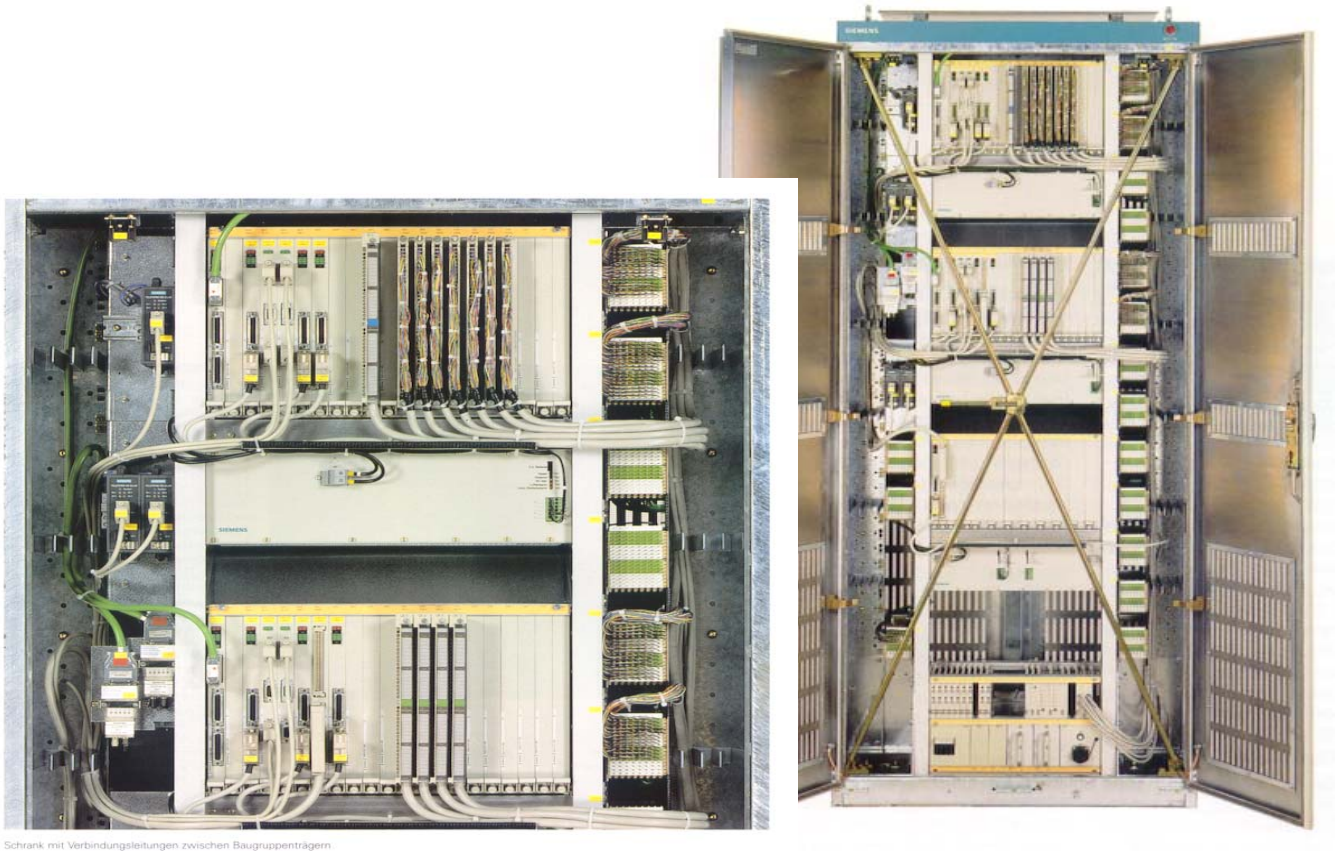


Figure 1-37 Teleperm XS Cabinets

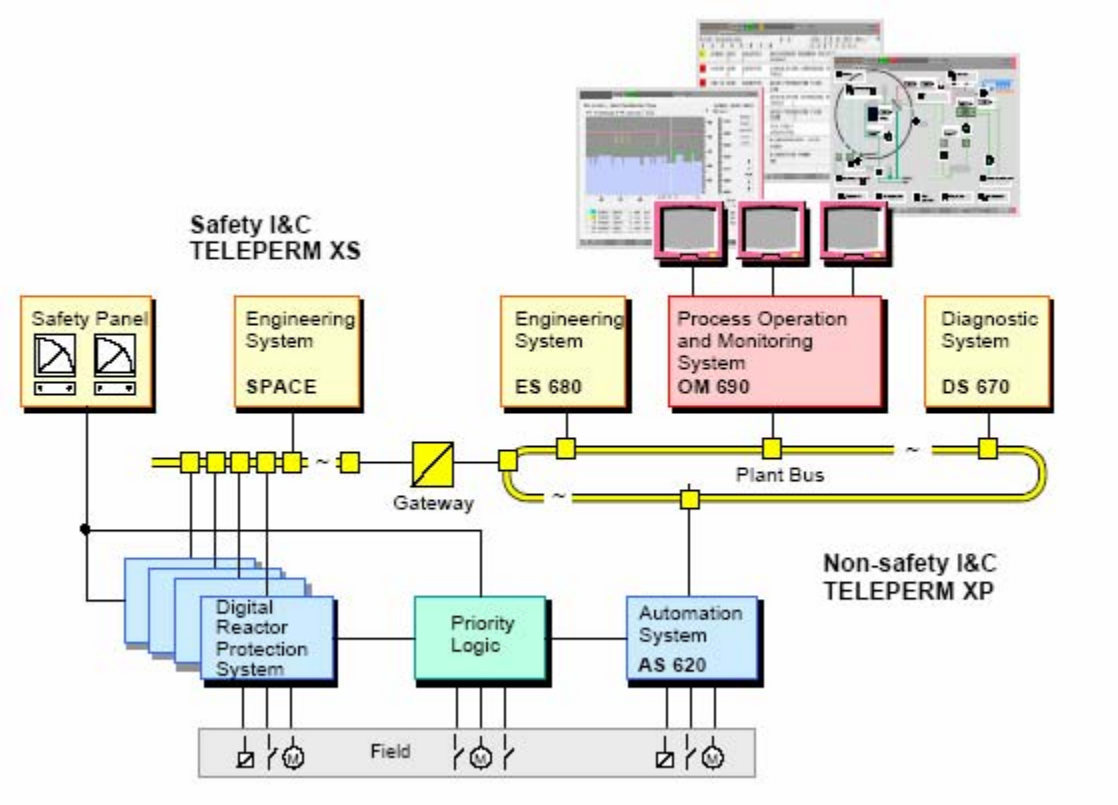


Figure 1-38 Overall Teleperm Architecture

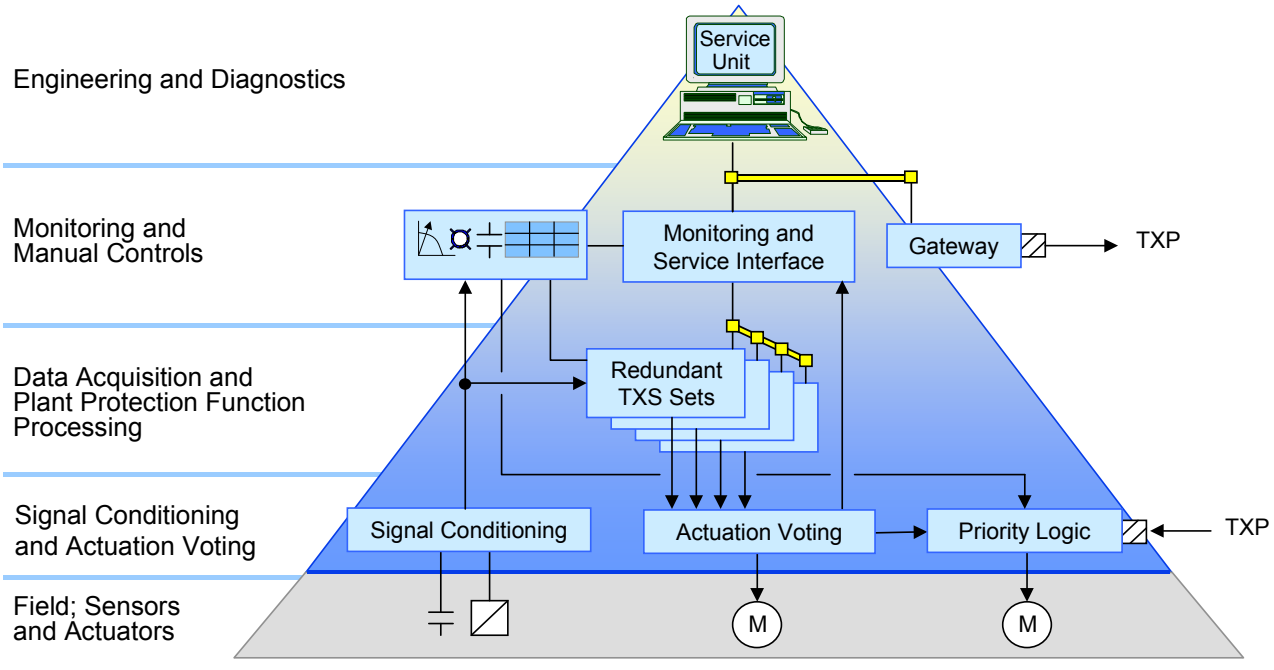


Figure 1-39 Teleperm XS Hierarchy

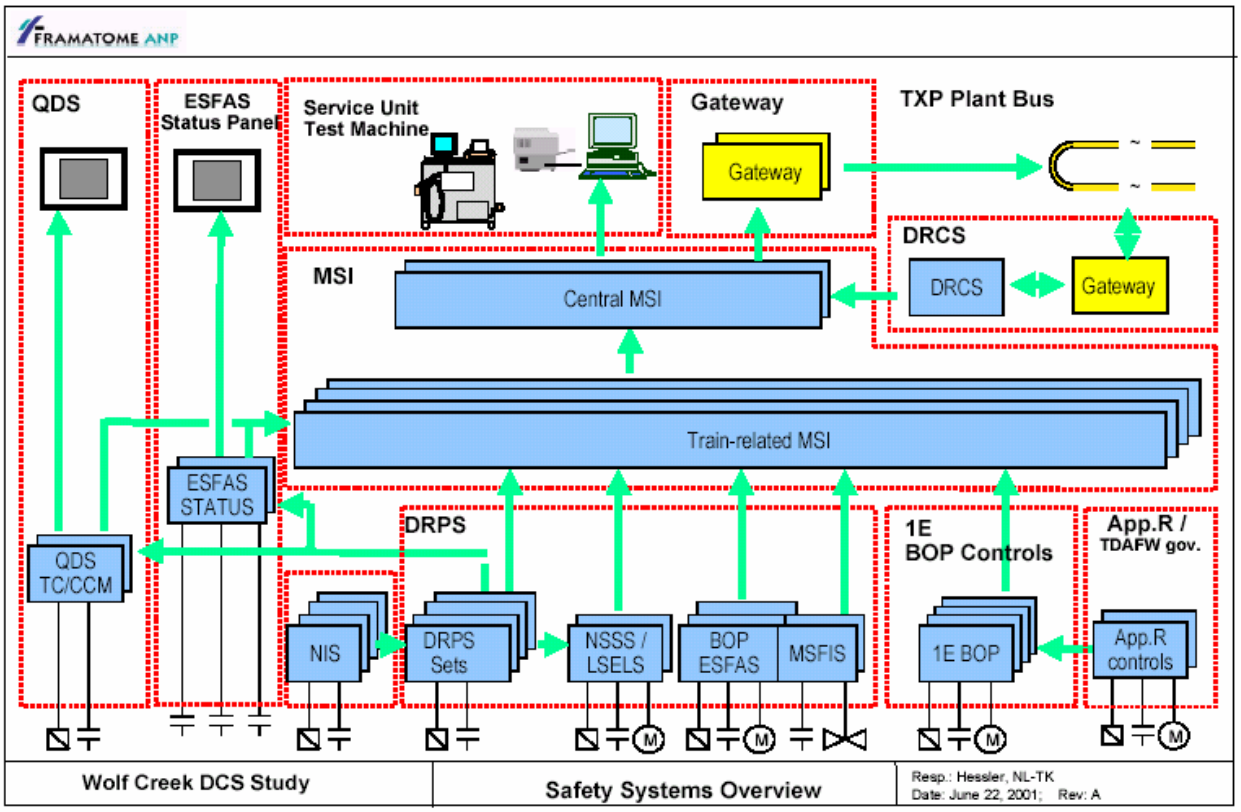


Figure 1-40 Teleperm XS Safety System Overview

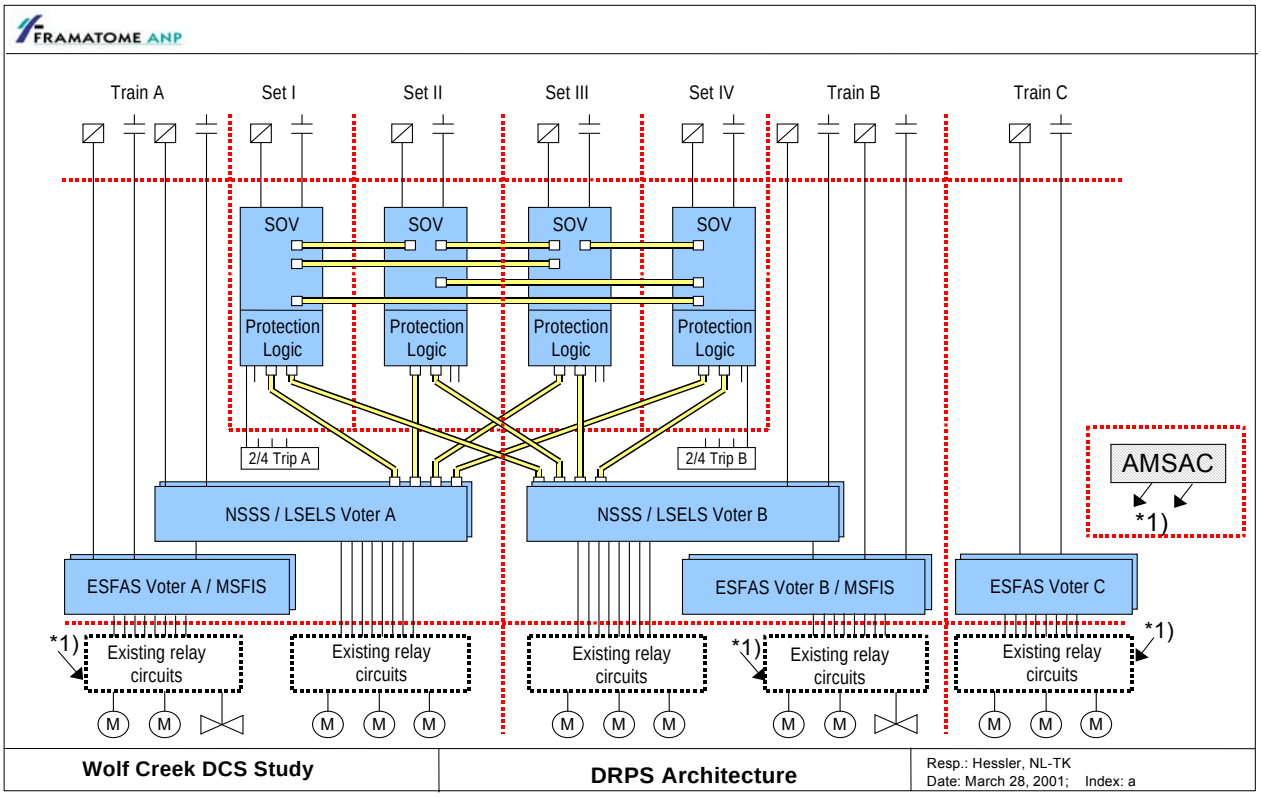


Figure 1-41 Teleperm XS Safety System Architecture

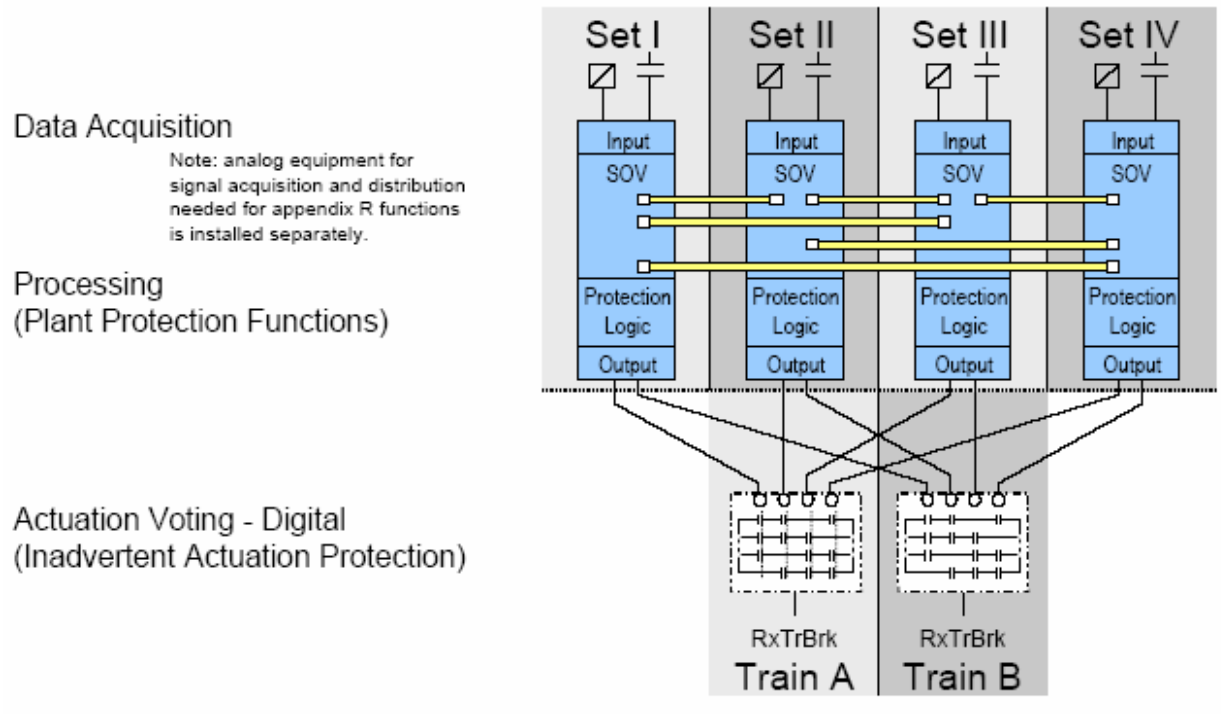


Figure 1-42 Teleperm XS Reactor Trip System Architecture

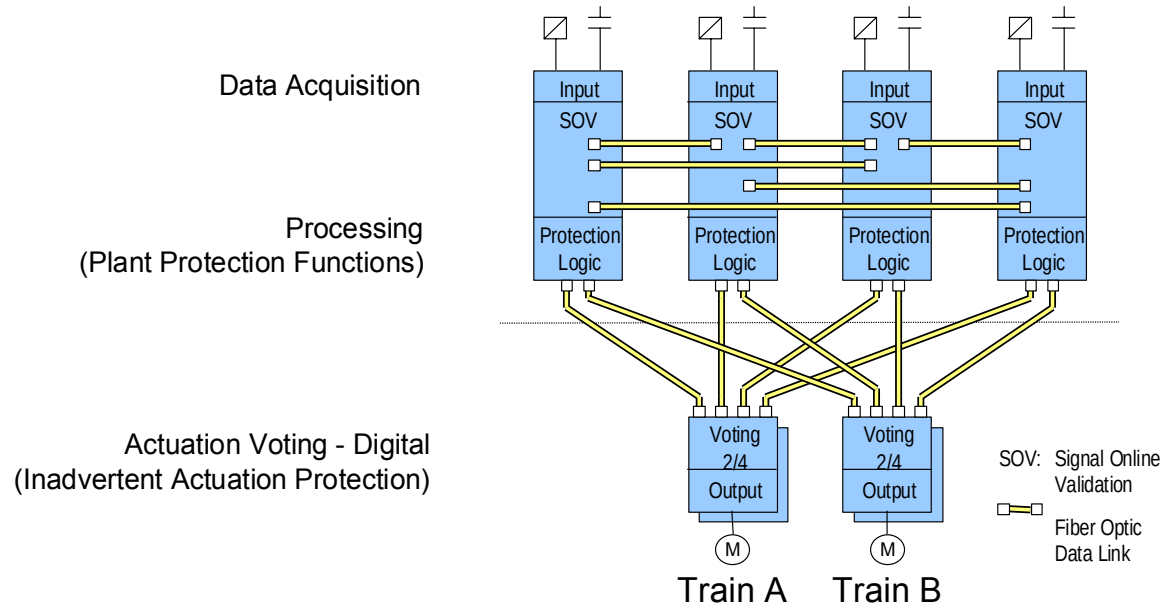


Figure 1-43 Teleperm XS Engineered Safeguards Voters

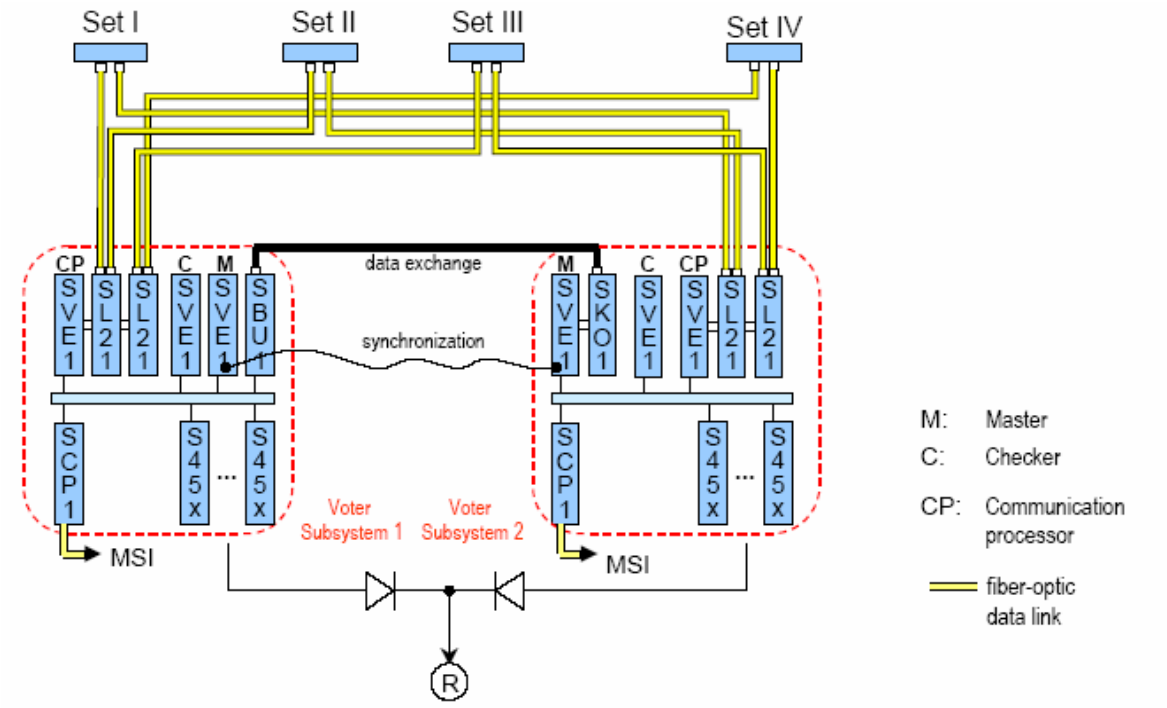


Figure 1-44 Teleperm XS ESFAS Voter Configuration

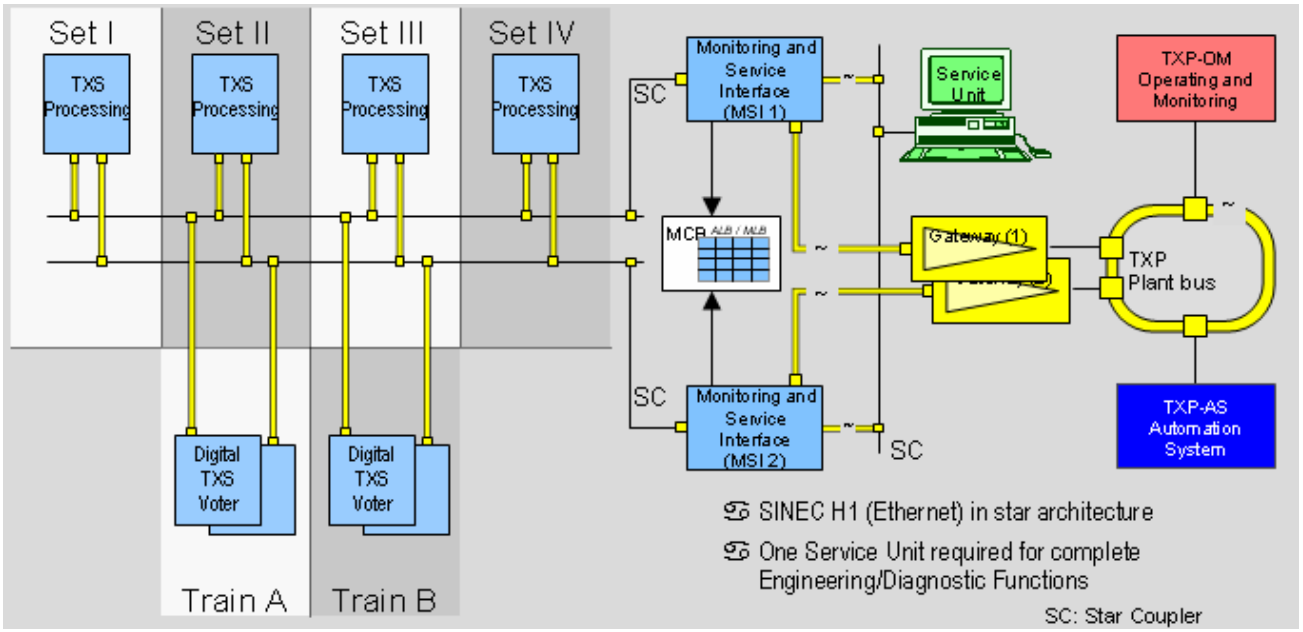


Figure 1-45 Teleperm XS Monitoring & Service Interface

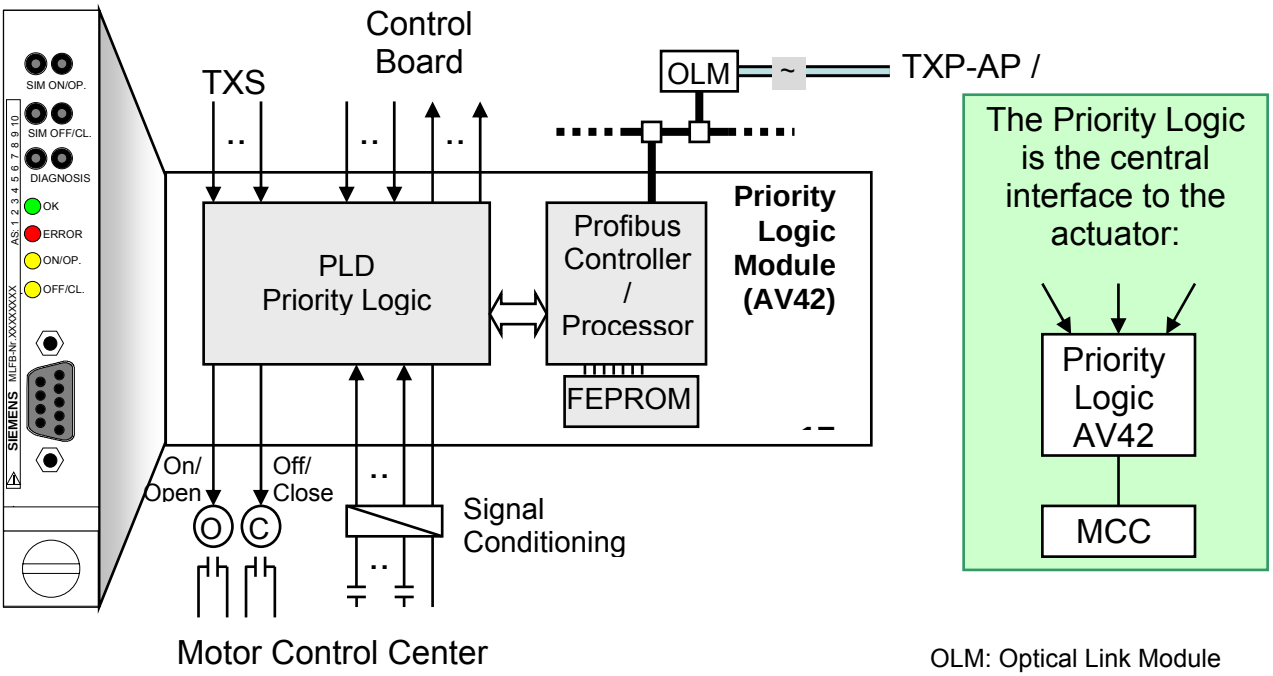


Figure 1-46 Teleperm XS Priority Logic Module

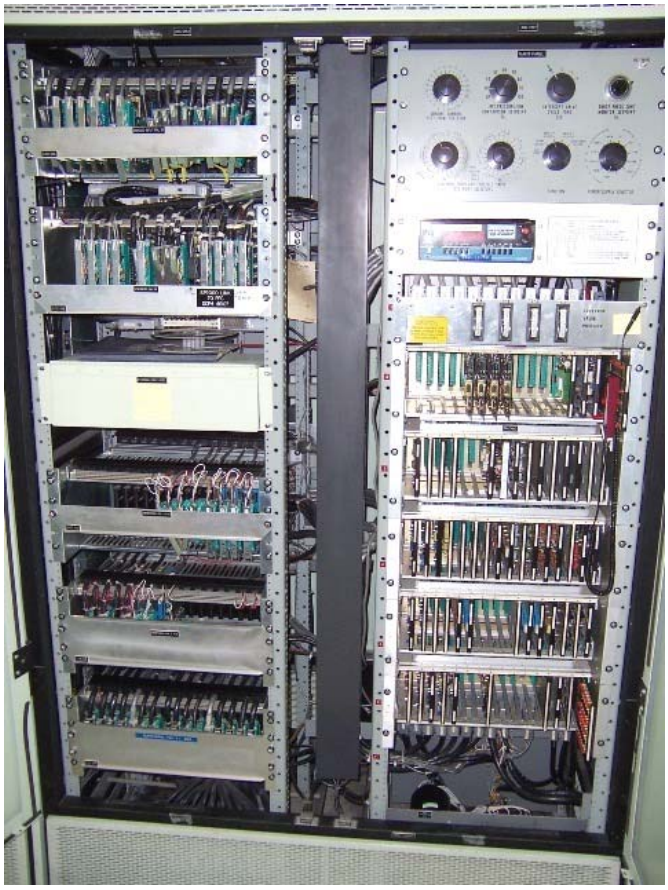


Figure 1-47 Old P2000 Equipment

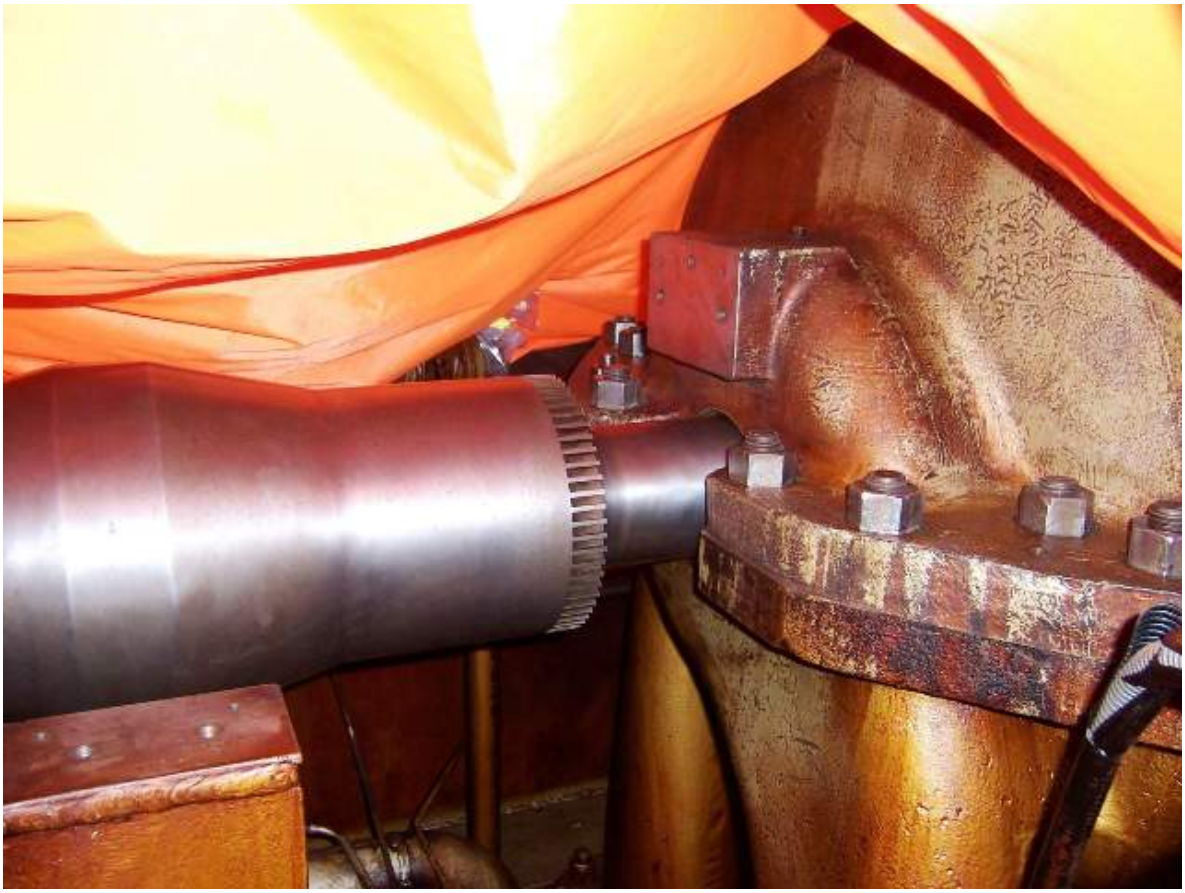


Figure 1-48 New Speed Pickup Gear

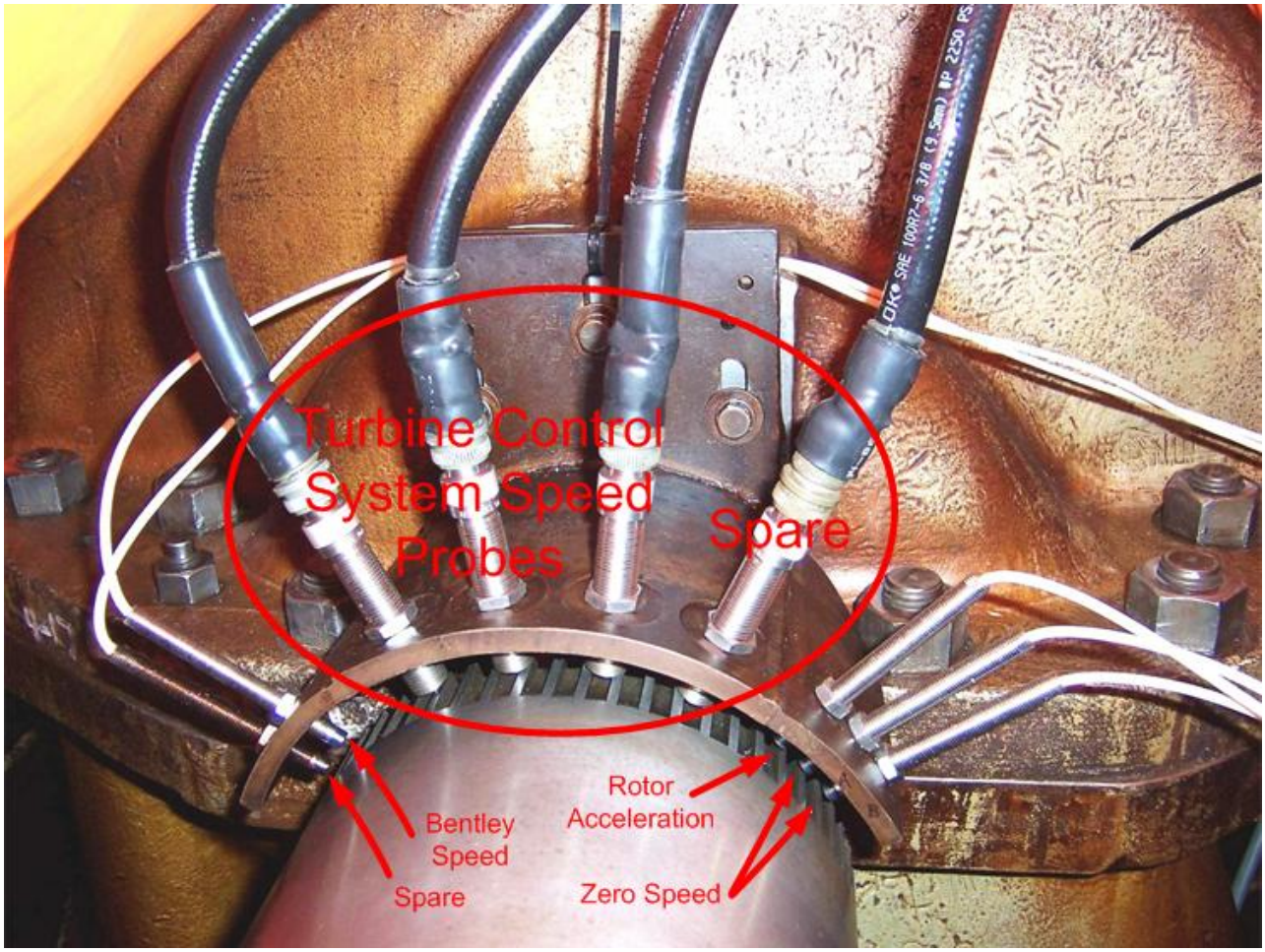


Figure 1-49 New Speed Pickup Probes

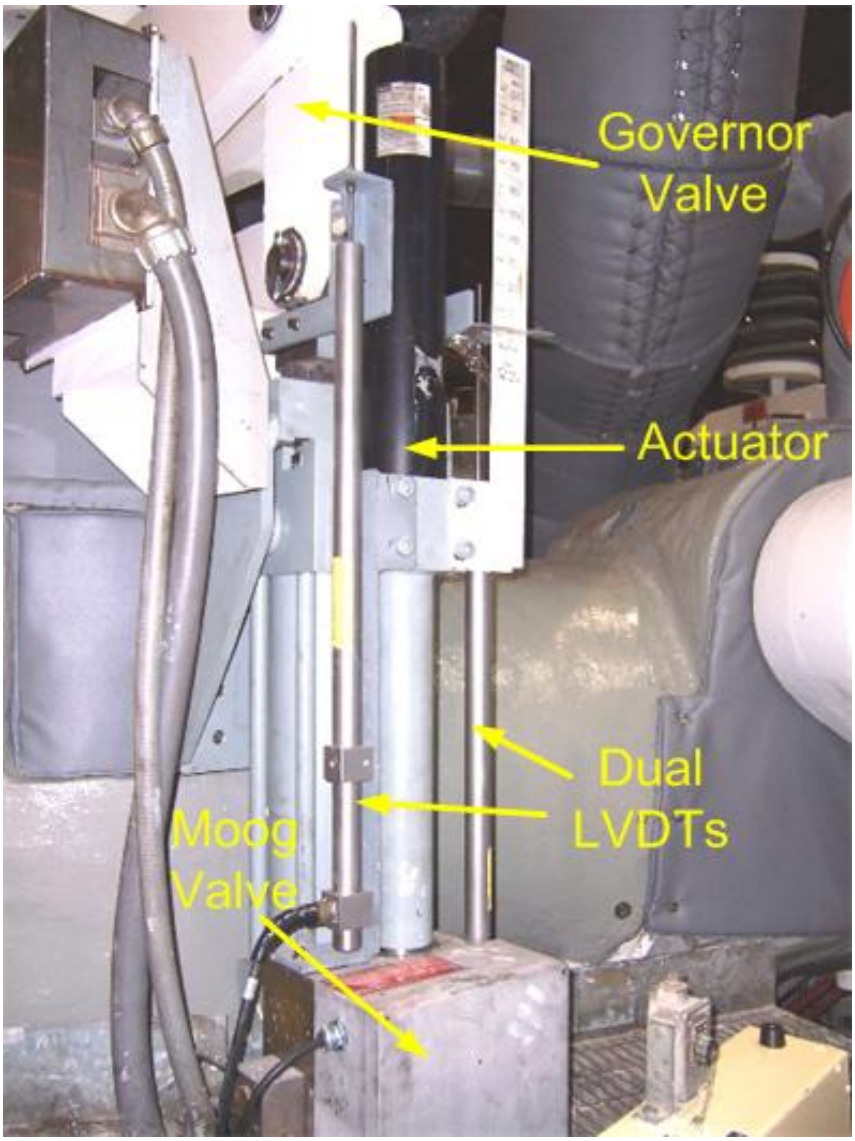


Figure 1-50 New Dual LVDT Sensors on Governor Valves

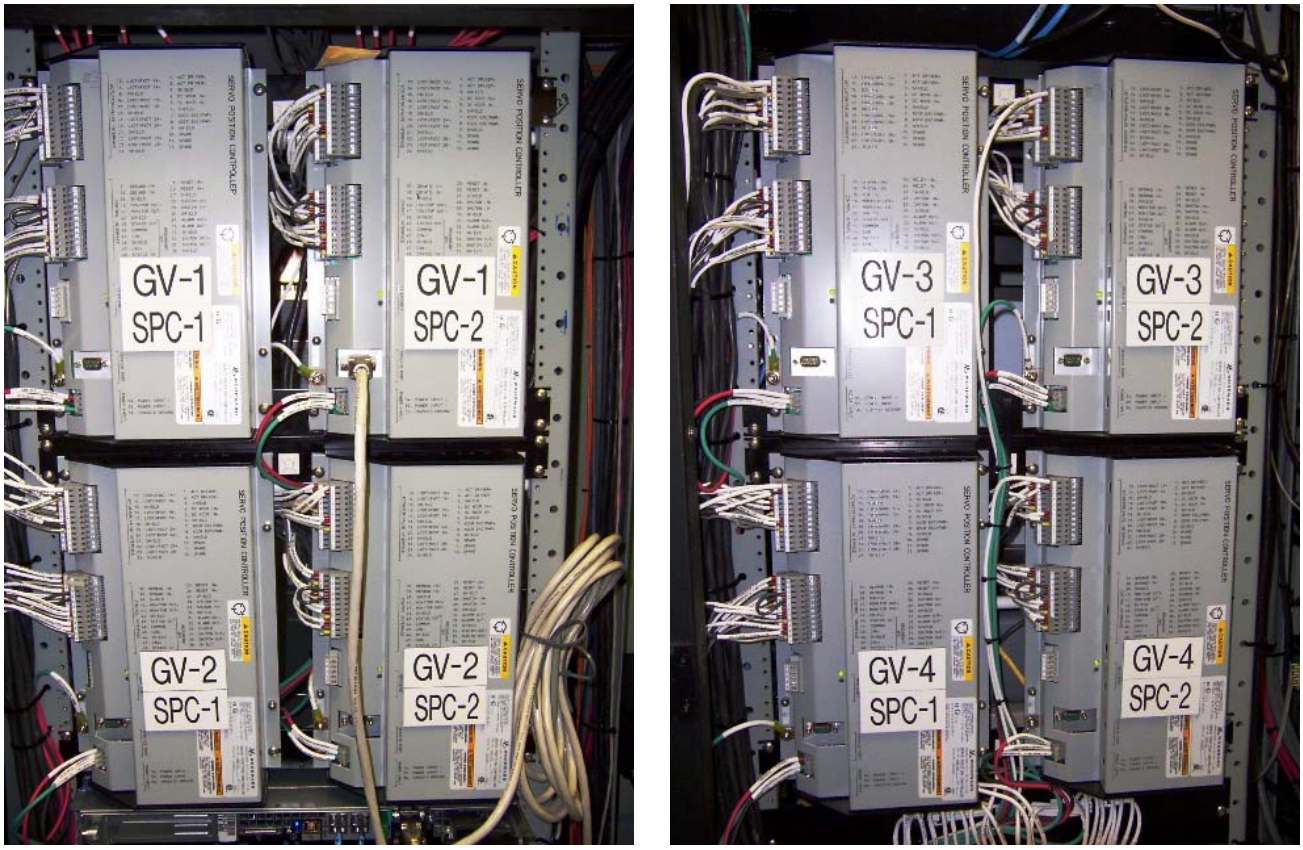


Figure 1-51 Dual Servo Positioners for Each Governor Valve

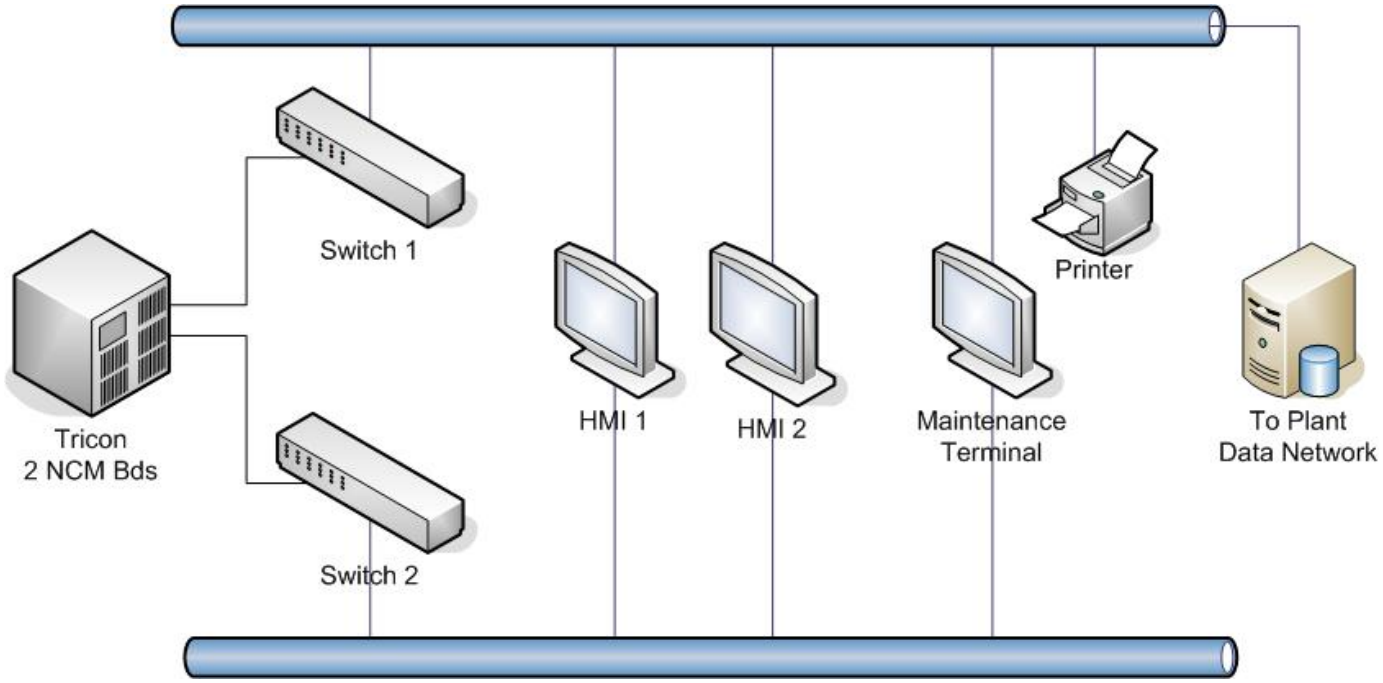


Figure 1-52 Main Turbine Control System Network Architecture

Figure 1-53 New Equipment Mounted in Cabinets

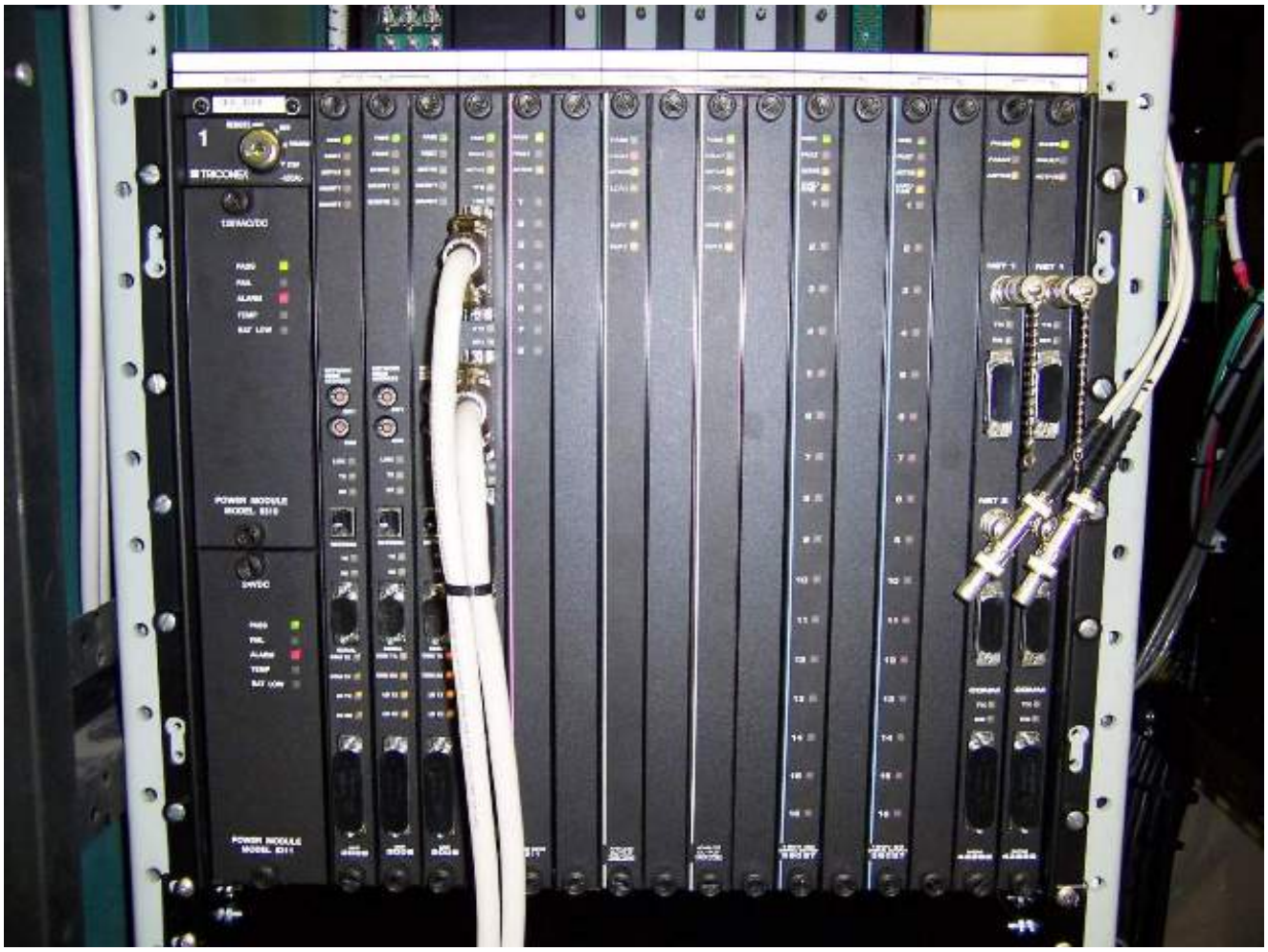


Figure 1-54 Main Processor Chassis

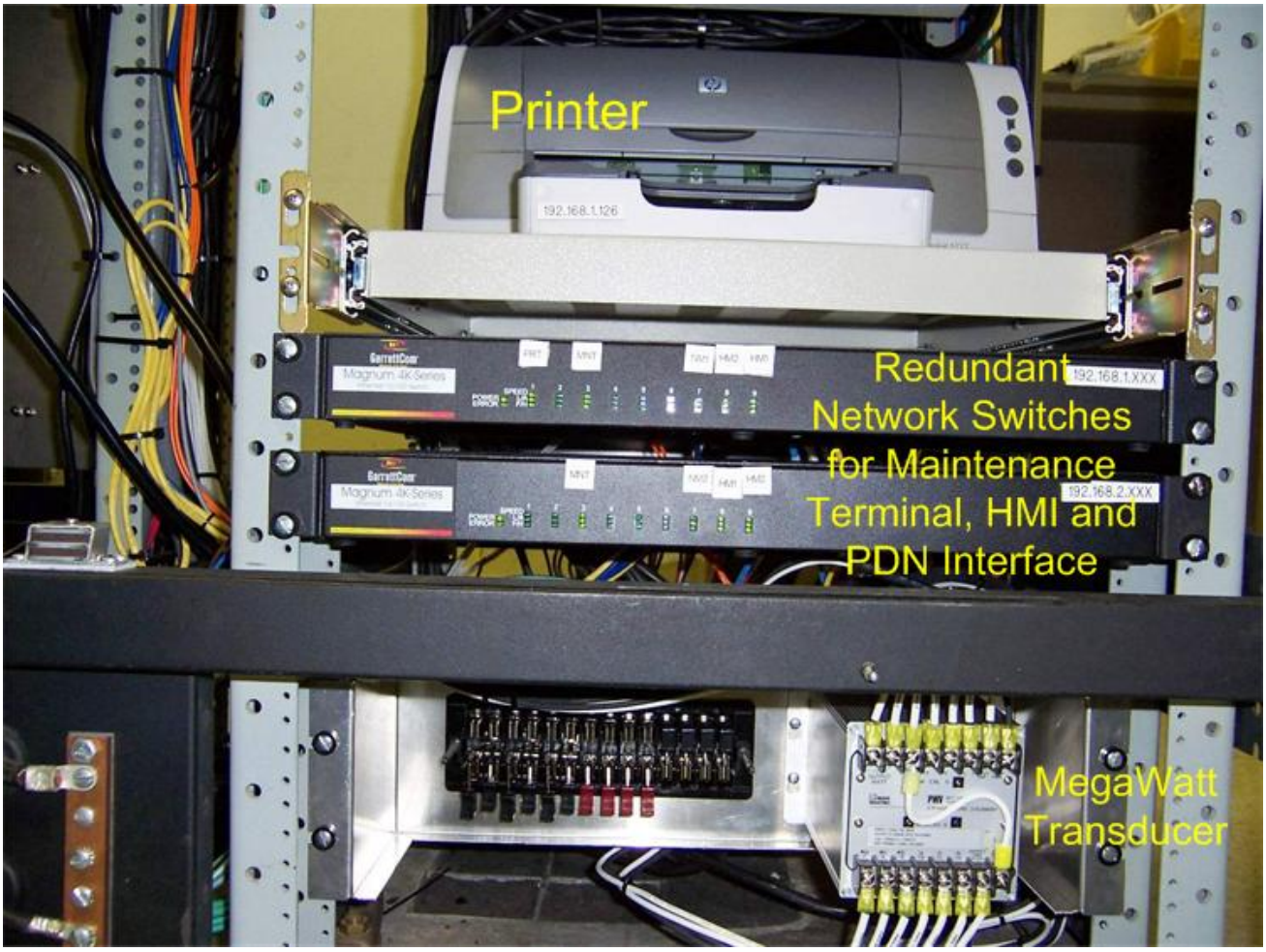


Figure 1-55 Redundant Network

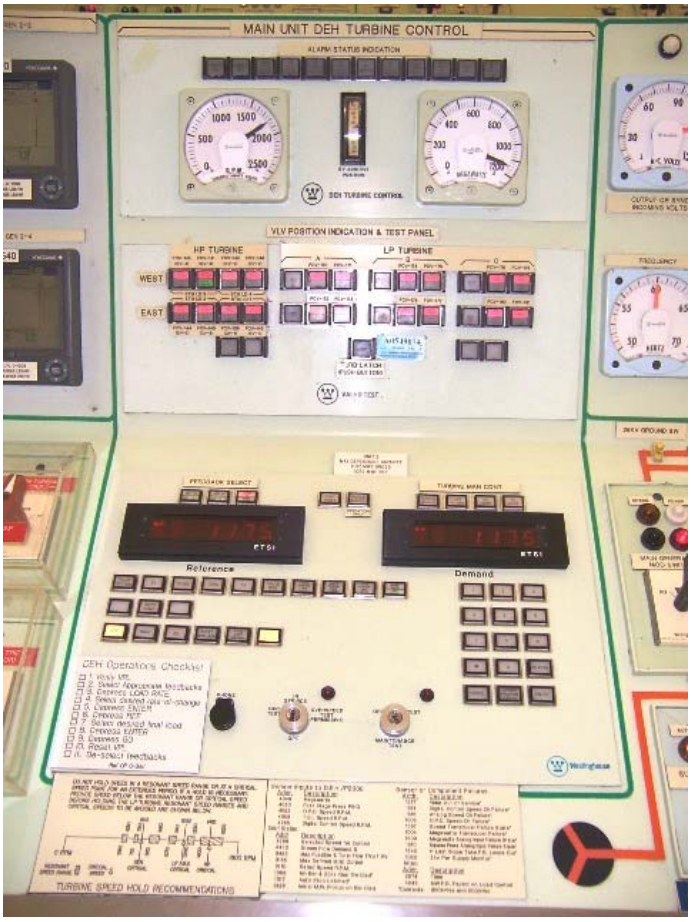
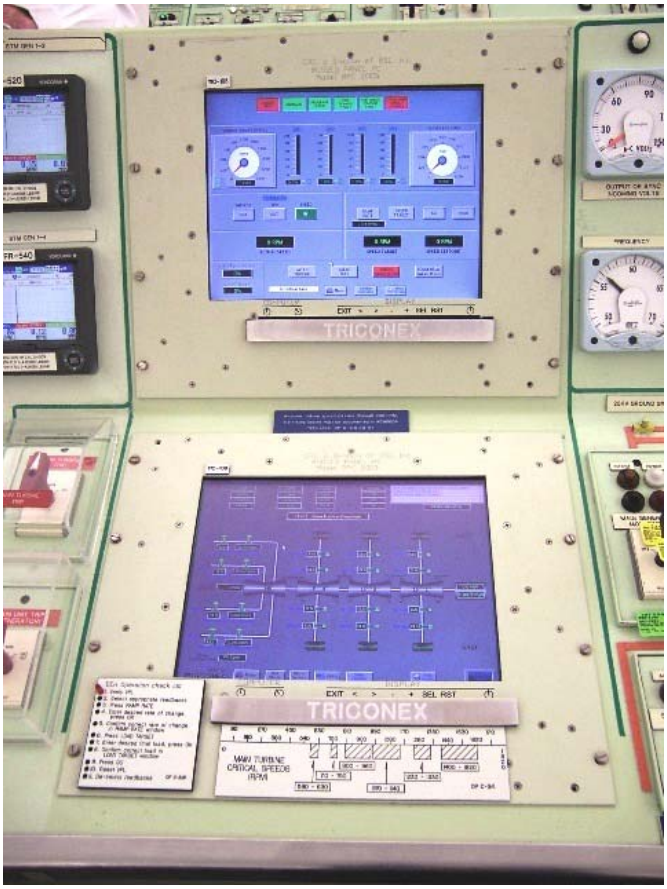


Figure 1-56 Human Machine Interface (HMI)



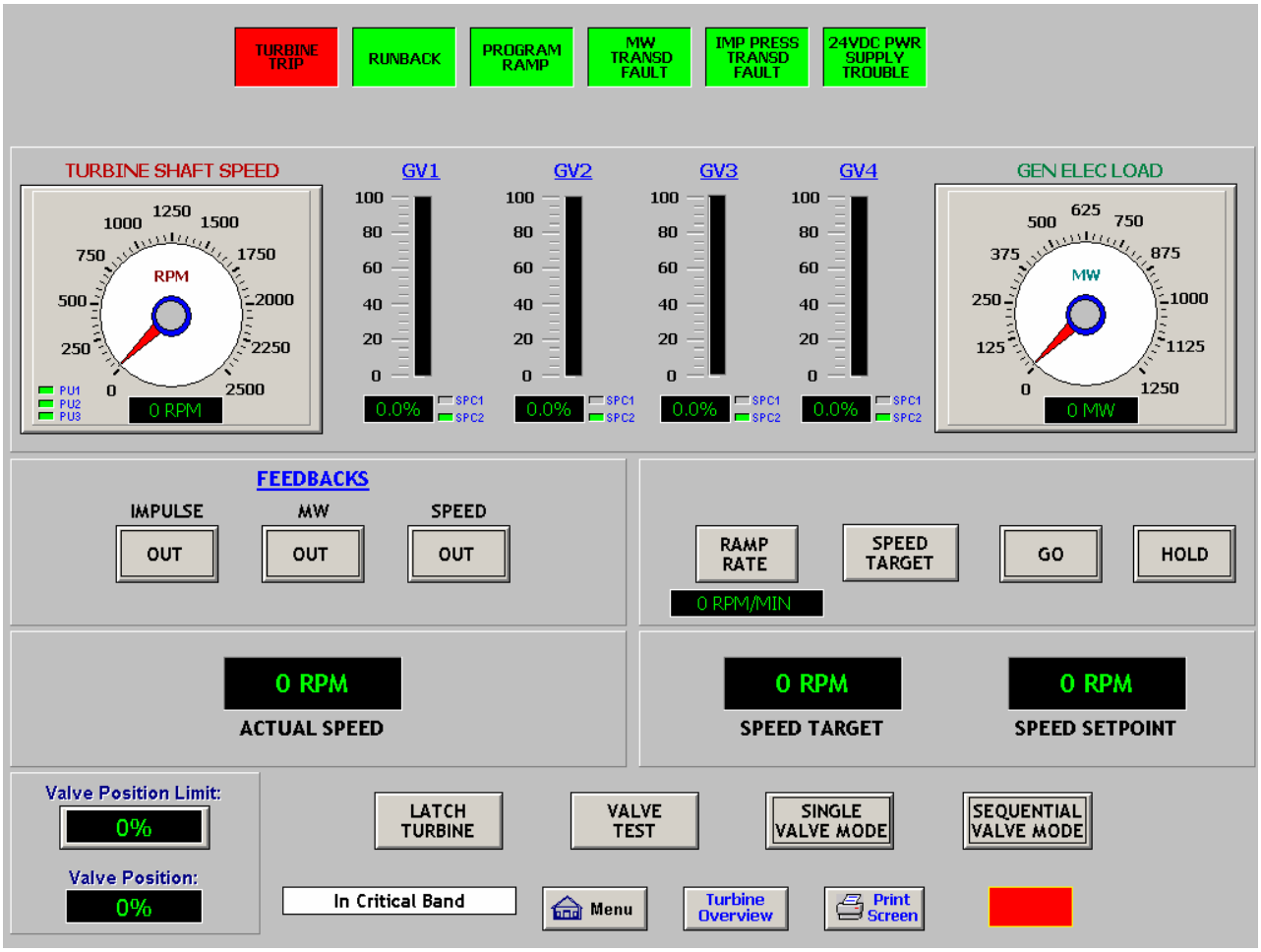


Figure 1-57 Main Screen

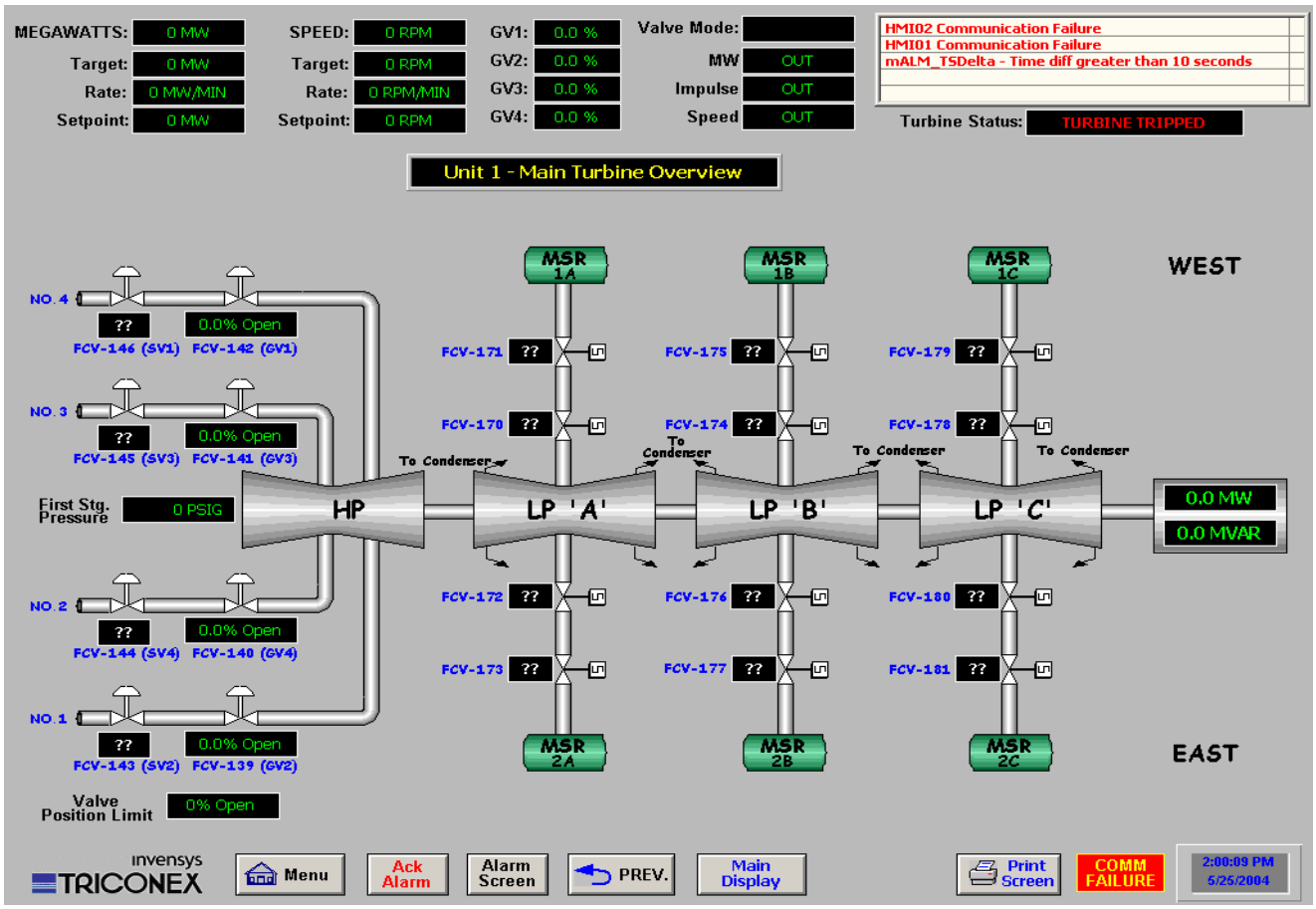


Figure 1-58 Main Turbine Overview Screen

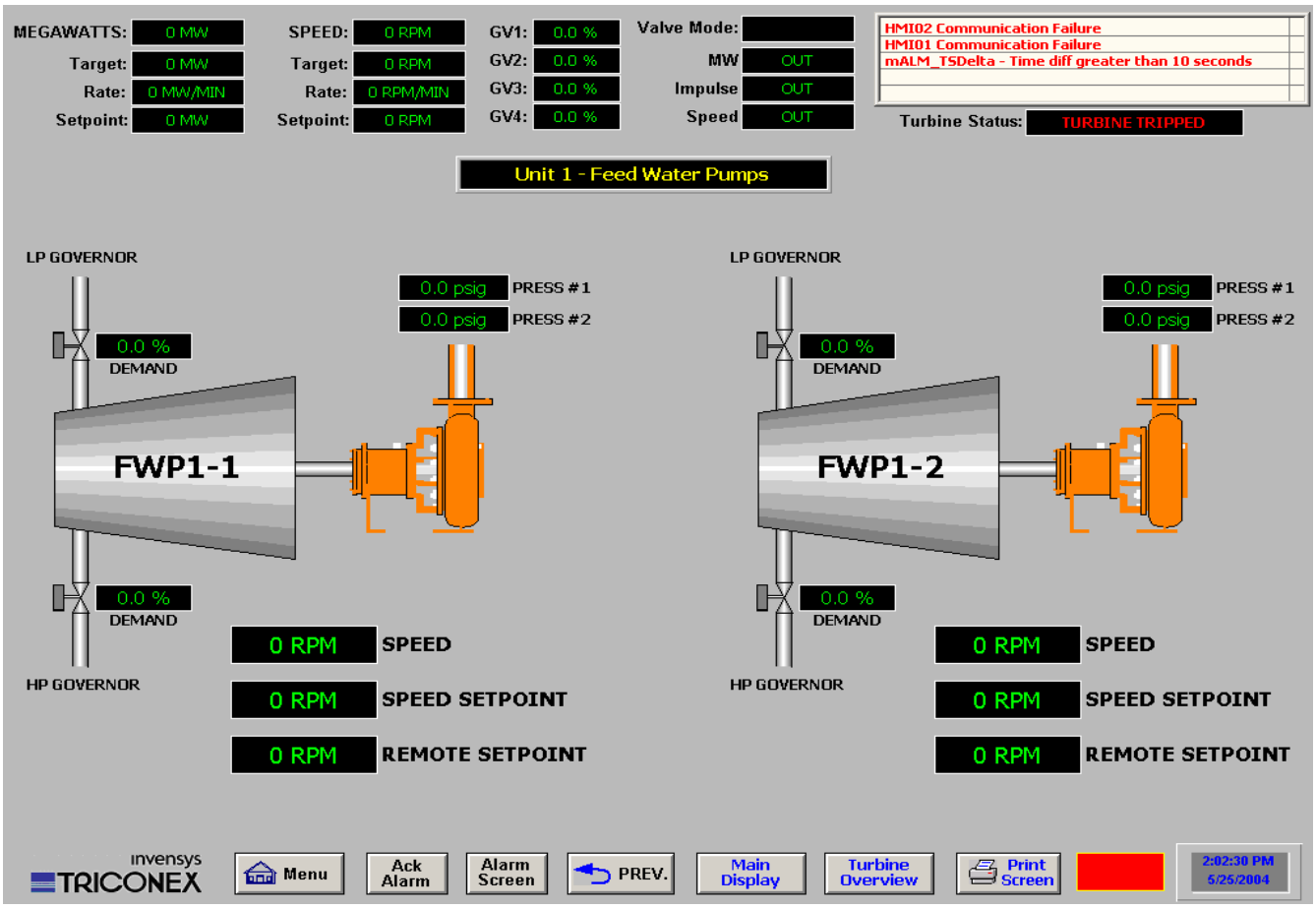


Figure 1-59 Feedwater Pumps Overview

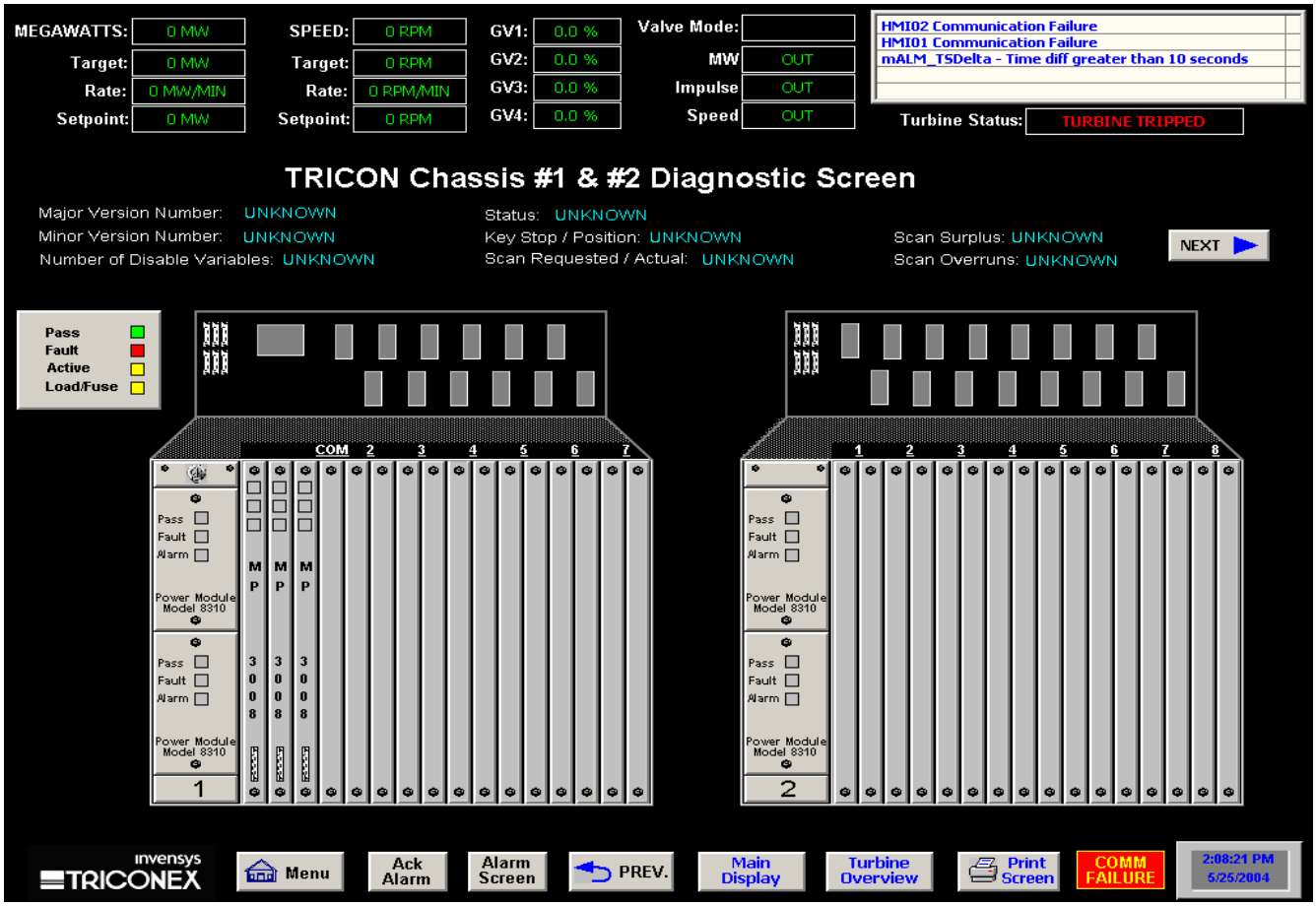


Figure 1-60 Tricon Diagnostics

Figure 1-61 Comparison of Protective Relaying Equipment from 1925 and 1994

Figure 1-62 Gas-Insulated Substation Bay with Integrated Control Cubicle

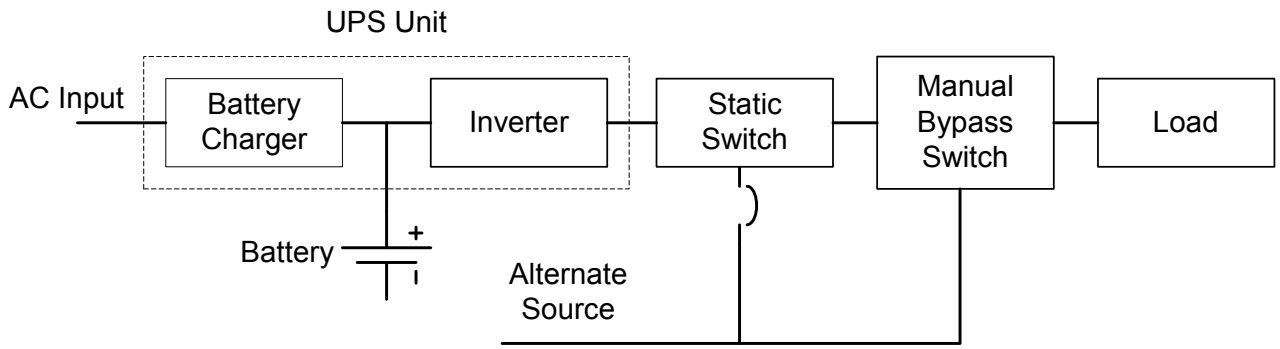


Figure 1-63 Single Unit Float UPS Configuration

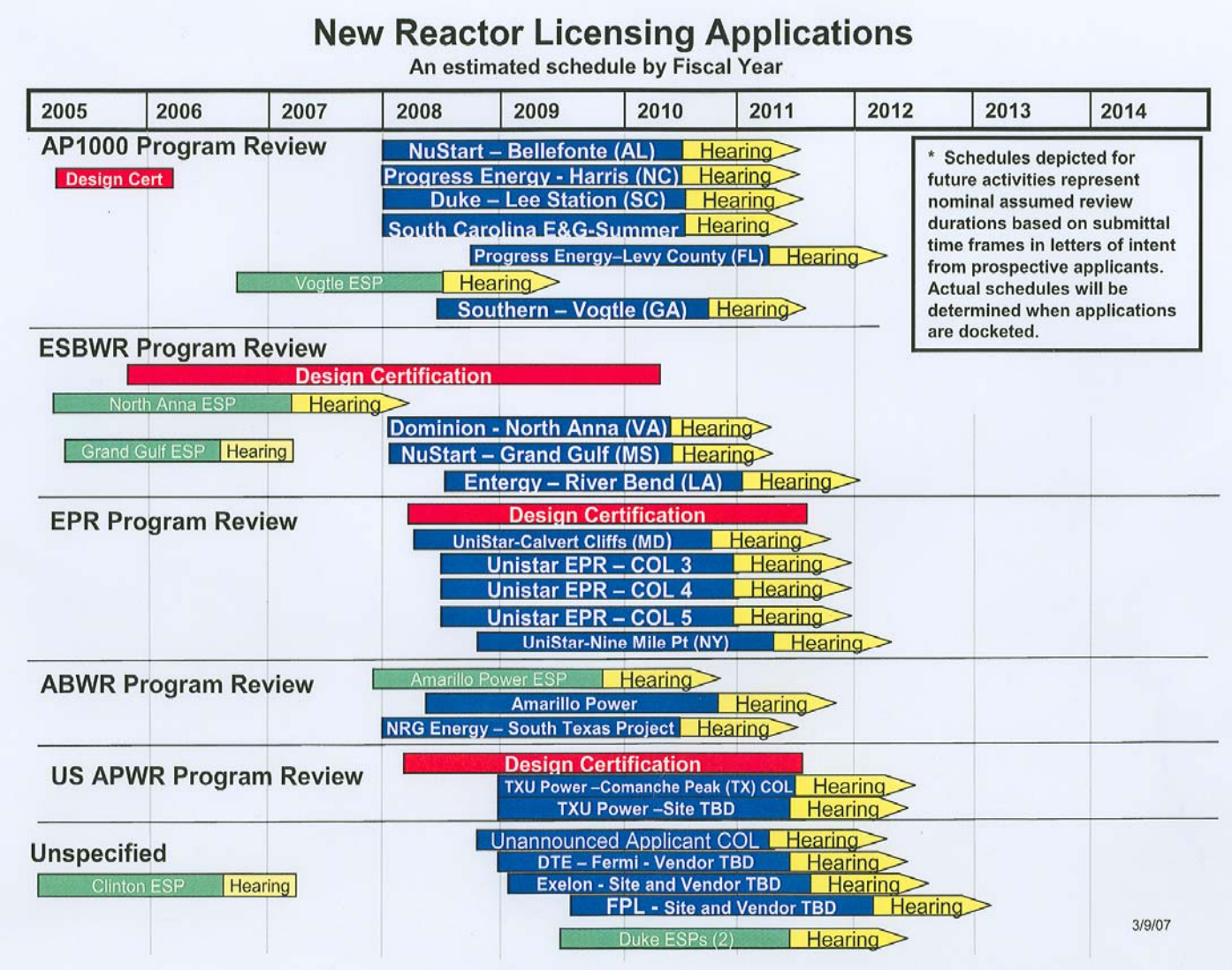


Figure 1-64 New Reactor Licensing Applications

AP-1000
Passive Containment Cooling

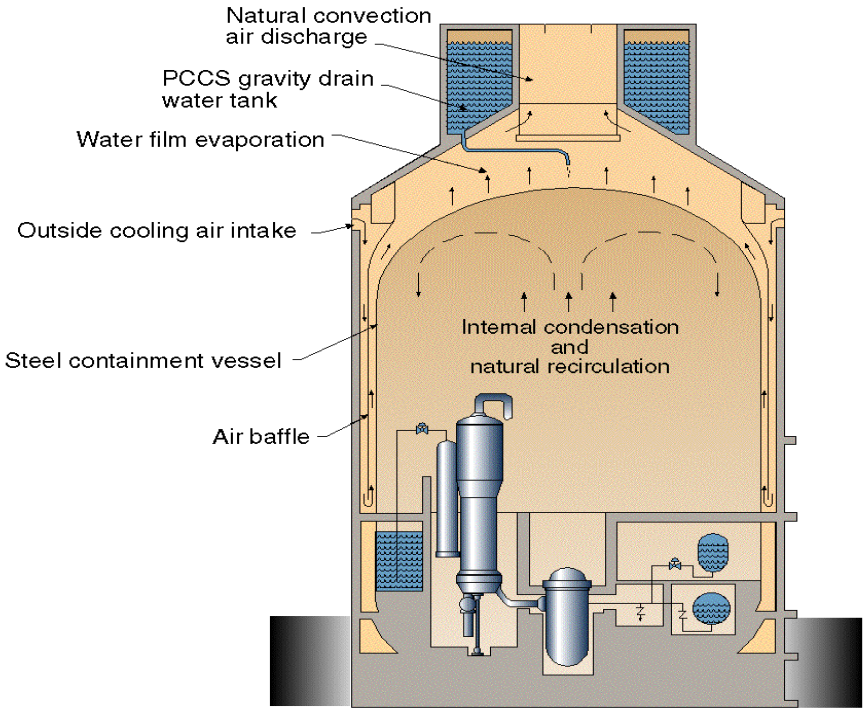


Figure 1-65 AP-1000 Passive Containment Cooling

Figure 1-66 Advanced Control Room Concepts

Figure 1-67 ESBWR Control Room Layout

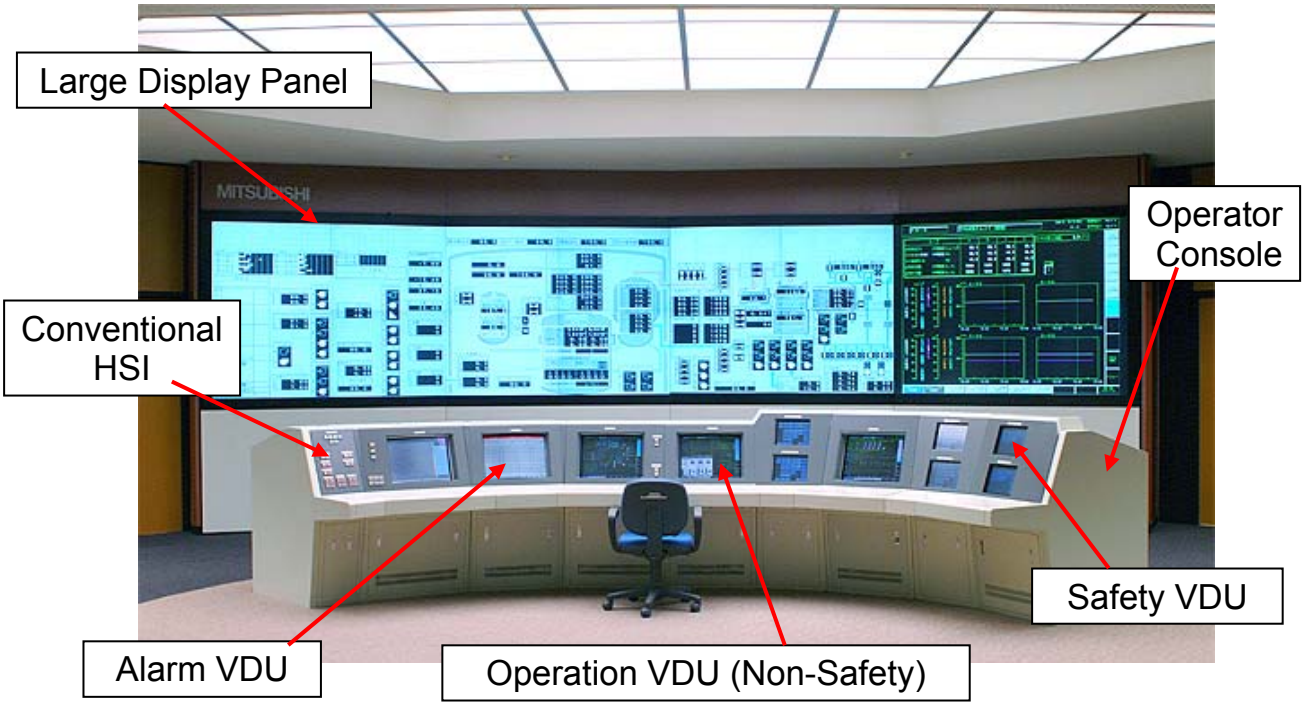


Figure 1-68 US APWR I&C System computerized Main Control Room

Figure 1-69 Slide 8

Reg. Guide 1.206 Section C.III.5 Design Acceptance Criteria

- Information necessary to verify completion of I&C design:
  - All I&C ITAACs
  - Describe implementation process for both hardware and software of I&C systems

Figure 1-70 Reg. Guide 1.206 Section C.III.5 Design Acceptance Criteria (1 of 4)

Reg. Guide 1.206 Section C.III.5 Design Acceptance Criteria

- Information necessary to verify completion of I&C design:
  - Typical software life-cycle process **planning**
    - Software management plan
    - Software development plan
    - Software test plan
    - Software QA plan
    - Integration plan
    - Installation plan
    - Maintenance plan
    - Training plan
    - Operations plan
    - Software safety plan
    - Software V&V plan

Figure 1-71 Reg. Guide 1.206 Section C.III.5 Design Acceptance Criteria (2 of 4)

Reg. Guide 1.206 Section C.III.5 Design Acceptance Criteria

- Information necessary to verify completion of I&C design:
  - Typical software life-cycle process implementation docs.
    - Safety analysis
    - V&V analysis and test reports
    - Configuration management reports
    - Requirements traceability matrix
  - Reference to DCD or certified design
  - Equipment qualification

Figure 1-72 Reg. Guide 1.206 Section C.III.5 Design Acceptance Criteria (3 of 4)

Reg. Guide 1.206 Section C.III.5 Design Acceptance Criteria

- Information necessary to verify completion of I&C design:
  - Information on the control of access
  - Repair provision
  - Identification provision, Reg. Guide 1.75
  - Human Factors considerations
  - Automatic control capability
  - Manual control capability
  - Interaction between sense and command
  - Derivation of system inputs
  - Setpoint determination

Figure 1-73 Reg. Guide 1.206 Section C.III.5 Design Acceptance Criteria (4 of 4)

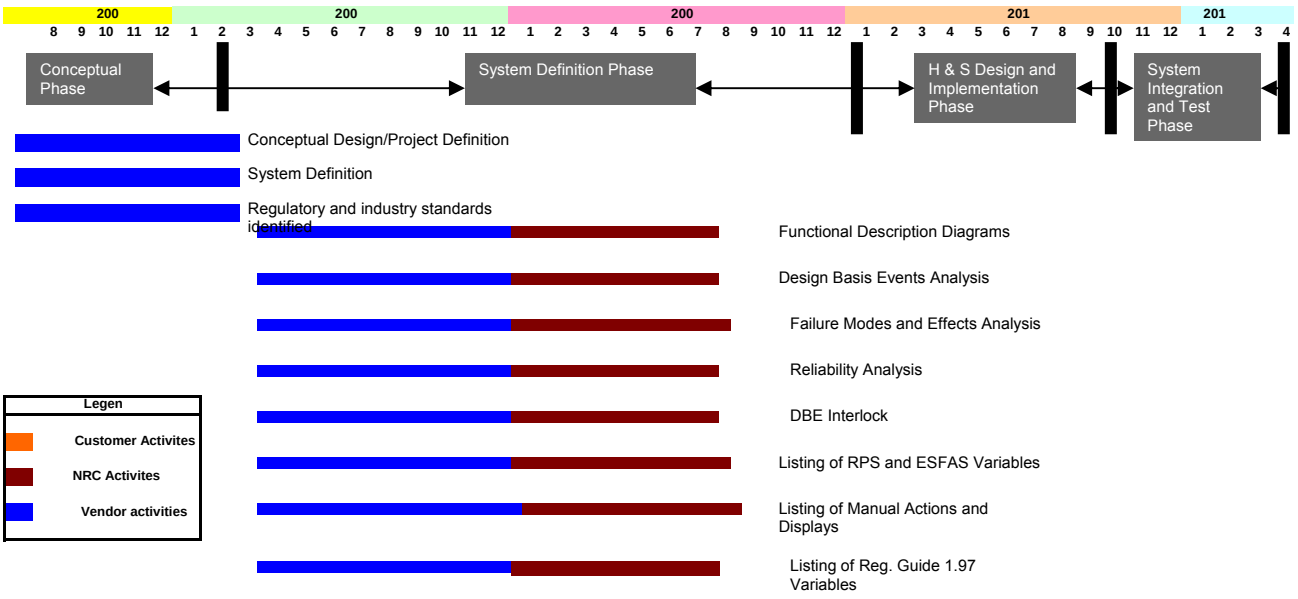


Figure 1-74 EXAMPLE - Proposed DAC and Status Report – I&C and HMI – Sheet 1

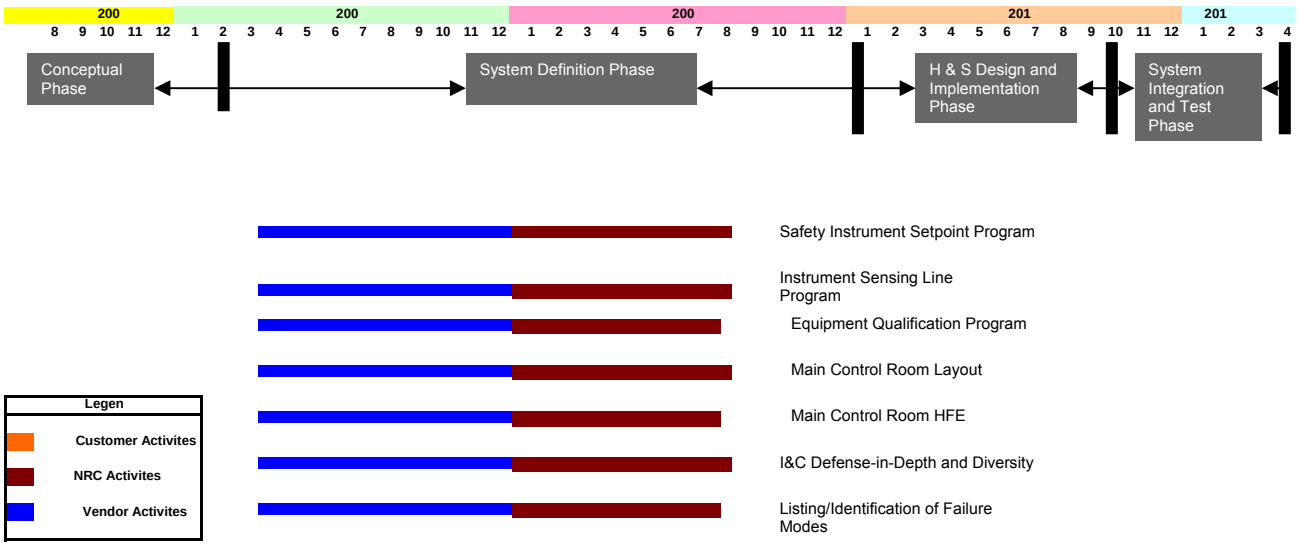


Figure 1-75 EXAMPLE - Proposed DAC and Status Report – I&C and HMI – Sheet 2

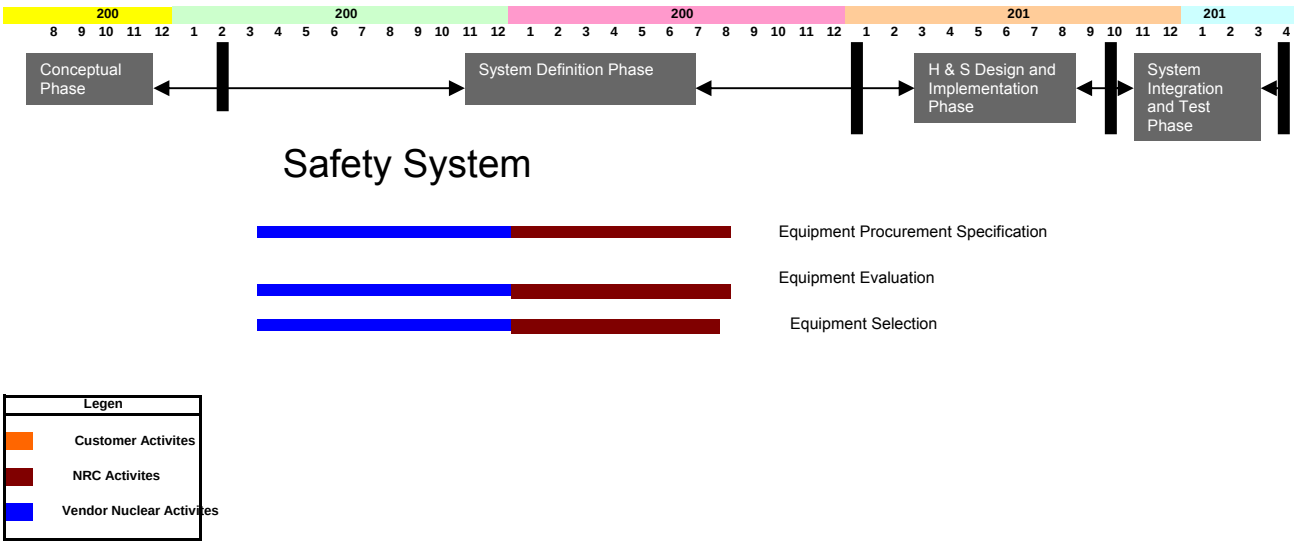


Figure 1-76 EXAMPLE - Proposed DAC and Status Report – I&C and HMI – Sheet 3

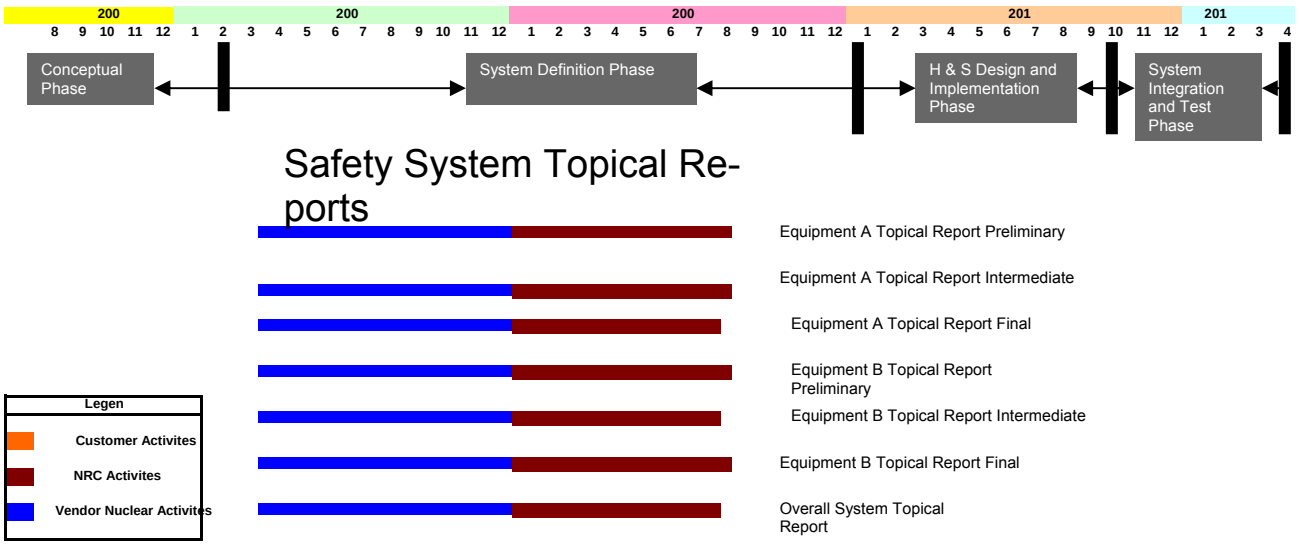


Figure 1-77 EXAMPLE - Proposed DAC and Status Report – I&C and HMI – Sheet 4

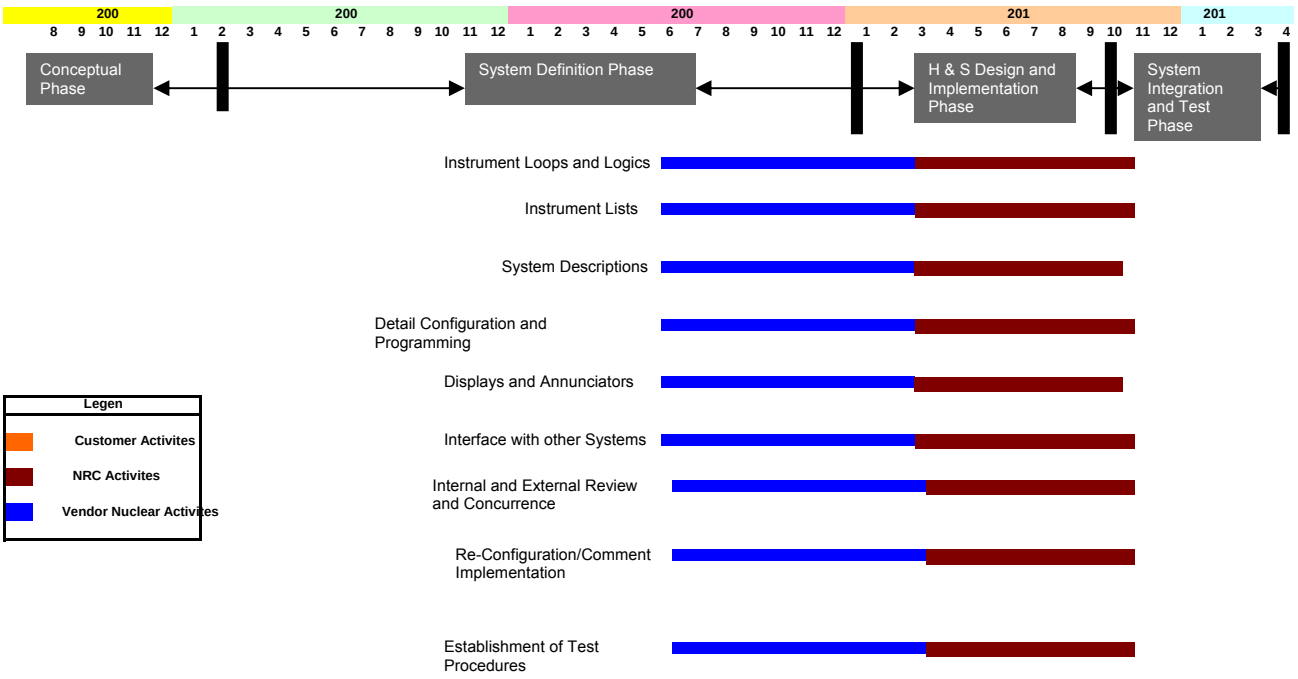


Figure 1-78 EXAMPLE - Proposed DAC and Status Report – I&C and HMI – Sheet 5

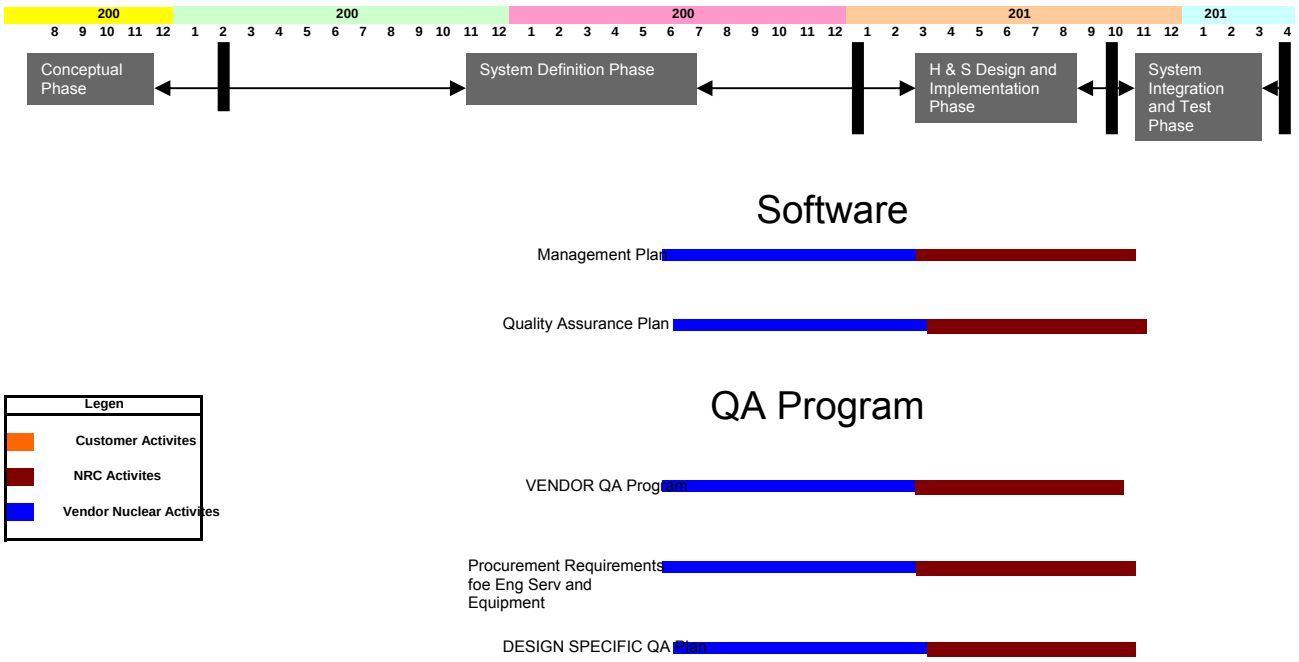


Figure 1-79 EXAMPLE - Proposed DAC and Status Report – I&C and HMI – Sheet 6

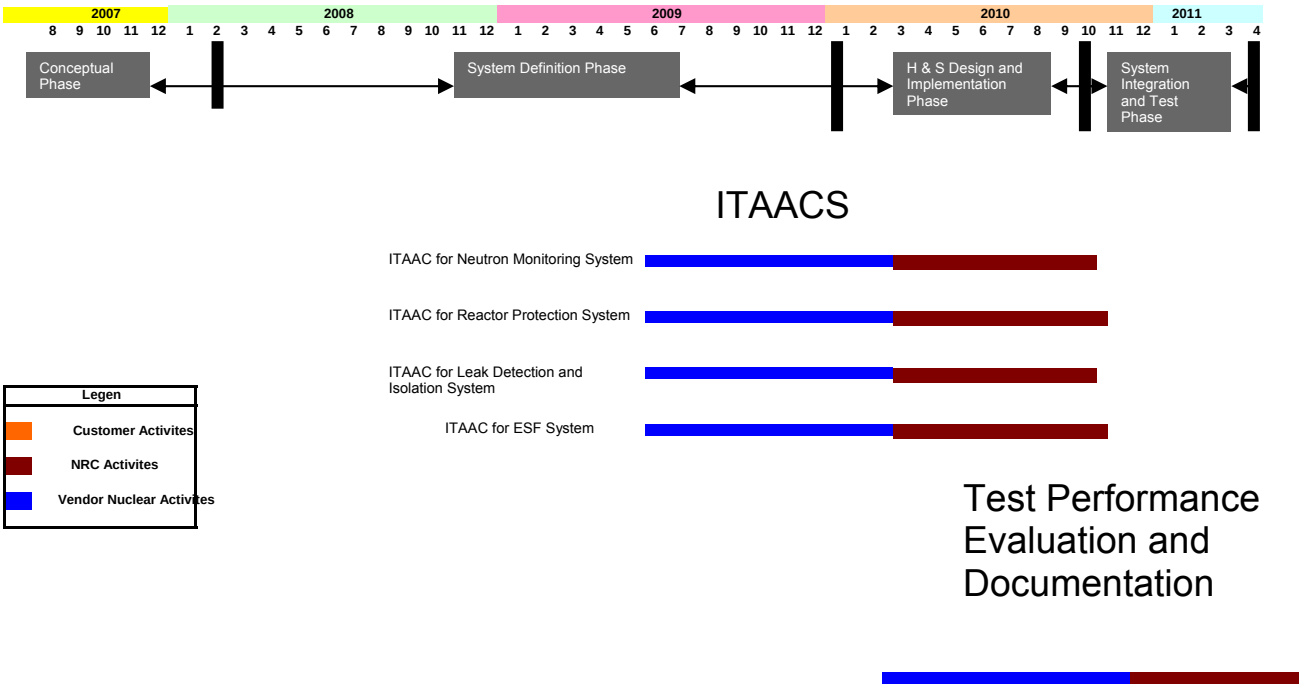


Figure 1-80 EXAMPLE - Proposed DAC and Status Report – I&C and HMI – Sheet 7

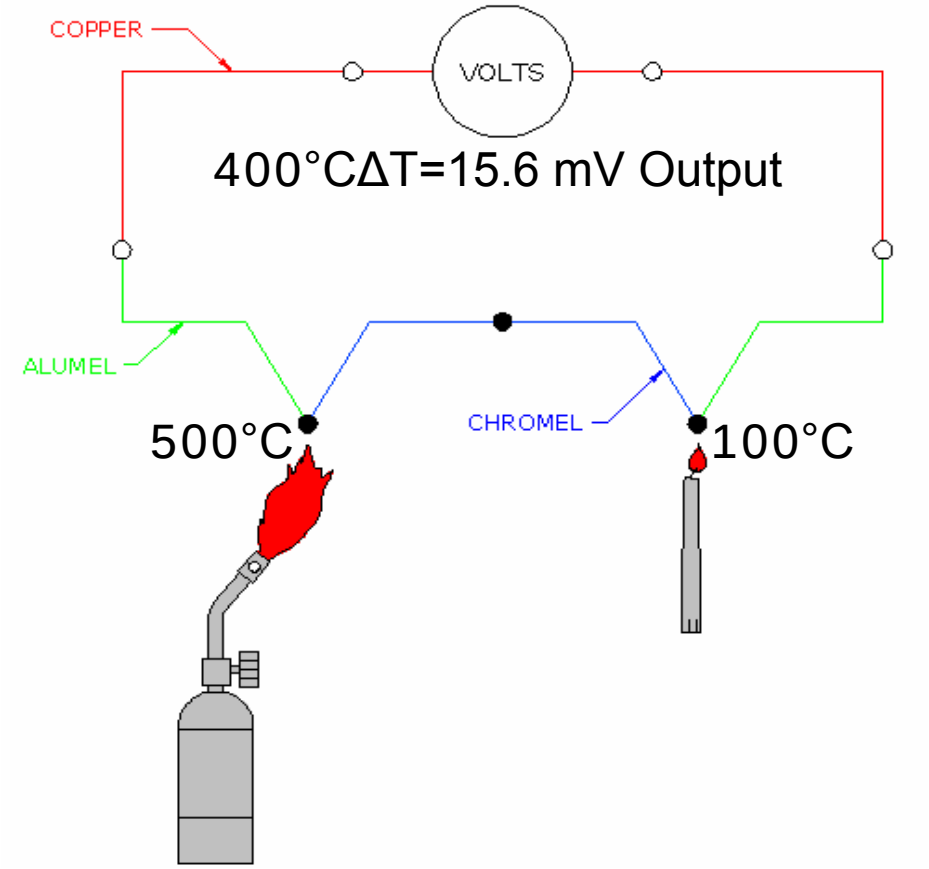
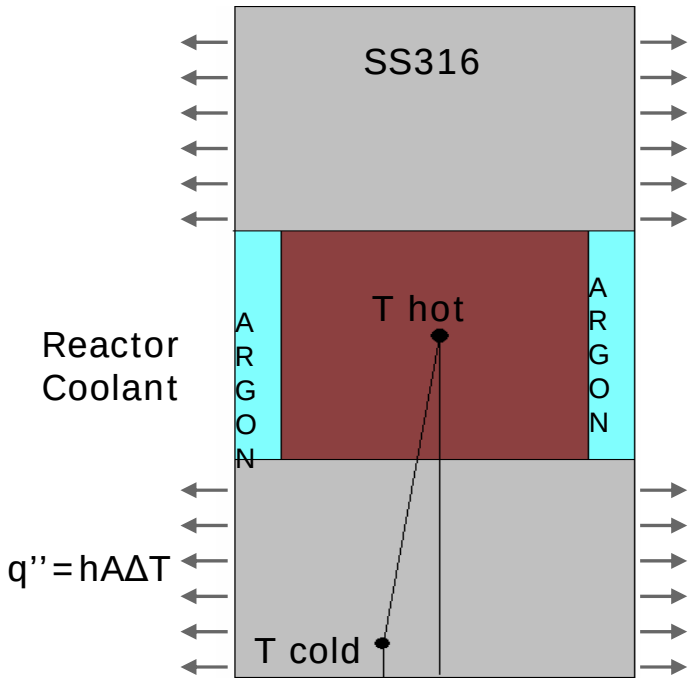


Figure 1-81 How a GT Works



- An argon heat dam provides a Δ T that is representative of the total power , Q, that is deposited under the heat dam. In a NPP, the power is generated from energy deposited by gammas and neutrons. The reactor coolant provides a heat sink for the system, creating a differential temperature across the TC junctions

Figure 1-82 How a GT Works

Source: Altera

Figure 1-83 Field Programmable Gate Array Illustration