U.S. Department of Energy
Office of River Protection
P.O. Box 450, MSIN H6-60
Richland, Washington 99352

JAN 14 2005

05-WED-001

Mr. J. P. Henschel, Director
Bechtel National, Inc.
2435 Stevens Center
Richland, Washington, 99352

Dear Mr. Henschel:

CONTRACT NO. DE-AC27-01RV14136 – TRANSMITTAL OF U.S. DEPARTMENT OF ENERGY, OFFICE OF RIVER PROTECTION DESIGN OVERSIGHT REPORT ON THE INTEGRATED CONTROL NETWORK (ICN) DESIGN STATUS (D-04-DESIGN-009), ASSESSMENT REPORT SUMMARY

This letter transmits for your information an Assessment Report Summary associated with the subject Oversight Report on the Waste Treatment and Immobilization Plant (WTP) ICN Design Status Review conducted in November and December 2004.

As the summary indicates, the assessment results determined that the ICN system (software and hardware) is being well engineered and designed, and is progressing according to schedule. A very strong plan has been structured and is being executed for software development, implementation, and testing. The control system design is consistent with the Basis of Design and implements key industry standards.

At this time there are no open items or new actions identified for the WTP Contractor.

A copy of the full report was provided to your staff, and you may request additional copies.

If you have any questions, please contact me, or your staff may call William F. Hamel, Jr., Director, WTP Engineering Division, (509) 373-1569.

Sincerely,

Roy J. Schepens
Manager

WED:WFH

Attachment

cc w/attach:
S. E. Anderson, BNI
S. Lynch, BNI

Attachment to
05-WED-001

Assessment Report Summary

ORP Design Oversight Report: Waste Treatment Plant Integrated Control Network (D-04-Design-009), November 2004

WED:WFH:
January 6, 2005

Attachment
05-WED-001

U.S. Department of Energy (DOE), Office of River Protection (ORP) Design Oversight Report: Waste Treatment Plant Integrated Control Network (D-04-Design-009) November 2004

Assessment Report Summary

During the months of November and December 2004 DOE ORP engineering staff conducted an assessment of the Waste Treatment and Immobilization Plant (WTP) project Integrated Control Network (ICN) design and development. The ICN provides the plant system controls for the WTP and the performing contractor for the ICN design is Bechtel National, Inc. (BNI).

The focus of the assessment was on the general overview of the ICN architecture, software development and status, and BNI's approach for software verification and validation. The assessment also considered responses to concerns and questions raised in a previous independent assessment conducted in July 2004.

Specific assessment objectives were:

1. Obtain a general status of the ICN system design and development to-date.
2. Gain a better understanding of BNI's software development process in order to evaluate progress and determine that software documentation will yield a quality software product.
3. Determine progress in Software Functional Specification (SFS) development.
4. Become familiar with BNI's approach for software verification, validation and testing.
5. Gain additional knowledge and insight into the ICN system architecture.
6. Determine that design is consistent with implementing standards and requirements.
7. Address and close issues from the independent review conducted in July 2004.

All of these objectives were accommodated by the BNI staff.

The assessment evaluated BNI software documentation, pertinent system descriptions and specifications, industry standards, design guides and other documentation, attended a formal presentation hosted by BNI Control and Instrumentation (C&I) and Commissioning and Testing (C&T) staff, and performed a field walk-through to verify that installed equipment is consistent with planning.

Specific key accomplishments in the BNI ICN work to-date include:

- The first controller enclosure equipment has been designed, fabricated, and delivered to the sight.
- Substantial headway has been made towards generating an estimated 750 life cycle documents including Software Functional Specifications, System Design Documents, Test Plans, etc.
- Software to implement control functions and requirements is well underway.
- BNI has satisfactorily addressed concerns raised from the independent review conducted in July 2004.

The assessment overall, affirmed that BNI is designing a plant control system that implements the latest industry developments in network communications and fieldbus technology and has put together a well structured plan for software development, and verification and validation testing, especially given the size and complexity of the ICN system. The control system design is consistent with the Basis of Design document and clearly implements key industry standards. BNI has developed detailed planning that is effectively being executed and the project appears on schedule. At this time there are no significant issues and no actions were identified from this review.

The *ORP Design Oversight Report, Waste Treatment Plant Integrated Control Network (D-04-Design-009)* resides on the ORP Records Management Information System (RMIS) and provides a detailed assessment report including an *Integrated Control Network Summary Description*, provided as Attachment 1 to the report. The ICN Summary Description is a condensed description of the ICN architecture and is based on information obtained through reviews of BNI documents and presentation materials.

ORP Design Oversight Report

Waste Treatment Plant
Integrated Control Network

D-04-DESIGN-009

November 2004

Concurrence: _____

William F. Hamel, Director
Engineering Division
Office of River Protection

Approved: _____

John R. Eschenberg, Project Manager
Waste Treatment and Immobilization Plant Project (WTP)
Office of River Protection

U.S. Department of Energy
Office of River Protection
Richland, Washington

Executive Summary

The Office of River Protection (ORP) engineering staff conducted an assessment of the Waste Treatment and Immobilization Plant (WTP) project Integrated Control Network (ICN) design and development. Bechtel National, Inc. (BNI) is performing the ICN design work. The focus of the assessment was on the general overview of the ICN architecture, software development and status, and BNI's approach for software verification and validation. The assessment also considered responses to concerns and questions raised in a previous independent assessment conducted in July 2004.

ORP engineering staff evaluated BNI software documentation, pertinent system descriptions and specifications, attended a formal presentation by BNI Control and Instrumentation (C&I) and Commissioning and Testing (C&T) staff, and performed a field walk-through to verify that installed equipment is consistent with planning.

Key products from this assessment are (1) this assessment report and (2) an *Integrated Control Network Summary Description*, provided in Attachment 1. The ICN Summary Description is based on information obtained through reviews of BNI documents and presentation materials.

Specific key accomplishments in the BNI ICN work to-date include:

- The first controller enclosure equipment has been designed, fabricated, and delivered to the sight.

- Substantial headway has been made towards generating an estimated 750 life cycle documents including software functional specifications, system design documents, test plans, etc.

- Software to implement control functions and requirements is well underway.

- BNI has closed 14 out of the 15 actions identified in the June 2003 Bi-Monthly Design Overview Meeting and has effectively addressed concerns raised from the independent review conducted in July 2004.

The assessment overall, affirmed that BNI is designing a plant control system that implements the latest industry developments in network communications and fieldbus technology and has put together a well structured plan for software development and testing, especially given the size and complexity of the ICN system. The control system design is consistent with the Basis of Design document and meets key industry standards. BNI has developed detailed planning that is effectively being executed and the project appears on schedule. At this time there are no significant issues and no actions were identified from this review.

Table of Contents

Introduction

This report documents the activities and conclusions connected with the design oversight assessment of the WTP Integrated Control Network (ICN). The assessment was conducted in November 2004 with document reviews extending into December. This assessment was scheduled by the Office of River Protection (ORP) WTP Engineering Division and was conducted in accordance with procedure, ORP PD 220.1-12, *Conduct of Design Oversight.*

The purpose and scope of the ICN design assessment (herein referred to as the "Nov-04 review") was primarily to obtain status on ICN software development and the software verification and validation approach BNI plans to implement. In addition, the review was intended to obtain greater understanding and awareness of the ICN system architecture design. The scope of the review focused mainly on progress made in the documentation associated with software development, software testing, and specific features of plant system architecture.

Methods employed in the review in order to gather information and arrive at conclusions included:

- Receiving a formal presentation by BNI Control and Instrumentation (C&I) and Commissioning and Testing (C&T) personnel with discussion.
- Performing various document reviews
- Performing a field walkthrough of some of the installed WTP equipment.

Background

In November 2001, BNI awarded the contract for development of the ICN to ABB (ASEA Brown Bovari). Through this contract BNI purchases the software and hardware system required to develop the *control software* for the WTP. ABB develops the *system software* and hardware which includes controller enclosures (including the devices that communicate with field equipment), network servers, etc. System software provides the environment by which the ICN control software can be developed and installed by BNI. System software is comprised of the ABB control system platform, various graphic symbols, Microsoft Windows operating system, system security software and network management software. The ABB system provides an integrated suite of software packages and development tools that allow BNI engineering to development and implement an operational control system for the WTP. The ABB system software also provides the interface between field equipment and plant control/operations functions defined by the control software.

In the June 2003, Bi-Monthly Design Overview, BNI presented their approach and process for developing *Control System Software Functional Specifications.* A brief report of that overview is provided in Attachment 2 and includes the BNI generated meeting minutes. At that time, there were no significant issues of concern for ORP. However, it was recommended that Software Functional Specification (SFS) development should be monitored closely since it comprised a tremendous amount of work required for the ICN design. Hence, one objective for the Nov-04 review was to assess SFS developments. The Jun-03 review meeting minutes recorded 15 actions primarily of a technical nature that needed to be addressed and closed. According to the Nov-04

presentation, all but one of these actions has been closed. Closure for the remaining action is ongoing and as is obvious from the description below, is expected to continue for sometime.

> No.4 – "C&I design personnel responsible for the WTP control system network security should be involved with ongoing development of industry standards to stay knowledgeable and current with security technology."

The June-2003 overview did not address in detail any of the elements listed below. The review primarily focused on the approach and documentation required for software development, particularly by way of Software Functional Specifications. Follow-on reviews will address in detail the listed items.

- Communication Systems Networks
- Software Implementation
- Software Life Cycle
- Safety System Requirements
- Human Machine Interfaces
- Control Rooms
- Area Software Functional Specifications
- Training Simulator
- Physical plant
- Acceptance Testing, Installation, and Commissioning

The Nov-04 review touched on several of the items listed above including, software implementation, software life cycle, human machine interfaces (software needs), and area software functional specifications.

The ICN system that was introduced in June 2003 had the following features:

- It was composed of three interconnected systems, Pretreatment facility (includes Balance of Facilities and the Lab), High Level Waste (HLW) facility, and the Low-Activity Waste (LAW) facility.
- Approximately 140 process controllers were planned for. (The number does not include the count for redundancy.)
- The system had approximately 30,000 inputs/outputs (I/O).
- The plant had approximately 170 plant sub-systems.

The controllers and I/O for the sub-systems in the three plant facilities as well as facility interconnection would require extensive software for process control and communications. This software would be generated primarily through development of an ICN Software Requirements Specifications (SRS), many Software Functional Specifications (SFS), many System Design Documents (SDD), several Test Plans and Test Reports.

In February 2004, BNI issued the *Software Project Plan for the Integrated Control Network.* The plan defines the primary work processes that will be implemented to provide the WTP with the appropriate software used to control and operate the plant. It identifies the mechanisms used

to produce the primary deliverables that will be developed throughout the software life cycle. Specifically the plan defines the process of acquisition, development, implementation, and testing of the control system software that comprises the ICN. The Nov-04 review evaluated BNI against the main features and deliverables identified in the Software Project Plan.

In July 2004, ORP obtained consultant service through British Nuclear Fuel Limited to provide an independent evaluation of the BNI ICN work. The report of that evaluation, *WTP Distributed Control System Review* (by Grenville Harrop) is provided in Attachment 2. That report though favorable, made recommendations and identified several general concerns. Several of those concerns were addressed by BNI in the Nov-04 assessment and will be discussed shortly.

Objectives

The objectives connected with the Nov-04 review included the following:

1. Obtain a general status of the ICN system design and development to-date.

2. Gain a better understanding of BNI's software development process in order to evaluate progress and determine that software documentation will yield a quality software product.

3. Determine progress in SFS development.

4. Become familiar with BNI's approach for software verification, validation and testing.

5. Gain additional knowledge and insight into the ICN system architecture.

6. Determine that design is consistent with implementing standards and requirements.

7. Address and close issues from the independent review conducted in July 2004.

One last objective for the review was to evaluate the documentation describing the ICN architecture in order to provide a consolidated summary description document for the purpose explained as follows.

The ICN is a complex system composed of several elements required to provide the process controls for the WTP. Documentation describing the ICN includes system descriptions, software plans, specifications, design guides, etc. This volume of documentation and the high technical content may not in most cases lend to an easily obtainable understanding of such an important portion of the WTP project, particularly for ORP personnel unfamiliar with plant control system technology. Hence, another objective in the Nov-04 review was to provide a condensed summary description of the ICN architecture. The summary description was assembled as an outcome of several document reviews conducted in the assessment. It is believed, that such a description will also provide a context in which related software developments described herein may be better understood. Attachment 1 provides a brief description of the ICN architecture, which may be considered a product of the Nov-04 assessment report.

Scope

The scope of the review was mainly on software development progress to-date, software test planning, document reviews for a deeper understanding of the ICN architecture, and closure of issues and concerns identified in the July-04 independent assessment.

Additional scope is reflected in the lines of inquiry stated below.

- Provide an example of code that has been written that shows how an operator or batch process can communicate via an ICN controller, with a field device/actuator/motor.

- Describe the layout/locations of controllers and the general approach to field wiring. What key facility-specific drawings are available such as instrument location drawings?

- Using a simple system, provide a system walk-through showing how the software products (SFSs, SDDs, Test Plans, etc.) result in software implementation.

- What technical problems or issues are being encountered in the software development?

Approach

The approach for this assessment involved the following:

- Formal presentation by BNI
- Document reviews
- Field walk-through.

These elements are explained further.

Presentation

Planning for the BNI presentation, *ICN Design Status Review* began in late October 2004 with an initial proposed agenda provided to BNI. This is provided as shown.

Proposed Agenda for an October/November 2004 ICN Review:

- *General status of design and engineering. (scope, cost, and schedule)*
- *Near-term objectives, key deliverables, etc.*
- *Current problems, issues, or concerns*
- *Process for software V&V and testing*
- *Responses to G. Harrop's concerns and observations*

Format for the Review:

The review is expected to be an informal discussion with appropriate handouts, drawings, listings, to include a general walkthrough of a Software Functional Specification and a System Design Document. No more than a morning or afternoon needs to be dedicated to this effort.

BNI answered this proposal with the following agenda.

BNI Agenda in Response to ORP

* *ICN Overview - Brief description of the make-up of the ICN. Standard terms and definitions (10 mins)*

* *Review of 2003 Design Review Presentation and Action Items (10 mins)*

* *ICN Project Timeline (10 minutes)*
* *ABB Contract Deliverables*
* *Internal Project Deliverables*

* *ICN Software Project Plan - Overview of the planned software development process and phased deliverables (20 mins)*

* *Software Development Status (SFSs, SDDs, and Test Plans) (10 mins)*

* *Approach to Verification and Validation (60 mins)*
* *Test Plans*
* *Acceptance Criteria*
* *Sub Projects/FATs, component and system testing*

* *ORP DCS Review report (60 mins)*
* *Standardization - Controls in place to ensure standardization across facilities*
* *Process Design Uncertainties - Prioritization to ensure development work is appropriately channeled.*
* *Systemization - Approach to systemization in the ICN design.*
* *Prototyping - The use of prototyping through ICN development to prove aspects of the design and implementation*

* *Wrap-up (10 mins)*

The meeting took place on November 9, 2004 according to the final agenda below. The meeting included a presentation packet of useful materials for discussion and allowed for an informal question and answer exchange between OPR engineering oversight personnel and BNI C&I and C&T engineers.

Introduction 8:00 AM – 8:15 AM
- Safety Topic
- Objective and Purpose
- Review of 2003 Design Review Actions Items

ICN Overview 8:15AM – 8:30 AM
- Overview of ICN
- ICN Project Timeline

ICN Software Development and Status 8:30 AM – 9:30 AM
- Software Project Plan
- System Walkthrough and Status
- Technical Problems and Issues

Break 9:30 AM – 9:45 AM

Approach to Verification and Validation 9:45 AM – 10:45 AM
- Project Strategy for Software V&V
- Out-Plant ICN Software and Hardware Testing
- In-Plant ICN Software and Hardware Testing

ORP DCS Review Report 10:45 AM – 11:45 AM
- Standardization
- Process Design Uncertainties
- Systemization
- Prototyping
- Simulator Utilization
- Operations Research Flowsheet and Modeling Approach

Wrap up 11:45 AM – 12:00 PM

Document Reviews

The following documents were reviewed (some in much greater detail than others):

- ***Planning Documents:***

24590-WTP-DB-ENG-01-001, Rev 1B, *Basis of Design,* Sections 7 and 9

24590-WTP-J-01-003, Rev 0, *Software Project Plan for the Integrated Control Network*

- ***Specifications:***

24590-WTP-3PS-JD01-T0001, Rev 2, *Engineering Specification for Plant Wide Controls Systems (Integrated Control Network)*

24590-WTP-3PS-JD01-T0410, Rev A, *Engineering Specification for System Design Document for the Integrated Control Network*

24590-WTP-3PS-JD01-T0010, Rev A, *Software Requirements Specification for the ICN-System*

24590-WTP-3PS-JD01-T0002, Rev 0, *Control Library Specification for Integrated Control Network (ICN)*

24590-WTP-3PS-EFD0-T0001, Rev A, *Engineering Specification for Facility Network Infrastructure*

24590-HLW-3PS-DIW-T0001, Rev 0, *Software Functional Specification for HLW Demineralized Water (DIW) System*

- ***Design Guides:***

Industrial^{IT} Integrated Automation Solutions for Process Automation based on Aspect Object Technology, System Guide (System Baseline , May 2002) by ABB (Asea Brown Bovari)

24590-WTP-GPG-J-004, Rev 0, *Guidelines for Design of a FOUNDATION Fieldbus H1 Segment*

24590-WTP-GPG-J-001, Rev 0, *Design Guide: Preparation of Control System Software Functional Specifications*

24590-WTP-GPG-J-014, Rev B, *Design Guide: Control Systems Design Process Guide*

- ***System Descriptions:***

24590-WTP-3YD-PCJ-00001, Rev 0, *System Description for Process Control System (PCJ)*

24590-WTP-3YD-ASJ-00001, Rev A, *System Description for Autosampling Control System*

24590-WTP-3YD-MHJ-00001, Rev 0, *System Description for Mechanical Handling Control System (MHJ)*

24590-WTP-3YD-FNJ-00001, Rev 0, *System Description for Facility Network Infrastructure*

- ***Standards:***

ANSI/ISA-S88.01-1995, *Batch Control Part1: Models and Terminology*

ANSI/ISA-S50-02-1992, *Fieldbus Standard for Use in Industrial Control Systems Part 2: Physical Layer Specification and Service Definition*

IEC 61131-3, *Programmable Controllers Part 3: Programming Languages*
ANSI/ISA-S5.5-1985, *Graphic Symbols for Process Displays*

ANSI/ISA-S5.1, *Instrumentation Symbols and Identification*

ANSI/ISA-S5.3, *Graphic Symbols for Distributed Control/Shared Display Logic Instrumentation and Computer Systems*

- ***WTP Control System Architecture Diagrams:***

24590-PTF-JJ-PCJ-00001001
24590-PTF-JJ-PCJ-00001002
24590-HLW-JJ-PCJ-00001
24590-LAW-JJ-PCJ-00001
24590-BOF-JJ-PCJ-00001

24590-BOF-J1-FNJ-00001

- ***Presentation Materials and Reports:***

Bi-Monthly Design Overview, June 26, 2003, *Control System Software Functional Specifications*

Design Overview Assessment, November 9, 2004, *ICN Design Status Review*

WTP Distributed Control System Review, by Grenville Harrop

- ***Other Documents:***

24590-WTP- 3PS-JD01-T0003, *Control Library Terms, Definitions, and Symbols & Legends for the Integrated Control Network*

Field Walk-through

On November 24, 2004 a Field walk-through was conducted in order to observe and verify placement of specific ABB controller and I/O cabinets.

Oversight Assessment Results

The results of this oversight assessment are organized according to the objectives listed previously.

1. Obtain a general status of the ICN system design and development to-date.

The ICN is comprised of control software, system software and hardware that together provide the means for control and operation of the complete plant system which includes physical components such as piping and process equipment, instrumentation, and human administrative components. The ICN hardware (servers, human-machine interfaces [HMI], controllers, etc.) is defined by the system architecture discussed in Attachment 1, *Integrated Control Network Summary Description.* Plant system control software is the ICN software that is either developed or configured to enable the automation of the ICN.

BNI develops the application/control software utilizing the system software provided by ABB. The application software integrates various control elements (control strategies, software function blocks, device drivers, etc.) to create equipment/control modules and from these modules create functional control units. These developments further allow for integration of control units and equipment/control modules to form plant system control and functionality among a host of plant sub-systems as well as intra-facility control functionality.*

> * The terminology use in this paragraph is based on specific definitions provided in ANSI/ISA-S88.01-1995, *Batch Control Part 1: Models and Terminology*, regarding the concept of the physical model. See Appendix A for a brief explanation of the physical model.

BNI develops the application software in parallel with ABB system development (system software and hardware). Both trains of activity converge at functional acceptance testing of plant facility systems. This is shown in Figure 1 as well as the major activities required prior to the facility systems being shipped to the field for installation.

A timeline of system activity is provided in Figure 2 and represents a general schedule for ICN system development and progress to-date according to the major facilities. Most of the work up till now has been in system design with some fabrication being completed with BOF controllers. A field walk-through was recently made and it was observed that ABB controller and I/O cabinets were placed in the following locations.

Building 87 Main Switchgear Building
Building 91 BOF Switchgear Building
Cooling Tower Electrical Room
NLD Pump House

Major progress has also been made in the area of software development.

The BNI approach for software development involves several life-cycle phases including planning, defining requirements, software design, software implementation, and testing. (The process for software development is explained later.) Each of these phases has defined products and deliverables as shown in Figure 3.

Status of these deliverables is explained as follows.

- Out of the planning phase, the ICN Software Project Plan (Rev 0) was issued in February 2004. This plan identifies and defines the work effort and products for developing the software components of the ICN. It is the only document to be produced from the planning phase.

Out of the requirements phase various documents are produced including the ICN Software Requirements Specification (SRS), Area Software Functional Specifications (ASFS), Software Functional Specifications (SFS), and the Control Library.

- The ICN-SRS (Rev 0) was issued in October 2004. This specification contains the requirements for the ICN software and provides requirements traceability, but does not include plant system functional requirements.

- Work has begun on the five ASFSs but none have yet been released and are currently on hold pending the resolution of a Basis of Design change regarding changing the automation control philosophy of the WTP. The ASFS includes the functional requirements and conceptual and preliminary design for recipe control between plant systems within a facility or between separate facilities.

- There are 139 SFSs that will be produced for the WTP. Out of this number, 1 SFS has been issued Rev 0 and 73 have been issued Rev A. Each SFS is specific to at least one plant system and includes the functional requirements and conceptual and preliminary design for basic and procedural control.

- There are 2 documents associated with the control library, (1) Control Library Specification for the ICN and (2) Control Library Terms, Definitions, and Symbols & Legends for the ICN. Both documents were recently issued (Rev 0).

Out of the design phase several documents will be produced. These include, System Design Documents (SDDs) specific to each ASFS and SFS, and software Routines that populate the control library.

- Five SDDs associated with the five ASFSs have not yet been started for the same reason the ASFSs have not yet been started.

- Out of 139 SDDs (one for each SFS) 42 have been issued Rev A.

- Out of approximately 150 routines, 10 have been issued Rev 0.

From the software implementation phase the following status is reported according to software projects (explained in the next section). The percentages represent an approximately amount of software that has been implemented.

- ICN system project – 10%

- Facility projects (5) – 16%

- Control Library – 15%

From the testing phase, Test Plans (TPs) and Test Reports (TRs) will be generated. Testing includes Development Testing and Functional Acceptance Tests (FATs). Status is as follows.

- ICN system project:
  1 TP and 1 TR for Development Testing, planned but not yet started
  1 TP and 3 TRs for FATs planned but not yet started.

- Facility projects (5):
  5 TPs and 144 TRs for Development Testing, planned but not started

- Control Library project:
  1 TP issued Rev 0 for Development Testing
  10 TRs out of approximately 150 TRs for Development Testing have been issued Rev 0

The status above indicates adequate progress is being made in the production of software development documentation. In the BNI presentation there was no mention (even when asked) of schedule lags or problems connected with this work. However, Level 4 Schedule information remains to be evaluated, particularly in regard to SFS progress.

2. Gain a better understanding of BNI's overall software development process in order to track progress and determine that software documentation will yield a quality software product.

There are four types or categories of software that must be developed for the WTP control system. These are:

- *Application software* for integration of control elements, integration of plant control units, integration of plant systems (intra-facility), and integration of facilities (inter-facility).

- *Common control element software* for standardized software functionality building blocks, common control strategies and routines, equipment/device drivers, etc. and also HMI faceplates for most control elements.

- *System-wide software* for alarms, trends, security, batch functions, ICN interfaces, etc.

- *Computer system environment software* for graphics symbols and objects, system security software and network management, and interface to field equipment.

For purposes of developing the software listed above, BNI has organized the plant system software scope into seven project areas. These are:

- PTF Project (this project includes the LAB and BOF)
- HLW Project
- LAW Project
- PTF/HLW Inter-facility Project
- PTF/LAW Inter-facility Project
- ICN system Project
- Control Library Project

These software projects encompass the software necessary for *intra*-facility systems and processes as well as for *inter*-facility processes. The details and scope associated with each of these projects is provided in the *Project Software Plan*.

Table 1 below shows the relationship between the software type, the projects in which the software will be developed, and the contractor responsibility.

Table 1

Software Type	**Software Project**	**Scope Responsibility**
Application Software	PTF Project HLW Project LAW Project PTF/HLW Inter-facility Project PTF/LAW Inter-facility Project	BNI
Common Control Element Software	Control Library Project	BNI
System-wide Software	ICN system Project	BNI
Computer System Environment Software	Software and Hardware platform upon which the BNI software is built	ABB

The software types interface with each other functionally, and comprise a layered software architecture. This is shown in Figure 4. The computer system environment layer depicted in Figure 4 includes both the system software and hardware developed by ABB. Each of these layers is described in detail in the *Project Software Plan.*

The phases in the software life cycle include:

- Planning
- Requirements definition
- Design
- Software implementation (programming)
- Testing

These phases are requirements driven and result in specific products. Software life cycle methodology requirements are specified in 24590-WTP-QAM-QA-01-001, *Quality Assurance Manual.* The software life cycle requirements are implemented in 24590-WTP-GPP-IT-008, *Software Life Cycle Management,* which is the procedure driving the development of 24590-WTP-PL-J-01-03, *Software Project Plant for the Integrated Control Network.* The *Software Project Plan* defines the work and products necessary to meet the requirements of IT-008 and is the product of the planning phase.

Documents produced in the development phases are listed in Table 2 below according to the software project.

Table 2

	Software Project	Requiremts	Design	Implementn	Testing
1	PTF/HLW Inter-Facility	ASFS	SDD		TP1 and TR
2	PTF/LAW Inter-Facility	ASFS	SDD		TP1 and TR
3	PTF Intra-Facility PTF Facility Sub-projects	ASFS SFSs	SDD SDDs	PTF SS	TP2 and TR TP3s and TRs
4	LAW Intra-Facility LAW Facility Sub-projects	ASFS SFSs	SDD SDDs	LAW SS	TP2 and TR TP4s and TRs
5	HLW Intra-Facility HLW Facility Sub-projects	ASFS SFSs	SDD SDDs	HLW SS	TP2 and TR TP5s and TRs
6	ICN System	SRS*	SDD		T6 and TR
7	Control Library	Routines ⟶		Lib. SS	TP7 and TR

*ICN-Software Requirements Specification (SRS) is a single document providing requirements input to the Control Library, SFSs and to SDDs. Requirements are obtained or derived from documents such as PSAR, SRD, ORD, BOD, design guides, etc.

Area Software Functional Specification (ASFS) – provides the functional requirements and conceptual and preliminary design for recipe control between plant systems within a facility and between separate facilities.

Note: Recipe control is essentially the control necessary to produce a batch. A recipe contains "the necessary set of information that uniquely defines the production requirements for a specific product" (S88.01). A batch is "the material that is produced or that has been produced by a single execution of a batch process" (S88.01).

Software Functional Specification (SFS) – provides the functional requirements and conceptual and preliminary design for basic and procedural control for a specific plant system within a facility. Each plant system will be described in an SFS and some SFSs may contain more that one plant system.

Note: See Appendix A for definitions of basic control and procedural control.

Software Requirements Specification (SRS) – contains the software requirements for the ICN software and the Requirements Traceability Matrix for non-functional requirements.

System Design Document (SDD) – contains the detail design for software, and also contains the Requirements Traceability Matrix for plant system functional requirements. SDDs receive requirements from the ICN SRS, from ASFSs, and from SFSs.

Routines – documents the ICN Control Library typical routines.

Test Plan – includes plans to test the software in order to verify and validate software implementation.

Test Report – contains the documentation of the test system setup, specific test cases, specific test procedures and results of specific software life cycle tests.

System Software – is the implemented facility software using the COTS software supplied by ABB.

Requirements documentation provides input for design documentation, which feeds software implementation (programming). Testing documents provides verification and validation that software functions according to requirements.

How this process specifically applies to a plant system was verified by a system walk-through presented by BNI. The walk-through showed the process from system requirements definition through design and implementation and ultimately to control system hardware and plant equipment functionality. This walk-through presented code examples that showed how the ICN interfaces and communicates with the field equipment. The walk-through directly addressed lines of inquiry stated under the Scope section of this report.

The system walk-through verified that the BNI software development process is very well planned and executed, especially given the tremendous complexity of the WTP system. Moreover, the documentation is essential and appears to result in functional software that meets requirements.

3. Gain familiarity regarding the development and content of SFSs and SDDs in order to determine how software requirements are obtained and accommodated.

Development of Software Functional Specifications and System Design Documents are key documents in the software process.

- Plant system software cannot be implemented without both SFSs and SDDs.
- For each SDD there is an SFS and before the SDD is developed the SFS must be produced.
- The SFS and SDD are the main links between physical plant system design and software design.
- At least 139 SFSs and 139 SDDs will be developed for the WTP.

SFS/SDD development therefore, comprises a significant work scope for the ICN design.

The SFS

The purpose of the SFS is to translate project requirements into software functions and consolidate diverse information into one cohesive system-based design deliverable. Since documents upstream of the SFS rarely identify requirements as software requirements, design teams are formed to identify which requirements are best met utilizing software.

In collaboration with plant systems engineers and other stakeholders, C&I engineers gather requirements affecting plant system software. The objective in this effort is to gain concurrence on software requirements and design and communicate this information to the Plant Wide System group via the SFS. The SFS receives a broad-based review to ensure that the needs and requirements of all stakeholders are met. The SFS also provides the initial basis upon which successful testing and systems turnover can be planned for. The requirements defined in the SFS are conveyed through a common set of controller programming languages in accordance with industry standards.

The SFS has five key sections as discussed below.

- Section 1.0 – *Control Summary*: provides a brief overview of the system's processes from a control's point of view. This section also provides an equipment list and an interfacing system list.

- Section 2.0 – *Design Inputs*: provides the listing of system design inputs and references the source or justification for ranges and setpoints.

- Section 3.0 – *Physical Model*: The physical model is defined in ANSI/ISA S88.01-1995, *Batch Control Part 1: Models and Terminology* and is especially applicable to specifying a batch control system. See Appendix A. The physical model defined by S88.01 is used extensively in the design of the WTP software. The physical model describes the physical assets (e.g., melters, pumps, piping headers, etc.) of a plant in terms of equipment entities. The entities are organized in a hierarchical fashion and a rigorous association exists in the SFS between entities and the entities' design components.

- Section 4.0 – *Procedural Element Definition*: Procedural control is a set of steps that define a portion of an overall processing task (i.e., Sample, Transfer, Melt, Evaporate, etc.). Procedures run on equipment entities and those procedures written for a specific entity can only manipulate devices defined in that entity. The procedure is defined, by name, and associated with an entity. Appendix D of the SFS provides the detail design of the procedural element.

- Section 5.0 – *Physical Model Definition*: Equipment entities defined in section 3.0 are detailed in this section. The definition includes defining which elements are part of each entity and referenced to the basic control elements and equipment state diagrams. Elements are defined as individual valves, pumps, transmitters etc. An element can only be part of one entity. Appendix E and F of the SFS provides the detail design of the basic control.

The SDD

The purpose of the SDD is to translate the functional design stated in the SFS into software design that can be implemented on the system hardware. The SDD bridges the gap between design and implementation by integrating the target system software structure with the functional design. The SDD records the results of the software design process and shows how the software product will be structured to satisfy the design identified in the SFS.

The SDD contains:

- Human Machine Interface Design (Section 3.1)
  - System overview graphic
  - Process graphics
  - Operation specific displays
  - Faceplates
- Requirement Traceability Matrix (Appendix A)
  - Identifies Test Acceptance Criteria from System descriptions
- Software Structure (Appendix B)
  - Each equipment entity, procedure, and element are defined in terms of the target software
- IO definition (Appendix C and D)
- Configuration Parameters (Appendix G)

Evaluation of the *HLW Demineralized Water (DIW) System* SFS and SDD verified the effectiveness of the BNI process for gathering software functional requirements and translating those requirements into design.

4. Become familiar with BNI's approach for software verification, validation and testing.

Basic Strategy for Software Verification and Validation

The BNI software V&V program is established to meet the following general requirements.

- Testing shall be sufficient to determine that the software produces a valid result for its intended function.

- Test results shall be documented including test method, acceptance criteria, test result, and acceptability.

- Changes to software shall be controlled and documented.

- Testing shall be conducted to ensure that changes do not introduce errors.

BNI will meet these requirements by performing as much "out-plant" testing as possible in order to minimize "in-plant" testing. In-plant testing is essentially field testing after equipment has been installed. Out-plant testing would be performed prior to field installation. For the WTP, in-plant testing must be limited due to the following reasons.

- There is limited time to perform low-level testing of software performance in-plant.

- There is limited time available for any potential re-work based on field identified logic errors.

- There is limited ability to perform plant system testing in the absence of the control system, due to a plant design that features centralized control of plant equipment.

These problems tend to make software testing after installation more difficult to accommodate.

Increased out-plant testing can be accommodated due to the following.

- Software developers are integrated with WTP plant system engineers and designers which, allows software to be developed as the plant physical design evolves. This reduces errors and minimizes changes since mechanical system design can be completed prior to completing software development.

- Control system hardware will be available for programming and testing prior to field installation.

- Control hardware is consistent across WTP designed control functions and with many of the major vendor-designed systems.

- End users will be present during software development and testing and therefore, can better assume design authority and control from software developers without the need for additional testing.

The BNI approach for the software testing will involved the following:

- Out-plant testing will demonstrate and prove that facility level software meets acceptance criteria to the greatest extent possible.

- Out-plant test platforms (software and/or hardware) will be designed to accommodate the greatest portion of the testing requirements than can be reasonably achieved.

- Test requirements that cannot be met due to test platform limitations will flow to subsequent testing.

- The testing strategy will provide adequate test overlap to ensure that interface functions are tested.

- Configuration management processes will maintain software integrity from the test phase through the operational phase.

- Field testing will be performed only as required based on the following conditions.

    --Field-test the software features that cannot be adequately tested on out-plant test platforms.

    --Re-test software features on a graded approach based on safety, quality, or economic impact.

--Field testing of plant systems will be primarily to demonstrate that the integrated system performance meets Test Acceptance Criteria established by the Design Authority.

Figure 5 depicts the WTP ICN software strategy in terms of the types of testing required and how it will be performed according to test plans (TP). The strategy reflects logical planning and appropriate documentation for executing necessary software testing.

Software V&V testing will be performed in parallel to SFS implementation and ICN hardware design and fabrication. V&V will continue on through system functional acceptance testing, where the system software will then be baselined for software maintenance and ultimate turnover to plant start-up personnel and resources. The schedule logic for the associated activities is shown in Figure 6.

Out-Plant Testing

Out-plant testing will be performed via Hardware Acceptance Tests (HAT) and Functional Acceptance Tests (FATs). Upon completion of the FATs, the control system will be sent to the field for installation.

HATs are performed on the ABB-built target control system in Richland. The target control system is the actual equipment to be installed. This testing will be conducted by ABB and witnessed by BNI engineering. The focus of the testing is on software environment performance and functionality and to ensure the system is compliant with specifications.

FATs are also performed on the ABB-built target control system in Richland. This testing will be conducted by BNI engineering (C&I), witnessed by C&T, and supported by ABB. The focus of this testing is on system integration in order to reduce checkout in the field.

Schedule logic for activities leading up to functional acceptance testing were previously shown in Figure 1.

In-Plant Testing

In-plant testing will be conducted by BNI C&T after the control system is installed in the field. This testing will be supported by BNI engineering (C&I) and ABB. The focus of this testing will be on items not tested during earlier test phases and will be to verify operability and performance of each control system environment.

Test Process and Documentation

The basic process for performing testing is as follows.

- Develop a test plan for V&V
- **Verify** that design meets the requirements
- **Verify** that implementation incorporates the design

- Developing and approving test cases
- **Validate** the software by executing the test cases
- Report verification and validation results

The documentation required for V&V includes Test Plans and Test Reports.

Test Plans contain:

- Verification and Validation requirements for the appropriate software architecture layer.

- The process for Verification Testing
  - Comparing design to requirements
  - Comparing (via walk-through) implementation to design

- The process for identifying validation test cases
  - Each requirement identified will be explicitly tested
  - The level of the documentation for each test case will be graded in accordance with the risk associated with the requirement

Test Reports contain:

- Test Environment

- Verification test results
  - Test results will include highlighted copies of documents used in the test
  - Test failures are documented by redlining the appropriate test documents

- Validation test results
  - Test results for all requirements
  - Test cases approved and executed
  - Test failures are documented on the appropriate test case form

Test plans are developed according to the software architecture layer. With reference to the software architecture shown in Figure 4, Table 3 below identifies the software layer and the associated test plan and test scope.

Table 3

Software Layer	**Test Plan**	**Testing Scope**
Inter-Facility Software Layer	TP-1	Inter-facility Recipe Procedural Control Tests
Facility Software (Intra-Facility) Layer	TP-2	Intra-Facility Recipe Procedural Control Tests
Inter-Facility Software Layer	TP-3	Inter-Facility Basic Control Tests
Facility Software	TP-4	Intra-Facility Basic Control Tests
Sub-project/Unit Software (Plant	TP-5	System Unit Procedural and Basic

System) Layer		Control Tests
System Wide Functions (Global Function) Layer	TP-6	ICN (System-wide Functions) Tests
Control Library (Software Object) Layer	TP-7	Control Library Typical Tests
All Layers	TP-8	Functional Acceptance Tests

Test plans are described in more detail as follows.

- Test Plans 1 and 3 provide for testing software for logic between systems not within the same Facility. TP-1 is designed to test the Procedural Control portion of the Facility to Facility functions and TP-3 is designed to test the Basic Control portion of the Facility to Facility functions.

- Test Plans 2 and 4 provide for testing software for logic between systems within the same Facility. TP-2 is designed to test the Procedural Control portion of a Facility's System to System functions and TP-4 is designed to test the Basic Control portion of a Facility's System to System functions.

- TP-5 tests software components functionality as extracted from the system Test Acceptance Criteria (TAC). Plant system layer software is tested for intended functionality and is exercised on the ICN Development System to see if it can be forced to produce an invalid or improper output state.

- TP-6 tests Global Functions including, but not limited to, Ethernet & Control Networks, Displays, Diagnostics, Multiple events and alarms, and Network interfaces. This test provides verification and validation that the global functions of the ICN meet the design requirements

- TP-7 tests Library Elements logic created to be reused time and again and only needs to test the functions of the library elements once. Library elements support software logic functions throughout all testing and are therefore indirectly tested repeatedly during Plant System Software testing.

- TP-8 involves Functional Acceptance Testing. Following all the testing on the ICN development system, implemented software is tested on the target hardware (final system hardware). TP-8 tests hardware integration (HAT), software integration, scalability of ICN components for the facility overall performance.

In-Plant Testing

For the ABB supplied software and hardware, *Component Level Testing* is performed in which, all I/O is tested in-plant. However, a variety of field devices will be tested on the Developmental System in the course of setting up for Foreign Device Drivers. This is essential for risk mitigation to ensure that the I/O will work in the field. COTS applications and environmental

software is tested indirectly through its use in testing software objects in the other tests performed.

Field testing will be performed after installation to progressively prepare components and systems toward integrated plant operation. To accomplish this, several areas of testing will be conducted as described below:

- ICN component testing will be performed prior to energizing ICN components to check for proper installation and termination; to perform signal attenuation and scheme checks; grounding and power checks; and configuration verification.

- ICN system testing will be performed to accept the ICN prior to proceeding to plant system testing. System testing will involve checking network communication and integration, system loading, reliability and software integration.

- Plant system component testing will be conducted to prepare for system level testing. This will involve checking system components for proper installation and configuration, checking power supply/motive force, device function, smart device firmware version, and loop checks through the ICN.

- Plant system testing will prepare systems for integrated plant testing. This testing is performed to demonstrate system performance based on TAC, and graded re-testing of system functions based on safety, quality, economic risk

5. Gain additional knowledge and insight into the ICN system architecture.

Insight into the ICN system architecture was obtained by the BNI presentation and discussions with the system engineers. Most of information about the ICN architecture however, was gained through various document reviews. An ICN Summary Description report was written in follow-up to these reviews. This report is provided in Attachment 1.

6. Determine that design is consistent with implementing standards and requirements.

The documents evaluated for this element are those listed below.

- ANSI/ISA-S88.01-1995, *Batch Control Part1: Models and Terminology*

- IEC 61131-3, *Programmable Controllers Part 3: Programming Languages*

- ANSI/ISA-S5.5-1985, *Graphic Symbols for Process Displays*

- ANSI/ISA-S5.1, *Instrumentation Symbols and Identification*

- ANSI/ISA-S5.3, *Graphic Symbols for Distributed Control/Shared Display Logic Instrumentation and Computer Systems*

These standards are listed in chapter 9 of the BOD for Control and Instrument Basis of Design. (24590-WTP-DB-ENG-01-001, Rev 1B, *Basis of Design*)

It was verified that the standards are also referenced in the following documents:

- 24590-WTP-3PS-JD01-T0001, Rev 2, *Engineering Specification for Plant Wide Controls Systems (Integrated Control Network)*

- 24590-WTP-3PS-JD01-T0410, Rev A, *Engineering Specification for System Design Document for the Integrated Control Network*

The ICN Software Plan references S-88.0 for definitions and this standard is specifically applied in 24590-WTP-GPG-J-001, Rev 0, *Design Guide: Preparation of Control System Software Functional Specifications*

The ABB System Guide indicates the ABB system software utilizes the programming languages defined in 61131.3, and the SFS for *HLW Demineralized Water (DIW) System* was evaluated, specifically logic diagram (LD-01), where it was verified that this diagram implements the functional blocks and definitions provided in 61131.3.

As verified by review of the BNI Software Library specification, sampled SFSs & SDDs, and the Control Library Terms, Definitions, and Symbols & Legends for the ICN; standards, S5.1, S5.3, and S5.5 are also being implemented.

7. Address and close issues from the independent review conducted in July 2004.

In this section concerns from the July 2004 report are addressed by BNI. The concern is first stated generally as it appears in the July report followed by the BNI response. The adequacy of the responses speaks for themselves.

The concerns fall into three areas:

- Standardization and Consistency: How does WTP C&I manage standardization and consistency in control system design?
- Prioritizing Design: Discuss how control system design is prioritized and managed.
- ICN Systemization Design: Explain how ICN system architecture is arranged.

Concern (2.2): Standardization and Consistency

The actual concern is not stated here. However, BNI captured the essence of the concern with the following statements.

- Design within C&I is separated into Central and Facilities groups.

- Geographical dispersing of the groups should include a standardized approach to control and operation.

- Extra effort needs to be sustained so that design philosophies maintain synchronization and rationalization such as SFS synchronization.

- Differences in implementation or “look and feel” between process areas need to be avoided and inter-process transfers and interactions need to be managed.

In responding to this concern, explained how the C&I group manages standardization and consistency in the control system design. This is described here with respect to SFS developments and the Human Machine Interface (HMI) design.

SFS Design Documents and Coordination

The document basis for designing SFSs is maintained by C&I Central and utilized by Facilities. These documents include:

- SFS Document Template that provides the SFS outline and diagram templates.

- Design Guide (24590-WTP-GPG-J-001) that provides guidance on preparing SFSs.

- Control Library (24590-WTP-3PS-JD01-T0002) that provides Facilities with pre-developed software logic elements such as pump/valve control typicals and function blocks.

- Desktop Instructions that explain how system design details are written within the SFS. There are currently six Desktop Instructions.
    - SFS Document
    - System Overview Diagrams
    - Software Scoping Diagrams
    - Sequential Functional Charts
    - Functional Diagrams
    - Logic Diagrams

The interaction between C&I Central and Facilities is also a large factor in maintaining SFS standardization and consistency. C&I Central maintains the documents required for Facilities to design SFSs in collaboration with the Facilities. SFS Coordinators are assigned to each facility to serve as a liaison between C&I Central and Facilities. The SFS Coordinators function in the following capacities.

- The SFS Coordinators interact with C&I Central to resolve any Facility issues that could impact SFS design documents (Control Library, Templates, etc.).

- Within Facilities, the SFS Coordinator is a single point of contact to other SFS Coordinators and SFS authors for guidance on SFS design.

- SFS Coordinators collaborate with other Facility SFS Coordinators to ensure consistency of design across Facilities.

- All SFS Coordinators meet with C&I Central on a biweekly basis to address current SFS issues and any updates, among which includes consistency of design.

SFS Reviews are also conducted in which SFS authors host design reviews at the 60% and 100% level. These are multidiscipline reviews attended by:

  - C&I Central
  - C&I Facilities
  - C&T (Commissioning and Training)
  - E&NS (Environmental and Nuclear Safety)
  - Mechanical Systems/Mechanical Handling/HVAC
  - Electrical

Meeting minutes are captured and issued for the SFS Design Review and comments are incorporated into the SFS. The SFS is also sent to affected disciplines for an Engineering Document Review (EDR).

Human Machine Interface Design and Coordination

Operator Interfaces are standardized in accordance with Basis of Design (24590-WTP-DB-ENG-01-001 Section 7.3.6) that states:

> "Human factors engineering principles will be applied to all aspects of operator interface design. … A simple and consistent operator interface throughout the WTP will be developed to minimize the potential for operator confusion."

C&I Central creates HMI graphics for ALL Facilities and C&I Central, Operations, and Human Factors maintain a collaborative focus on consistency and operability to maintain the same "look and feel".

The design documents that allow for a standardized and consistent HMI design include:

- Engineering Specification for System Design Document for the Integrated Control Network (24590-WTP-3PS-JD01-T0410) that defines how elements are to be presented on the HMI screen. This includes color schemes, symbols, and methods of control.

- Control Library (24590-WTP-3PS-JD01-T0002) that contains typicals designed with designated areas for operator inputs/outputs showing what control or indication is required (indication, alarms, etc).

- Primary Documents (P&ID) and SFS Functional Diagrams that define the process and interrelation of the components. These documents detail what elements are used and how to use them in the context of the process.

There are also HMI Graphics Reviews that are conducted in the following fashion:

- C&I Central, Operations, and Human Factors conduct design reviews on each HMI.

- Detailed Meeting Minutes are written and issued as a CCN in order to track issues covered in each review.

- Results of the HMI development are published in the System Design Document (SDD).

Concern (2.3): Re: Prioritizing Design

"There appears to be some uncertainty about the detail design within C&I of certain process functions or stages….This has been quoted as one reason for the postponement of the application of comprehensive, sequence or procedure based, automation. This needs to be fully explored so that the limits and areas of most risk are understood. Any high-risk areas need to be resolved with software implementation delayed until design is more certain….software implementation should be prioritized to ensure work is not inappropriately channeled to uncertain areas.

The BNI Response:

Design uncertainty occurs if vendor information on system equipment does not support the SFS development schedule or if there are unresolved issues related to process design (i.e., hydrogen mitigation with respect to PJM control design).

Design uncertainty, related to C&I process design, is managed through prioritizing the design and scheduling work based on resolution of design uncertainties. Scheduled work is logically tied to vendor submittals. If documents must be issued and the schedule cannot be readjusted, items with design uncertainty are placed on HOLD showing that continuing work is at risk.

BNI used the recent procurement of the Autosampling system (ASX) to explain how this process was applied.

The ASX is common to the major plant facilities and involves vendor supplied equipment to perform auto-sampling. In the first contract award, it was determined that the ASX vendor would not meet specification requirements within their initial bid. Hence, the ASX contract was re-bid and subsequently awarded to a new vendor that will meet the specification requirements. This change of procurement created uncertainty in ASX design. Consequently, ASX P&IDs contained a HOLD that reflected the fact that auto-sampler vendor information was not yet received. The HOLD on the primary document was carried on to documents within C&I that were affected. For example, the ASX SFS incorporated the HOLD. HOLDS within the SFS document are tracked throughout the software life cycle. Once cleared from the P&ID, the HOLD is cleared on other affected documents.

Concern (2.4): Re: ICN Systemization Design

…As may be understood or expected the DCS system architecture shows examples where more than one DCS Controller can cover an overall process or service function…. Also, the routing of

signals to/from a controller can be heavily influenced by geography for considerable cost advantages in routing to the nearest available controller. Is there a general criteria or policy that would override these types of considerations? ...have systemization considerations been included on the design and management of all systems…?

The BNI response:

BNI provided a direct quote from the Basis of Design (Section 7.3.2) that adequately addresses the concern. The quote is as follows:

Where practical, the components of the control system will be systemized per the WTP system and area definitions. This segregation will allow the potential for phased delivery and commissioning of the control system, as well as reducing susceptibility to common mode failure.

Where systemization is impractical due to technical or cost considerations, several functions may be assigned to a single component. The following criteria should be satisfied when combining multiple functions:

- A logical procurement strategy should still be possible.

- The equipment covered by the functions should be suitable for installation, commissioning, and operation in parallel or as a single unit.

- The software implementing the functions on each distributed element will be modular and consistent in configuration with all other distributed modules to facilitate diagnosis and repair during commissioning and future maintenance.

The C&I approach to the ICN design is also significant to addressing the concerns above and maybe expressed as follows.

- Design is systemized at the highest levels through primary and supporting documentation, such as P&IDs, MHDs, System Descriptions, etc.

- As design evolved, geographical considerations were factored into the design.

- System architecture was rationalized based on procurement strategies for components such as cross-system MCCs and equipment packages; cost effective use of hardware; and reduced cabling.

As a result of the design rationalization, less than 10% of I/O is geographically separated from its related system controller, the most effective use of available space will be made, and more effective remote I/O and controller utilization will be achieved.

The rationalized design is also supported by the following ICN features:

- Modular software components that can be loaded on line by application

- Controller redundancy.
- Redundant power supplied by normal and UPS sources.
- Hot swappable components.
- Redundant communications.
- Extensive self-diagnostics.

These characteristics also increase availability and facilitate commissioning and maintenance.

Design rationalization also supports the following commissioning strategy:

- Network infrastructure functional prior to system testing.
- ICN system functional prior to plant system tests.
- Component testing on a system basis.
- System testing following component testing.
- C&T procedures will allow hot work in enclosures with commissioned systems.

In addition to the concerns above, the July-04 report also made suggestions that BNI responded to in the Nov-04 assessment. The suggestions recommended Prototyping and use of the Simulator. The following provides explanation.

Suggestion (2.5-1): Prototypes

"Use selective prototypes.

The project may see benefit in identifying controllers …to bring forward, complete and test early. At least one such controller should be completed early from each major process area…."

BNI responded as follows.

All components of the WTP software are prototyped which also involves various degrees of simulation. Prototyping aides in quickly exposing implementation constraints not clearly defined in the vendor literature. Prototyped software may eventually become base-lined software or it may be completely discarded. Software prototyping is used to train programmers. Only after capturing the experience with the prototype is the formal development process initiated. Early prototyping is fundamental to success in the WTP design. Some prototyping activity examples include:

- Foreign Device communication, semocode, addressable relay, multilin, digitrip, foundation fieldbus devices
- Typicals
- Peer to Peer communication
- Software Structure
- Graphics
- Batch (PTF-CRP, PTF-FRP)
- Equipment FAT and early software development activities (rev A SFS)

With regard to Foreign Device communication, a major project goal is to be involved in prototyping communication with smart field devices or systems well before final software is required. This involves obtaining the device or at least the communication component. Once the device or component is obtained, the communication portion of the software is prototyped. Prototyping involves, simulation, working with the vendor etc. in order to prove that the ABB system can communicate with the device or system. The software life cycle methodology is then applied to the prototyped software.

Another area involving prototyping deals with equipment Functional Acceptance Testing; with the goal of being involved in the acceptance of vendor supplied packages. The non-QAS software related to packaged equipment follows a software life cycle. The software is field tested prior to acceptance of the equipment. As a by-product of testing, all of the prototyping of the various software and hardware components are validated. At this point the software and hardware have been simulated to the highest degree possible on the target system.

Also, the QAS software developed via the SFS for packaged equipment is prototyped.

Suggestion (2.5-2): Simulator

The essence of the suggestion is stated as follows.

Enhance the use of simulation by taking advantage of the Training Simulator and developing process models.

BNI responded as follows.

Software is simulated where necessary and practical and as mentioned above, software related to packaged equipment is simulated. Pulse Jet Mixer (PJM) software was simulated and involved utilizing process data acquired from an existing PJM system that was controlled via a third party controller. Simulation software has also been produced during Batch control prototyping i.e. simulating flow when a pump starts and the path is established.

Use of the Training Simulator could be used for validating that the Plant System as a whole meets the Test Acceptance Criteria related to process functionality, particularly if the process model performs exactly like the plant then errors related to the design of the software to meet the TACs could be found.

However, through prototyping and rigorously following the software lifecycle methodology, simulating the software using the Training Simulator is not required.
Simulation of the software occurs during the normal work process i.e. development, prototyping, testing and the software requirements are not complicated from a control system point of view. Also, the project schedule reflects plant system software validation activities completing prior to Training Simulator availability.

Suggestion (2.5-3): The OR Model

“Review the use of the integrated OR model.”

The suggestion was made primarily because the reviewer had questions regarding the OR model but did not have an opportunity to meet with the project staff associated with the OR model work. Had such an opportunity been available, the reviewer would have come to the conclusion that the OR model work has the following features:

- The model ensures the WTP design incorporates appropriate operational features to meet plant capacity requirements
- The OR model is in alignment with other plant models
- The OR model is linked with each of the plant facilities and the Lab
- The model is based on appropriate engineering data
- The model receives appropriate periodic reviews by BNI and ORP
- There is an OR Model Annual Assessment Report

These elements were discussed in detail during the Nov-04 BNI presentation.

Typical Schedule Logic – ICN Component Delivery and Out-Plant Testing

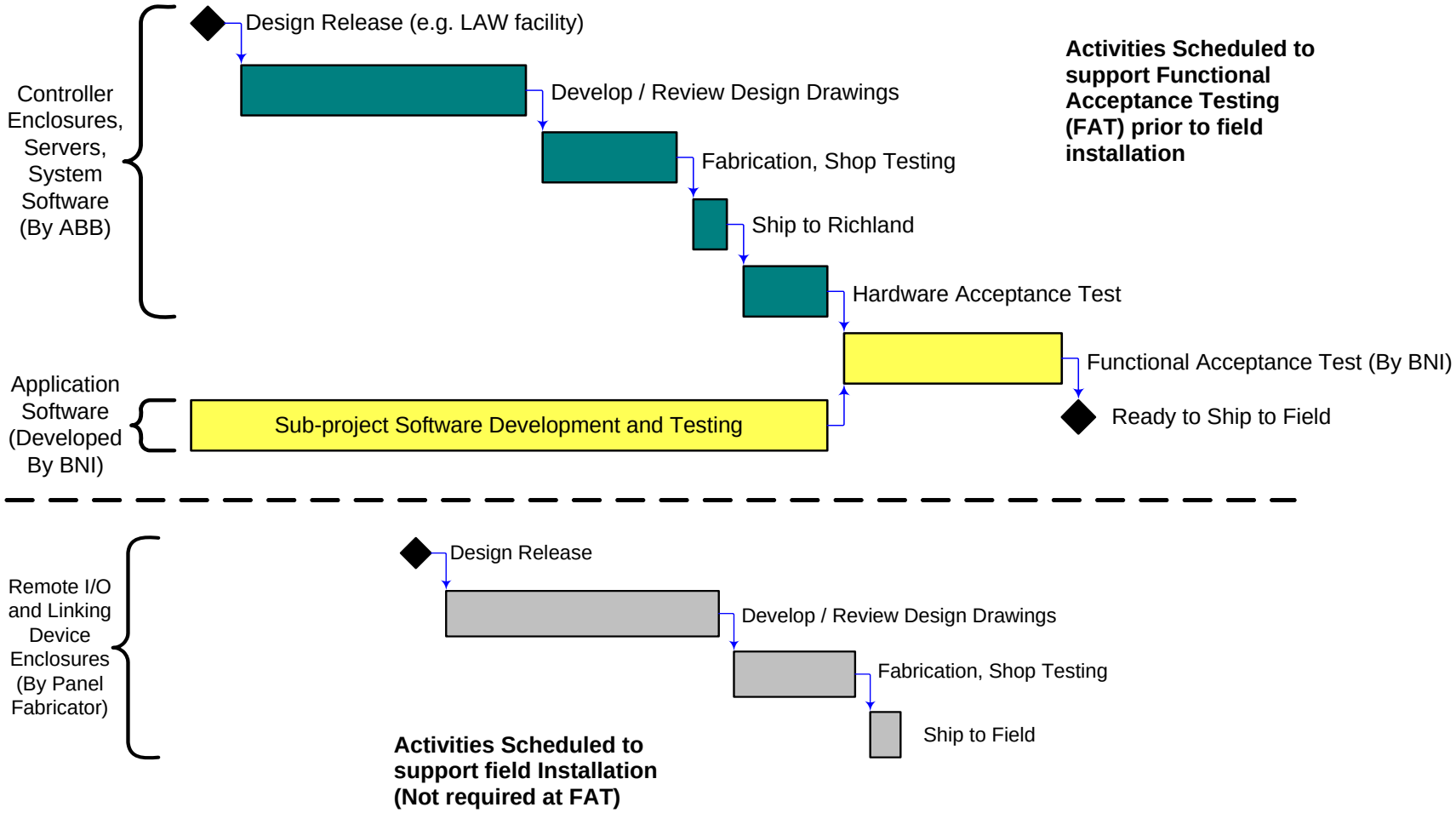


Figure 1

ICN Development Timeline

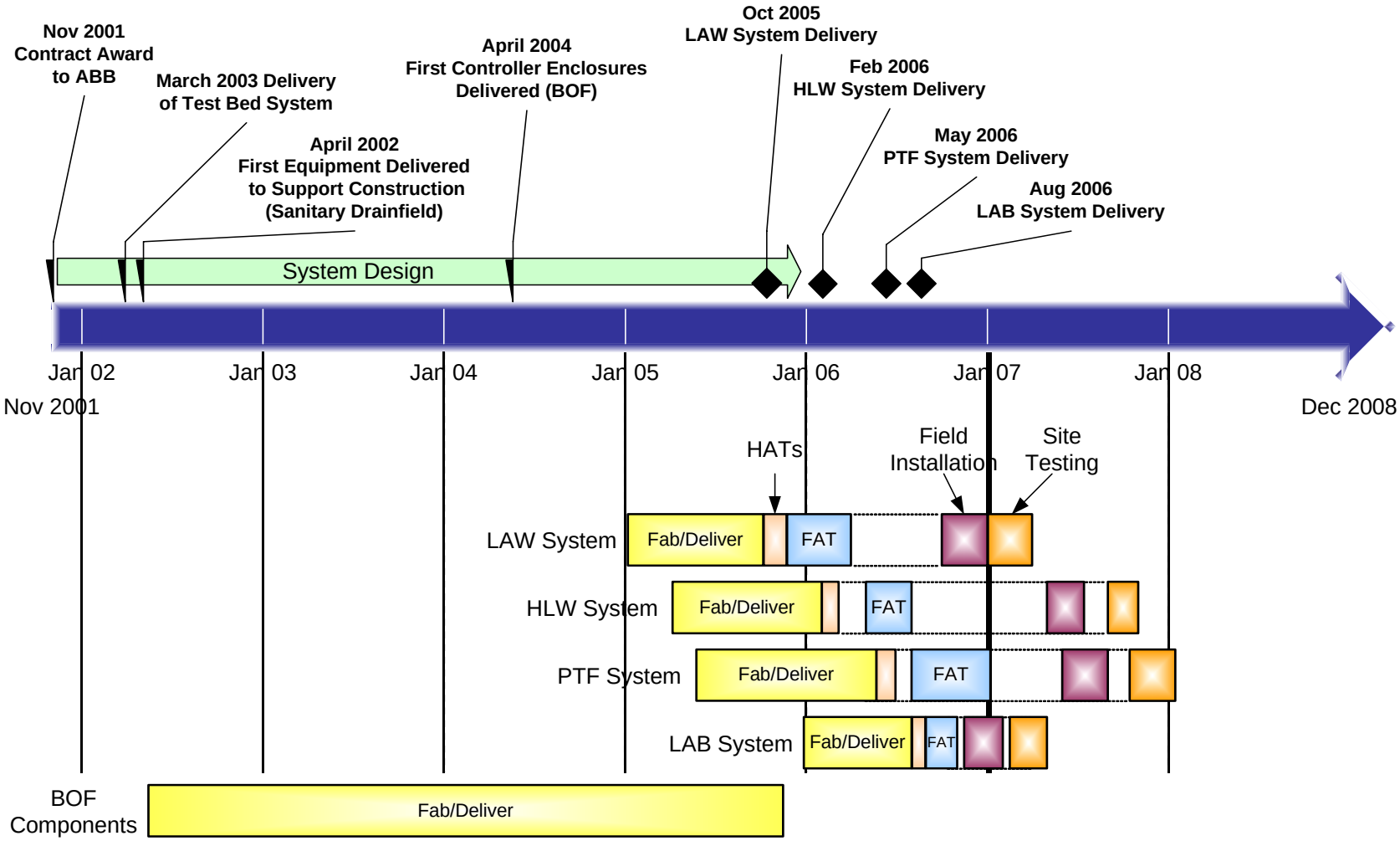


Figure 2

Software Life Cycle Phases and Products

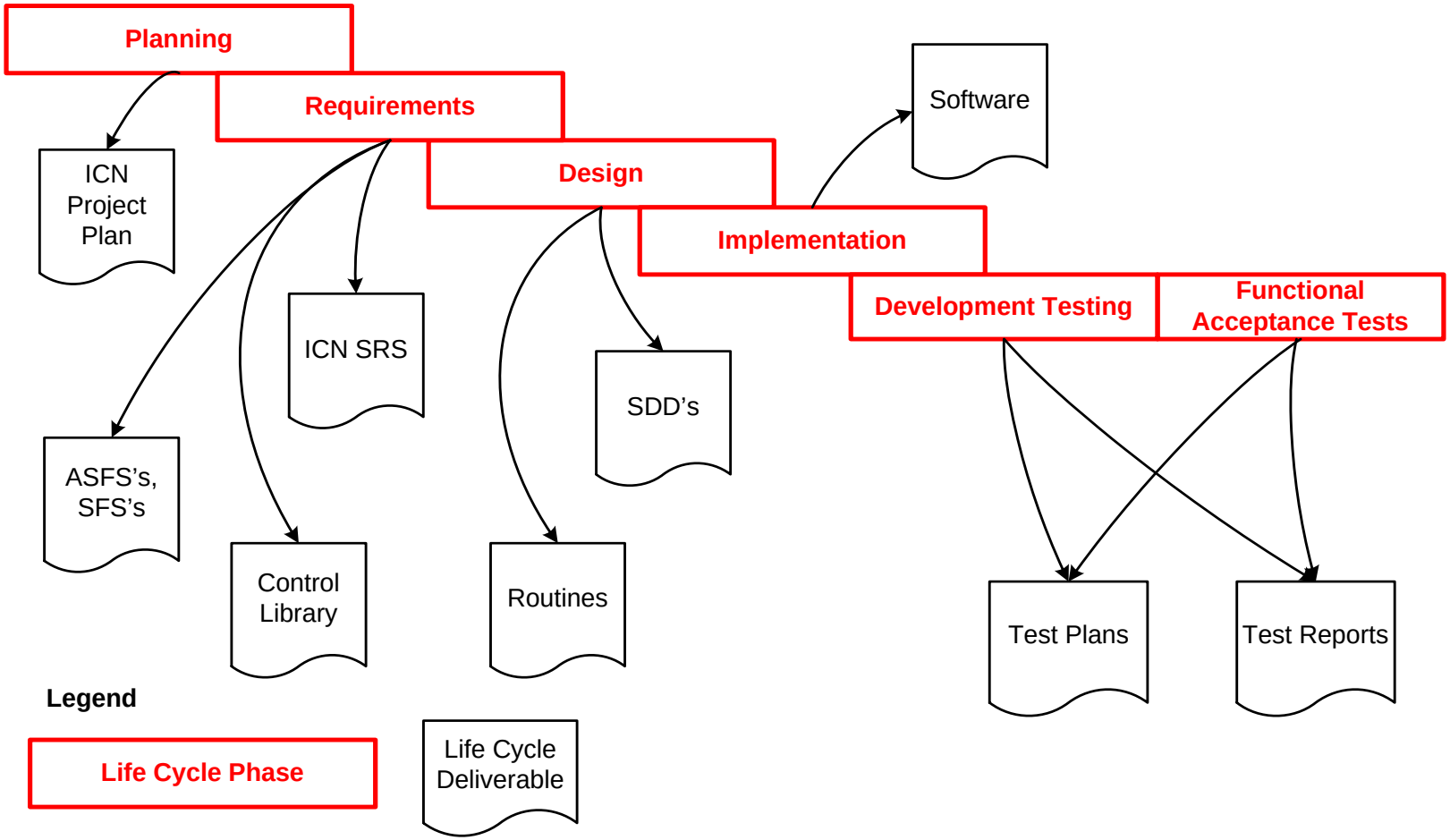


Figure 3

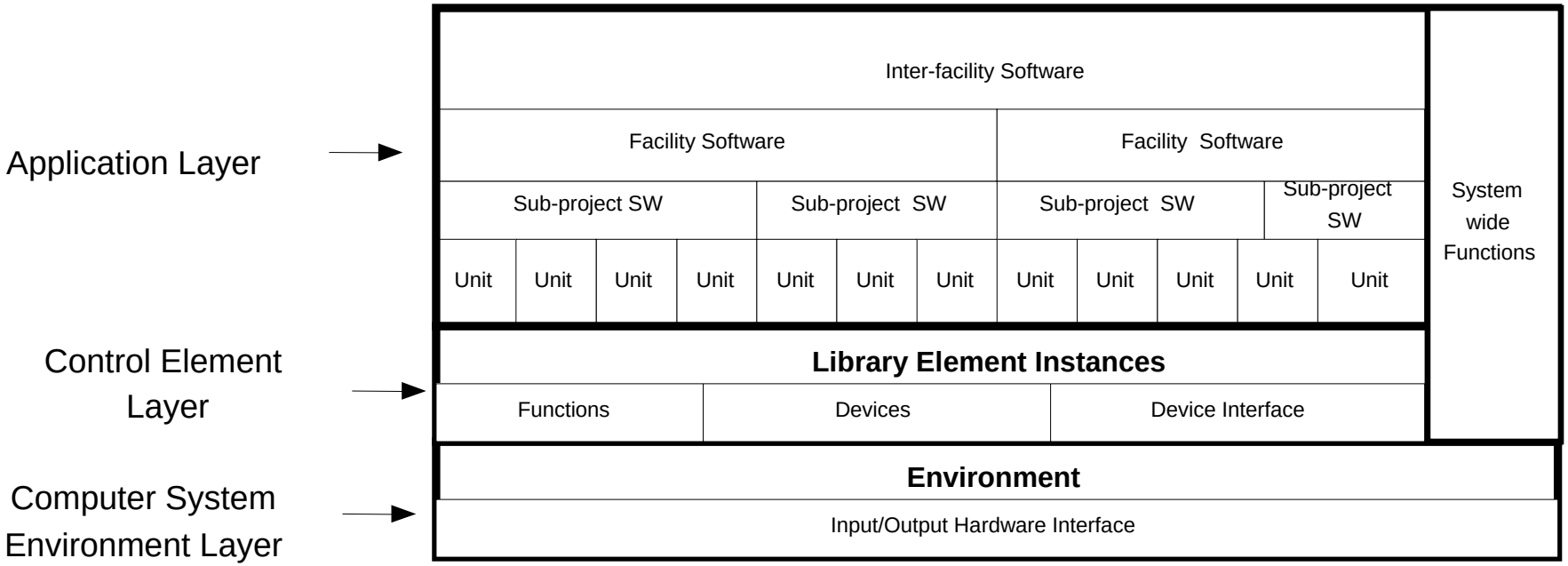

Application Layer
Control Element Layer
Computer System Environment Layer
Inter-facility Software
Facility Software
Facility Software
Sub-project SW
Sub-project SW
Sub-project SW
Sub-project SW
Unit
Unit
Unit
Unit
Unit
Unit
Unit
Unit
Unit
Unit
Unit
Unit
System wide Functions
Library Element Instances
Functions
Devices
Device Interface
Environment
Input/Output Hardware Interface

Figure 4

WTP ICN Software Verification and Validation Strategy

Test Requirements Flowdown by Test Platform

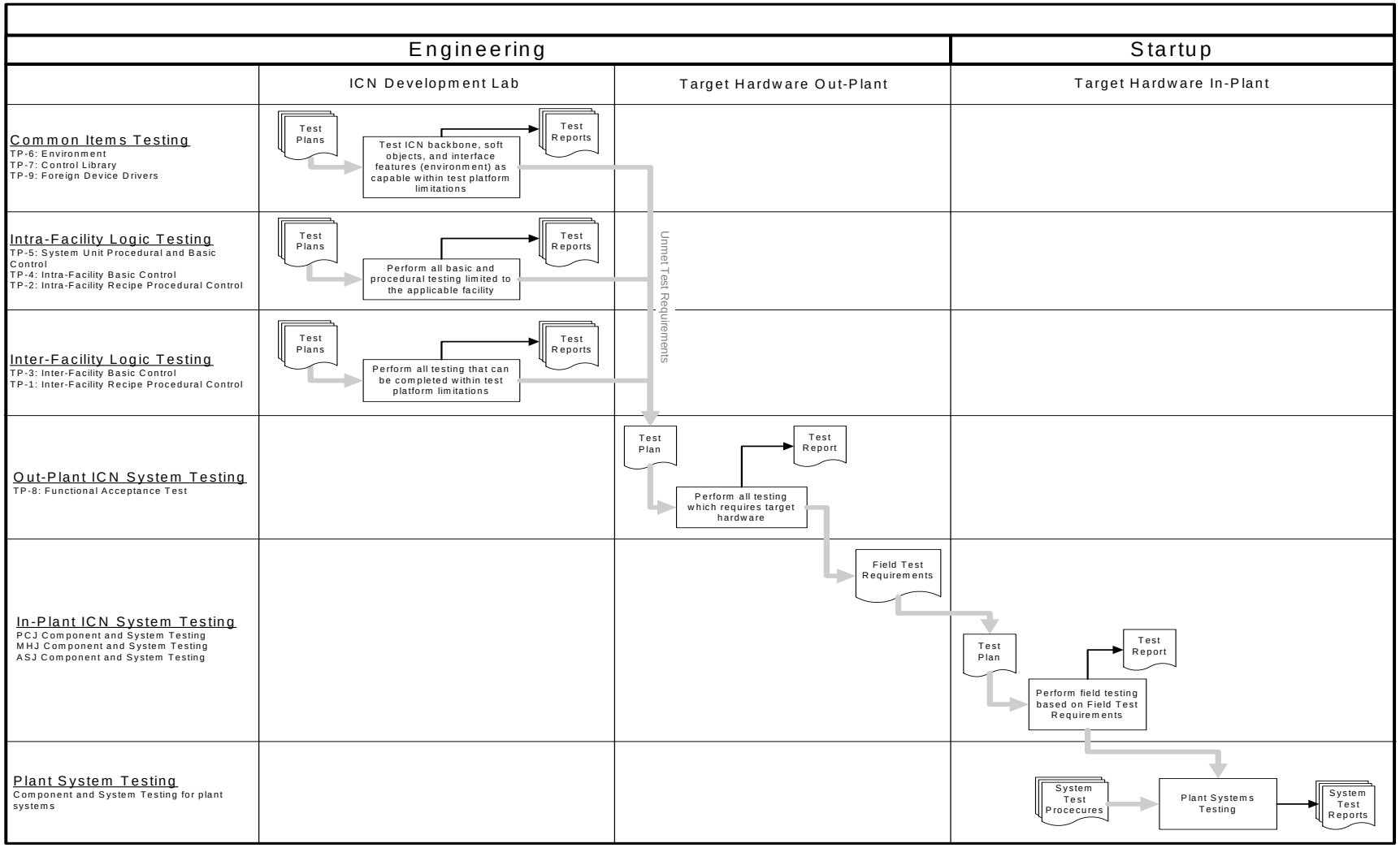


Figure 5

WTP ICN Software V&V Testing Schedule Logic

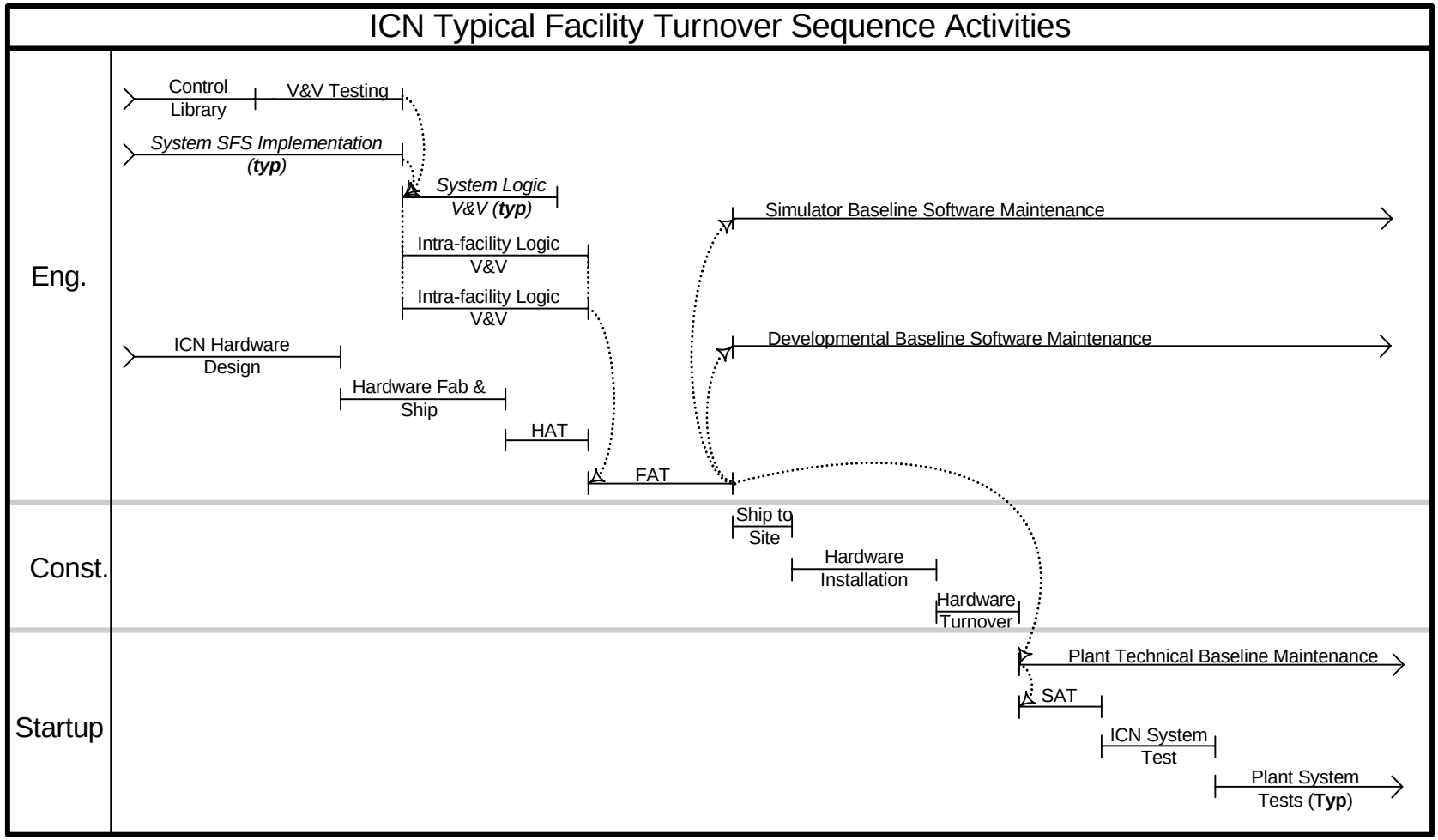


Figure 6

Appendix A – Physical Model

Software developmental work being performed by BNI for the WTP revolves around a concept called the physical model. This model is explained in detail in ANSI/ISA-S88.01-1995, *Batch Control Part 1: Models and Terminology*.

The following (simplified) explanation is provided (almost verbatim) from G. K. McMillan, *Process/Industrial Instruments and Controls Handbook.*

****

The physical model describes what equipment is available for the batch process. The physical assets of an enterprise such as an industrial plant, involved in batch manufacturing or processing (as in the case of the WTP), are usually organized in a hierarchical fashion as described by the physical model. Lower-level groupings are combined to form higher levels in the hierarchy. In some cases, a grouping within one level may be incorporated into another grouping at that level.

The model has seven levels (See Figure A), starting at the top with an enterprise, a site, and an area. These three levels are frequently defined by business considerations, and are not modeled further in S88.01. The three higher levels are part of the model to properly identify the relationship of the lower-level equipment to the manufacturing enterprise.
The lower four levels of this model refer to specific equipment types. An equipment type in Figure A is a collection of physical processing and control equipment grouped together for a specific purpose. This grouping is usually done to simplify operations of the lower-level equipment by treating it as a single larger piece of equipment.

Equipment entities are defined for the lowest four levels of the physical model (i.e., process cell, unit, equipment module, and control module).

Control Module

A control module is a collection of sensors, actuators, other control modules, and associated processing equipment. A control module acts as a single entity from a control standpoint, and it is the direct connection to the process through its sensors and actuators. The control module is the lowest level of equipment grouping that operates as a single entity. A control model executes basic control and cannot execute procedural control. The following are some examples of control modules:

1. A flow control loop that operates by means of the set point of the controller.

2. An on-off automatic block valve with limit switches that operates by means of the set point (e.g., open and close) of the valve.

3. A header that contains several automatic block valves and that directs flow to different destinations based on a set point to the header.

Equipment Module

An equipment module is a collection of control modules and/or other equipment modules. An equipment module can carry out a finite number of minor processing activities (i.e., phases), and it contains all the necessary processing equipment that is need to carry out these processing activities. This implies that in order to define an equipment module, knowledge of the specific minor processing activities and equipment capabilities must be obtained. The following are some examples of equipment modules:

1. A weigh tank that is shared by multiple units but that can only be used by one unit at a time.

2. A filter that is a permanent part of a particular unit.

3. An ingredient supply system that is shared by multiple units and that can be used simultaneously by all units.

Control modules and equipment modules are used because the combinations of various instrument functions can be addressed as a single entity.

Unit

A unit is usually centered on a major piece of process equipment, and it frequently operates on or contains the complete batch. Although a unit may operate on or contain only a portion of a batch, it cannot operate on or contain more than one batch at a time. Defining a control unit requires knowledge of the major processing activities as well as the equipment capability.

Units are the primary object for automatic control, and they have a direct relationship with unit procedures and operations. A unit is made up of control modules and/or equipment modules, but not other units, and there will often be multiple units involved in making a batch. Control modules and equipment modules can exist as:

- Permanently included parts of a unit
- Temporary attached parts of a unit
- Totally separate from a unit

When control modules and/or equipment modules are not part of a unit, they may be connected to a unit, and then may be commanded like any other object in the unit.

Process Cell

A process cell is a logical grouping of equipment that is required for the production of one or more batches. A process cell may contain more than one grouping of equipment that is needed to make a batch. That grouping is referred to as a Train. The equipment that was actually used to

execute a batch is referred to as the Path. A process cell frequently contains more than one batch as a time.

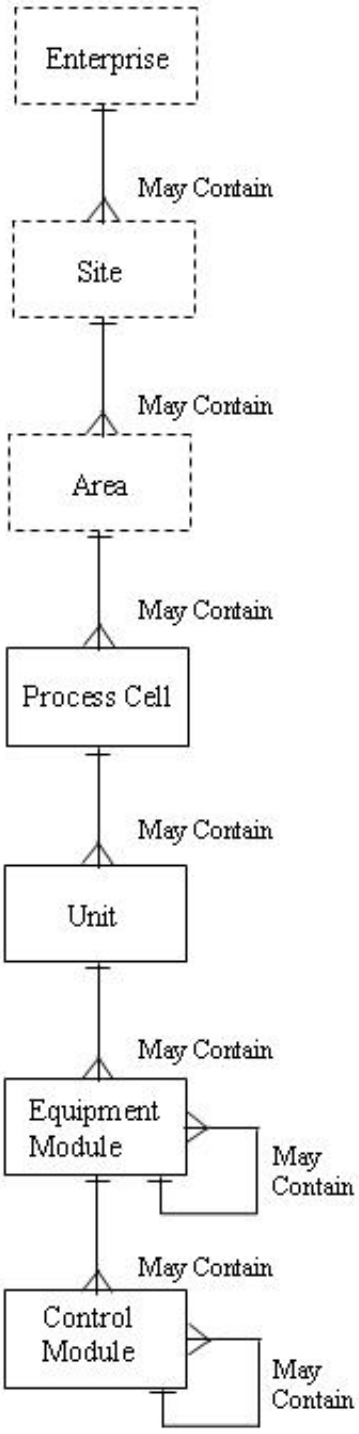
Equipment Control Terms

Basic Control – Basic control is dedicated to establishing and maintaining a specific state of equipment and process, and it includes the following:

- Regulatory control
- Interlocking
- Monitoring
- Exception handling
- Repetitive discrete or sequential control

Procedural Control – Procedural control is a characteristic of batch processes, and it is the control that directs equipment-oriented actions to take place in an ordered sequence in order to carry out some process-oriented task.

Batch control – Batch control encompasses the control activities and control functions that provide a means to process finite quantities of input materials by subjecting them to an ordered set of processing activities over a finite period of time using one or more pieces of equipment.



Physical Model

From ANSI/ISA-S88.01-1995, ***Batch Control Part 1: Models and Terminology***

Figure A

Attachment 1:

Integrated Control Network Summary Description

Attachment 1

To

ORP Design Oversight Report

Waste Treatment Plant

Integrated Control Network Summary Description

November 2004

U.S. Department of Energy
Office of River Protection
Richland, Washington

INTEGRATED CONTROL SYSTEM SUMMARY DESCRIPTION

The following report provides a brief overview of the Waste Treatment and Immobilization Plant (WTP) Integrated Control Network (ICN). This overview is intended as summary information for DOE Office of River Protection (ORP) technical and management staff and is a product of several document reviews performed during the ORP Design Oversight Assessment of the WTP ICN in November 2004. The contents of this report was compiled and consolidated from contractor generated documents (i.e. basis of design, system descriptions, specifications, design guides, etc.) as well as other literature such as *Process/Industrial Instruments and Controls Handbook*, by G. K. McMillan.

The DOE prime contractor responsible for delivery of the ICN is BNI. BNI has contracted with ABB (ASEA, Brown Bovari) for the ICN system development. ABB develops the system software, controller enclosures (including the devices that communicate with field equipment), network servers, etc. BNI develops the application software utilizing the system software developed by ABB.

Table of Contents

Terms and Definitions

Analog – Typically refers to a type of signal that represents a variable that may be continuously observed and continuously represented, as opposed to a signal that is either on or off, high or low, or is otherwise discrete. This type of signal may be considered analogous to some physical condition such as temperature, pressure, sound, etc.

ActiveX – Is a software architecture developed by the Microsoft Corporation that enables software components to interact with one another in a networked environment, regardless of the language in which they were created. ActiveX is built upon Microsoft's Component Object Model (COM, see definition below) and is essentially another term for Object Linking and Embedding (OLE, see definition below).

ASP – Active Server Page is a specification for a dynamically created Web page used in conjunction with ActiveX and HTML.

Basic control - Control that is dedicated to establishing and maintaining a specific state of equipment or process condition. Basic control may include regulatory control, interlocking, monitoring, exception handling, and discrete or sequential control.

Batch – The material that is being produced or that has been produced by the execution of a batch process or the entity that represents the production of a material at any point in the process. (i.e., a batch of concrete)

Batch control – Control activities and control functions that provide a means to process finite quantities of input materials by subjecting them to an ordered set of processing activities over a finite period of time using one or more pieces of equipment.

Bus – An electrical connection which allows two or more wires or lines to be connected together. In terms of a network, the bus network connects all the communications devices together.

Client – A device on a network that requests information or resources via a server (computer). Typically a client is a personal computer, workstation, or program that is served by another computer called a server. Clients come in two types, fat clients and thin clients. The difference between the two is that thin clients generally do not include storage memory, disk drives, or communications ports. They are low-cost and totally dependent on system servers.

Closed loop control – Control over a closed loop system by minimizing the error between a proscribed output and an adjustable input. A typical industrial closed loop system contains a primary element like a sensor, a device for comparing the sensor signal against a proscribe value and providing an error adjustment signal (setpoint controller), and a final control element like a valve that is adjusted in order to minimize the difference or error.

COM – A software architecture developed by Microsoft to build component-based applications. COM objects are discrete components, each with a unique identity, which expose interfaces that

allow applications and other components to access their features. COM also encompasses everything previously know as OLE.

Controller – A device which operates automatically to regulate a controlled variable. As used in the WTP, a controller is simply a remote field device computer containing a central processing unit, input/output capability, and memory for software and data storage. Controllers allow plant system process control to be located close to plant system equipment.

Control module – A control module is typically a collection of sensors, actuators, other control modules, and associated processing equipment that, from the point of view of control, is operated as a single entity. An example control module would be a regulating device consisting of a transmitter, a controller, and a control valve that is operated via the set point of the device. The control module represents the lowest level grouping of equipment in a plant systems' physical model that can carry out basic control.

Direct control – As applied within the WTP, direct control is synonymous with manual control or direct actuation as opposed to automatic control.

Discrete control – Simple on/off, run/stop, open/close, etc.

Ethernet – A local area network architecture/standard (network protocol) developed in 1976 by Xerox Corporation that utilizes primarily a bus topology. Ethernet dominates the network industry and supports data transmission rates of 10 Mbits/sec. A newer version, called Fast Ethernet, supports a data transmission rate of 100Mbits/sec. Both types will be used with the ICN.

Fiber Optics – A technology in which light is used to transport information from one point to another. More specifically, fiber optics are thin filaments of glass (a fiber optic cable) through which light beams are transmitted over long distances carrying enormous amounts of data at very high speeds.

HTML – HyperTest Markup Language is the authoring software language used on the Internet's World Wide Web.

Interlocks – Devices (relay contacts, switches, software, etc.) that connect pieces of equipment or equipment components together in such a way that one part cannot operate independently of the other or the functioning of one part is controlled by the functioning of the other.

Middleware – Software which resides between layers of software to enable the surrounding layers to work with each other. Middleware serves as a translation mechanism melding together application software across a network.

Multiplexing – The transmission of two or more signals over the same communication circuit (wire, cable, etc.).

Network – As applied to the WTP control system, a network is system of interconnected devices including computers, servers, human machine interface consoles, distributed controllers and other data communications devices. The devices are linked together and communicate via a fiber optics cable system (or other suitable wire media, such as shielded twisted pair, or coaxial cable).

Object – Any real-world entity (person, place, thing, concept, or event) that may be distinguished by its properties (attributes and behaviors), operations, and relationships.

OLE – OLE, object linking and embedding, is a compound document (a document that contains elements from a variety of computer applications) standard developed by Microsoft Corporation supported in the Windows operating system. It enables you to create objects (in this context, computer documents or files) with one application and then link or embed them in a second application (i.e., an Excel spreadsheet within a Word document). Embedded objects retain their original format and links to the application that created them.

OPC – Stands for OLE for Process Control and is simply the application of OLE technology to process controls. It is intended to foster greater interoperability between automation/control applications, field systems/devices, and business/office applications in the process control industry. OPC defines standard objects, methods, and properties, for servers of real-time information such as distributed process systems, programmable logic controllers, smart field devices, and analyzers in order to communicate the information that such servers contain to field devices compliant with OLE technologies.

Platform – A platform refers to the combination of hardware and software that forms the basis of a computer system. The platform also defines a standard around which a system can be developed. Once the platform has been defined, software developers can produce appropriate software and managers can purchase appropriate hardware and applications. The term is often used as a synonym of operating system.

PLC – A Programmable Logic Controller is a device originally intended to replace electrical relay logic used in industrial controls. Relay logic was dependent upon electromechanical relays that were bulky, comparatively slow, and consumed a lot of power. PLCs take advantage the electrical relay logic expressed in electrical ladder diagrams to implement relay logic via programmable electronics. PLCs receive inputs from field devices such as switches, sensors and transmitters, perform relay logic via on-board programmable software, and then provide outputs to drive switches, valves, actuators, etc.

Procedural control – Control that directs equipment-oriented actions to take place in an ordered sequence in order to carry out some process-oriented task.

Profile – A set of parameters defining the way a device acts. A profile is often used by one or more workstations or computers to determine the connections they will have with other devices and those devices they will offer for use by other devices. *Profiling* determines the profile of a piece of equipment on a network.

Protocol – A protocol is an agreed-upon format (or rule) for transmitting data between two devices. The protocol determines the following:

- the type of error checking to be used
- data compression method, if any
- how the sending device will indicate that it has finished sending a message
- how the receiving device will indicate that it has received a message

Real-time - is a term applied to computer systems in which, processing speed is so rapid that system output response to input appears immediate. Most general-purpose operating systems are not real-time because they can take a few seconds, or even minutes, to react. The term also refers to events simulated by a computer at the same speed that they occur in real life, such as plant operations.

Recipe – The necessary set of information that uniquely defines the production requirements for a specific product.

Regulatory control – In the industrial process control arena, this type of control usually refers to regulating or adjusting such process entities as flow, level, pressure, temperature, etc.

Sequence control – Control that ensures equipment elements are operated according to an established sequence (i.e. a valve is opened before a pump is turned on.)

Server – A server is a computer or device on a network that manages network resources. For example, a *file server* is a computer and a storage device dedicated to storing files. Any user on the network can store files on the server. A *print server* is a computer that manages one or more printers, and a *network server* is a computer that manages network traffic. A database *server* is a computer system that processes database queries.

Topology – The shape, layout, or configuration of a local-area network (LAN) or other communications system. Topologies are either *physical* (hardware) or *logical* (software). There are three common topologies used in LANs, Star topology, Ring topology, and Bus topology. The WTP ICN will use a bus topology. In a bus topology, all devices are connected to a central cable, called the bus or backbone. Bus networks are relatively inexpensive and easy to install for small networks. *Ethernet* systems use a bus topology.

Network System Overview

The WTP will utilize three major data networks for plant operations. These are listed below.

- Integrated Control Network (ICN) for process operation and control
- Plant Information Network (PIN) for managing plant data associated with production, operations and maintenance
- Information Technology Network (ITN) for providing users with essential data management tools

These networks function and interface via the Facility Network Infrastructure (FNI), which serves is the fiber-optics telecommunications backbone of the plant. See Figure 1.

These networks support the WTP operations in its five major facility areas; Pretreatment (PTF), High Level Waste (HLW), Low Activity Waste (LAW), Analytical Laboratory (LAB), and Balance of Facilities (BOF).

The networks are generally described in 24590-WTP-DB-ENG-01-001, Rev 1, *Basis of Design*, Section 9. Detailed information regarding the FNI is contained in 24590-WTP-3YD-FNJ-00001, Rev 0, *System Description for Facility Network Infrastructure.*

The ICN System Overview

The WTP control system is composed of Programmable Electronic Systems (PES) that are networked together on a common integrated control network. Generally, any piece of plant equipment that has an automating feature or component is included in a PES. The ICN is the real-time control and data acquisition platform responsible for process operation and control, as well as alarm and notification functions within the WTP. In conventional terms, the ICN is the plant Distributed Control System (DCS). The general features of a typical DCS are provided in Appendix A.

As indicated in Figure 1, the ICN is comprised of three major control systems:

- ***Process Control System*** for process control primarily in PT, LAW, & HLW with limited control functions in BOF and LAB.
- ***Mechanical Handling Control System*** for container and canister movement control and monitoring.
- ***Autosampling Control System*** to control equipment that obtains and delivers samples to the laboratory and tracks samples during the delivery process.

The ICN also interfaces with other plant control systems including the following:

- Programmable protection system
- Package-supplied programmable control systems
- Process and Mechanical Handling Closed-circuit TV system

These systems are explained below.

The Process Control System (PCJ) is a plant-wide system for monitoring and control of process, ventilation and services within the PTF, HLW vitrification facility, and LAW vitrification facility. This system also interfaces with utilities monitoring, stack & environmental monitoring (radiation and non-radiation), and programmable protection monitoring. Detailed information about the PCJ is provided in, 24590-WTP-3YD-PCJ-00001, Rev 0, *System Description for Process Control System (PCJ).*

The PCJ provides the following functions:

- Device interlocks
- Sequence control of directly controlled batch processes
- Startup, closed-loop control, and monitoring of continuous processes
- Monitoring and some control of electrical services and electrical switchgear
- Monitoring of independent protection trips
- Monitoring indications and alarms from the programmable protection system
- The PCJ also provides initiation of startup, monitoring of status, and initiation of shutdown of independently controlled services and utilities.

The Mechanical Handling Control System (MHJ) is used to control the mechanical handling equipment and packaged systems. Detailed information about the MHJ is provided in, 24590-WTP-3YD-MHJ-00001, Rev 0, *System Description for Mechanical Handling Control System (MHJ).*

The MHJ utilizes a number of operator interfaces for facility control room control, cave face control, or local control, and provides the following functions:

- Sequence control of discrete mechanical handling equipment
- Device interlocks
- Control of process functions integral to the mechanical handling system
- Tracking of canisters and containers
- Control of package-supplied equipment
- Monitoring indications and alarms from the PPJ system

The Autosampling Control System (ASJ) controls the taking and dispatch of samples from the process areas to the laboratory. These activities are managed by the ASJ, which coordinates and tracks the movement of samples. Sample information will be transmitted to the Laboratory Information Management System (LIMS) through the PIN. Detailed information about the ASJ is provided in, 24590-WTP-3YD-ASJ-00001, Rev A, *System Description for Autosampling Control System (ASJ).*

The Programmable Protection System (PPJ) provides independent protection and control of systems, structures, and components determined to be safety design class or safety design significant. This system is designed to operate automatically and transparently without operator intervention to bring process systems to a safe state or maintain a safe state when the normal control systems fail to keep the processes within the safe operations envelope. The PPJ system reports data and status of controls to the PCJ system for logging and operator information. Detailed information for the PPJ may by found in 24590-WTP-3YD-PPJ-00001, Rev 0, *System Description for Programmable Protection System(PPJ)* and 24590-WTP-3PS-JD03-T0002, Rev 1, *Engineering Specification for Programmable Protection System.*

Packaged systems have pre-developed, off-the-shelf, or customized controllers. These independent controllers may either interface with the control system by programmable logic controllers (PLC), or by the ICN, depending on the level of integration with the process. The interfaces are used for the following:

- Supervisory functions required for facilitating remote control
- Feedback to the control system to facilitate remote monitoring
- Interlocking between systems controlling an integrated part of the process
- Feedback for system diagnostics and health status

The Process and Mechanical Handling Closed-circuit TV System (PTJ) provides a means of remotely viewing and monitoring the process areas where hazardous conditions make hands-on process monitoring and inspection impossible. The PJT system also serves as a supplement to cave-face windows and mechanical handling tools. For more detailed information see, 24590-WTP-3YD-PTJ-00001, Rev. 0, *System Description for Process and Mechanical Handling CCTV System (PTJ).*

Basic Process Control System and Safety Instrumented Systems

The systems that comprise the ICN are considered to be the normal control systems for the WTP in the sense of normal, usual, or routine plant operations. The normal control system is also referred to as the Basic Process Control system. Plant controls for non-normal (non-basic) operations are typically governed by safety instrumented systems (SIS). An SIS is a system comprised of safety structures, systems, and components (SSCs) consisting of field sensors, a programmable protection system controller (like a PLC) or hardwired logic, and final control field elements (valves, actuators, etc.) that share logic to serve aggregate safety functions. See Figure 2. The PPJ is comprised of the SISs, which are identified and defined through BNI's Integrated Safety Management (ISM) process and in accordance with ANSI/ISA-84.01, *Application of Safety Instrumented Systems for the Process Industries*.

Figure 3 provides a high-level depiction of how the normal control system and the SISs interface within the WTP network layers. The dashed line between the normal control systems and the SISs is intended to represent the fact that SISs operate independently from the normal control system operations in order to ensure that the safety integrity of the WTP is not compromised.

Basic System Architecture

As also shown in Figure 3, the ICN directly interfaces with the WTP field network layer. Field networks allow process control to be distributed to plant systems and equipment that are in locations remote from the WTP facility control rooms (FCRs). Field networks directly interface with the automated components of the plant systems and may include sensors, final control elements (valves, actuators, etc.), packaged systems, and motor control centers. A significant benefit of field networks is that they result in less construction and field testing time primarily due to reduced field wiring.

The ICN and the field networks comprise the WTP control system architecture. Each facility has control via the ICN, over its facility-specific plant systems extending to the field networks. A basic architectural scheme is shown in Figure 4. The main hardware components within the ICN include (but are not limited to) operator or engineering workstations/control consoles referred to as Human Machine Interfaces (HMI), various system servers to handle network traffic and data processing, local operator interfaces (LOI) to operate and monitor the control system at locations other than in the control room, and plant system controllers.

The ICN encompasses three main areas of control distribution; PTF, HLW, and LAW. BOF and the LAB are considered part of the PTF in terms of monitoring and control. All three areas are interconnected by means of the FNI. Therefore, each facility has its unique portion of the WTP ICN in terms of dedicated PCJ, MHJ, and ASJ system elements. Each of the three facility areas has a dedicated control room. PTF has the plant's main control room (MCR) where, in addition to PTF control functions, HLW and LAW facilities may be monitored and controlled when their respective control rooms must be evacuated.

While most of the ICN equipment will reside in or near the respective facility control rooms, the controllers will be distributed throughout each of the plants. Figure 5 shows an expanded version of the basic ICN architecture according to facility/control area. The numbers in the figure represent the number of controllers distributed throughout the given facility. Since most of these controllers will be redundant, the controller count actually will be about double the numbers shown. Appendix B provides listings of controller assignments according to facility. Each controller is associated with at least one plant system and in most cases several plant systems are assigned to a controller.

More detailed architectural diagrams of the ICN are provided in drawings:

24590-PTF-JJ-PCJ-00001001
24590-PTF-JJ-PCJ-00001002
24590-HLW-JJ-PCJ-00001
24590-LAW-JJ-PCJ-00001
24590-BOF-JJ-PCJ-00001

A block diagram of the FNI (FNJ) may also be found in diagram:

Specific ICN Features

The specification for the ICN is contained in 24590-WTP-3PS-JD01-T0001, Rev 2, *Engineering Specification for Plant Wide Control Systems (Integrated Control Network).* This document is current as of April 2003 and includes general and specific ICN design requirements as well as requirements specific to the PCJ, MHJ, and ACJ systems.

Based on requirements from the ICN specification, a few of the higher-level general functions and features are provided below.

- The control system will be based on an "open" architecture. This means the system will have inherent capability to integrate and exchange information with other brand system devices and platforms. The system is essentially 'open' to a multitude of competing vendors via industry approved open systems communication standards and protocols.

- The control system architecture will allow each plant system to operate independently of all other plant systems, to the extent possible, and maintain redundancy for each plant system at the plant level.

- For functions that require high availability, the system will provide automatic switchover to a secondary system or provide an alternate means of acquiring required data or performing required functions so there is no loss of control or data.

- Where multiple communications systems are utilized, failure on one system will not cause failure or adversely affect any other system. That is, protection or redundancy will be provided to prevent the failure of a device or communication system from preventing communication to other devices or other communication systems.

- Due to the 40-year life expectancy of the WTP, the ICN control system will allow for phased upgrades to ensure the control system is operating on non-obsolete technology. Any system upgrades will be complete within no more than 8 hours of down-time to plant operations.

- The control system is expected to meet an availability target of 99.98% for each process unit.

  A process unit is defined as a collection of associated control modules and/or equipment modules and other process equipment in which one or more major processing activities can be conducted.

  Availability = MTBF/ (MTBF+MTTR)

  MTBF = Mean Time Between Failure and is a measure of system reliability, targeted for 17,500 hours for each process unit.

  MTTR = Mean Time To Repair (diagnose and repair faults) and is targeted for 4 hours for each process unit.

A failure is defined as any event that halts and prevents an operation from continuing under automatic mode control.

- The control system is required to maintain its reliability/availability targets for a commissioning period lasting 2-4 years and a production period of at least 10 years out of the 40-year designed plant life.

- The ICN hardware provider will fully support the hardware platform providing components that are form, fit, and function replacements for any failed or replaced equipment. The ICN hardware provider will give written notification at least seven years in advance of discontinuing any of the supplied hardware components.

- ICN communications will operate at a minimum data transmission rate of 100 Mbit/sec. over an Ethernet complaint communications network. This rate of response will accommodate most operator actions or requests to occur in less than 1 second from the time of operator initiation. The system will also be designed so that data communication to the PIN does not affect system response times.

Controllers and Plant Interfaces

The ICN interfaces with plant systems and equipment mainly via the controllers. The features that the ICN controllers will have include the following.

- Controllers will have power supplies, I/O modules, memory, communications hardware, and central processors.

- Redundant controllers will be “hot swappable” and will automatically fail-over to the backup or standby controller without loss of data. Transfers will be bumpless, and controllers that are replaced will automatically synchronize with the master upon installation.

Hot swappable means the component can be changed out without turning off power or impacting the operation of the system.

- Controller programming and monitoring will be accomplished by fixed workstations or portable computers over the Ethernet network.

- Controllers will retain their configuration settings for at least 30 days with no power applied.

Controllers will interface with plant system field devices via field networks. A typical field network arrangement might look as shown in Figure 6. The basic types of interfaces to plant equipment include:

- Remote I/O (Input/Output)
- Foundation Fieldbus
- Discrete bus (Profibus DP)
- Serial communication

Remote I/O refers to the equipment that allows for the handling of analog and discrete signals to and from field equipment and instruments. I/O is usually a rack of electronic modules that provide signal conditioning and or transformation, as well as isolation against high voltage transients that could damage or interfere with logic circuitry. Remote I/O will be located close to the field instruments and will include communication links and “smart” or “intelligent” I/O cards that directly interface with the controllers. I/O modules will be of the plug-in type and will be “hot swappable”.

A smart or intelligent device means the component has a microprocessor and communication capability.

Fieldbuses

A fieldbus is a digital, serial, data bus for communication with low level industrial control and instrumentation devices such as transducers, actuators, and local controllers. Fieldbuses allow essentially Local Area Networks (LANs) to be arranged at the field device level, hence, the term field networks. Fieldbus technology is based on an approach in which, the intelligence needed for device profiling and simple regulatory and (in some cases) discrete control is embedded into the primary sensing devices (sensors, transmitters, etc.) and actuating devices (valves, actuators, etc.). This eliminates the need for the plant distributed control system to perform routine process and discrete control.

Fieldbus technologies came about as open systems communication standards were developed, which led to open fieldbus standards. The primary benefits for an open fieldbus standard for intelligent field devices include the following.

- It accommodates obtaining multiple measurements that are communicated in a time-multiplexed manner over a digital transmission line, thereby providing more information at a reduced cost.

- It allows the ability to obtain more information regarding the field device at the source, thereby eliminating middleware that might pose ongoing maintenance problems.

- It reduces or eliminates I/O modules and/or controllers.

- Reduces wiring costs due to the multidrop nature of a serial fieldbus and the multiplexed nature of digital transmission. In other words, several fieldbus devices may be connected to the same two wires.

- The ability to obtain intelligent devices from many vendors, thereby ensuring a wider selection choice and competitive pricing.

There is a diversity of fieldbus technologies each having their own particular features. The WTP will utilize two of the most popular fieldbus technologies, *Foundation Fieldbus* and *Profibus DP*. Utilization of these two types of fieldbuses provides extensive market flexibility for instrument selection.

Foundation Fieldbus (FFB) is a serial two-way digital communications specification used to interconnect field-based intelligent devices such as sensors, actuators, and controllers in accordance with specific industry standards. It is designed specifically to meet the stringent, mission-critical demands for intrinsic safety and use in hazardous areas, volatile processes, and difficult regulatory environments. FFB is an open technology; hence diverse vendors can purchase the necessary electronics (chips, etc.) needed to manufacture FFB products. Thus, FFB capability can be easily specified in applicable instrument or equipment purchases.

Profibus (process field bus) like FFB is an international, vendor-independent, open fieldbus standard. Unlike FFB, it is designed for a wide range of applications, including discrete manufacturing, process control, and building automation. Profibus is a serial fieldbus system that supports the networking of intelligent field devices. Profibus DP* is optimized for high speed and inexpensive hookup and is designed especially for communication between automation control systems and distributed I/O at the device level. For the WTP, Profibus DP will be utilized as the standard communication interface for such devices as intelligent motor control centers and is the preferred device level bus where FF is not available or appropriate for discrete signals.

* The DP suffix refers to "Decentralized Periphery", which is used to describe distributed I/O devices connected via a fast serial data link with a central controller. To contrast, a PLC normally has its input/output channels arranged centrally. By introducing a network bus between the main controller (master) and its I/O channels (slaves), the I/O is decentralized.

Specific technical differences between these two fieldbus technologies are provided in Appendix D.

Since these technologies are based upon open standards, the WTP control system design at the field component level is highly adaptable to market changes and trends.

Serial Communication will be utilized between ICN controllers and specialty equipment or packaged systems not needing to share resources via a fieldbus configuration. Serial communications (bit streams, versus parallel multi-bit data lines) is also based upon industry standards and protocols, a common standard being RS232.

OPC

Another fieldbus standard that will be used within the ICN is referred to as OPC, which stands for OLE for Process Control. OPC is the application of OLE (See Terms and Definitions) technology to process controls. It is intended to foster greater interoperability between automation/control applications, field systems/devices, and business/office applications in the process control industry. OPC defines standard objects, methods, and properties, for servers of real-time information such as distributed process systems, programmable logic controllers, smart field devices, and analyzers in order to communicate the information that such servers contain to field devices compliant with OLE technologies.

Network Connectivity

The ICN network and field network elements will be interconnected in the following ways.

- Controllers will be interconnected with other controllers
- Controllers will be interconnected with field components (via fieldbuses, etc.)
- Controllers will be interconnected to servers
- Foundation Fieldbus devices will be interconnected to OPC servers
- Packaged systems will be directly connected to the ICN or OPC servers

General Design Philosophy

The general design philosophy for the WTP control systems is contained in 24590-WTP-GPC-J-014 Rev B, *Control System Design Process Guide.* The control and instrumentation design is based on guiding principles intended to support constructability, maintainability, and operability objectives. This philosophy will be implemented as follows.

Instruments will be located on racks or enclosures in the field. Remote I/O, fieldbus technology, and device level buses are used with the racks and enclosures to get measurements and control actions into or out of the ICN. Valve racks, utility racks, fluidic control racks, instrument enclosures, motor control centers, adjustable speed drives, switchboards, and switchgear are designed with remote I/O, fieldbus, or device level bus technology. The racks and enclosures are fabricated off site using selected vendors to detail the design, fabricate the racks, mount all instruments, tube and wire instrument components, install the I/O systems, and test the rack or enclosure.

Packaged systems procurements provide standard controllers, remote I/O, and standard instrumentation to the extent practicable. **Testing of these systems at the vendor's shop prior to site delivery will greatly facilitate acceptance tests, site installation, construction testing, and commissioning.**

The ABB System

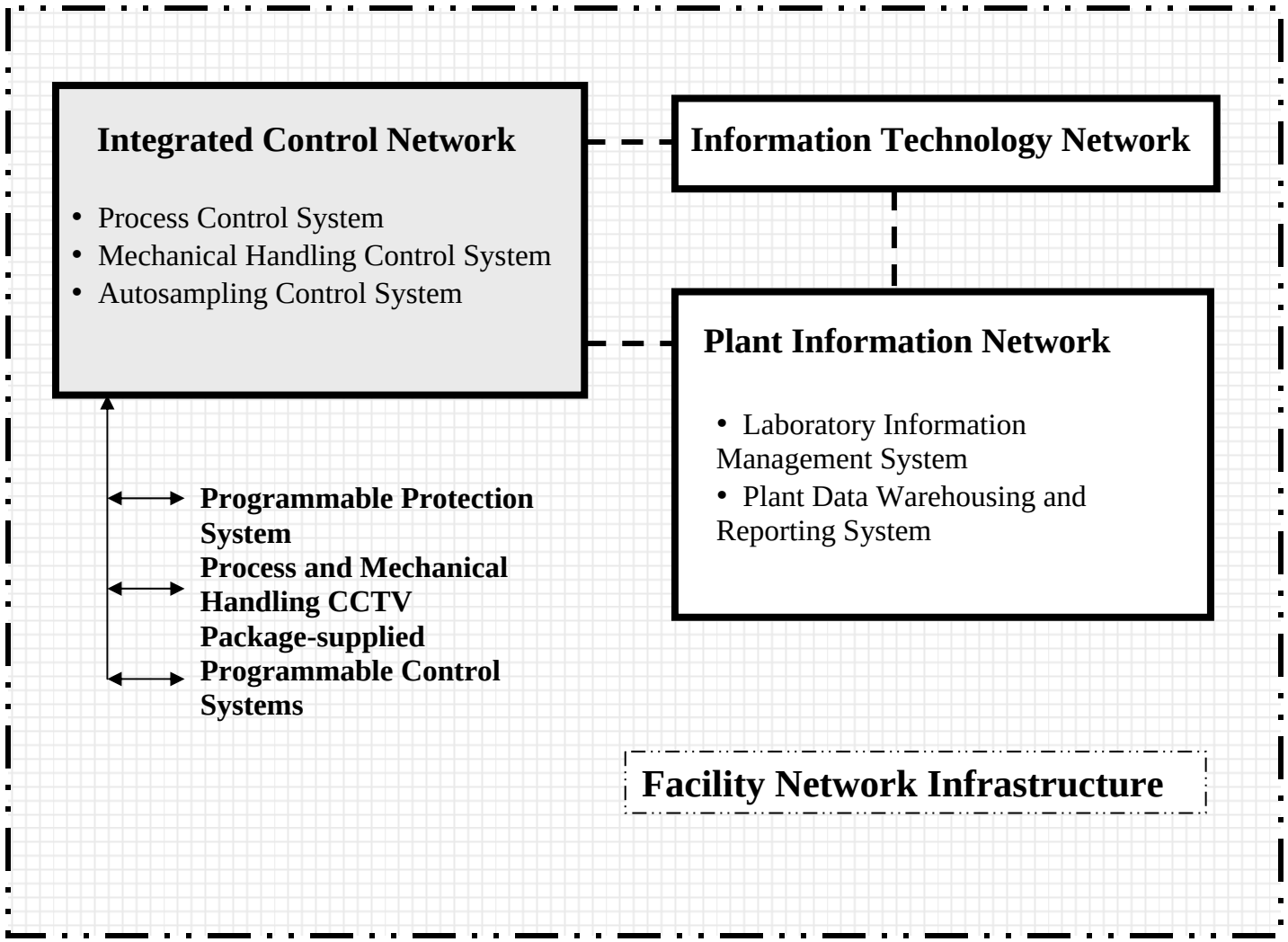
In November 2001, BNI awarded the contract for ICN development to ABB. Since that time there has been an ongoing collaborative work effort between ABB and BNI for system definition, software development, training, and coordination.

The ABB ICN architecture is shown in Figure 7. ICN system development is based upon a plant control configuration defined in ABB's ***Industrial^{IT} Integrated Automation Solutions for Process Automation based on Aspect Object Technology, System Guide.*** Aspect Object architecture is explained in Appendix E, which includes pages extracted from the ABB system guide. The system described in this guide generally appears to meet the requirements defined in the *Engineering Specification for Plant Wide Control Systems (Integrated Control Network)* and its installation to-date appears to be consistent with the *Control System Design Process Guide.*

At the heart of the ABB configuration is the AC800M process controller and associated hardware components. Figure 8 shows the AC800M controller with a functional overlay. A general hardware arrangement is shown in Figure 9. And Figure 10 shows the ABB controller and associated hardware in terms of a redundant configuration. Lastly, Figure 11 shows an actual controller cabinet with the various (redundant) ABB system hardware components. Cabinets

similar to this one will be assigned to each of the WTP process systems. As of November 2004, controller cabinets have been placed in the following WTP locations.

Building 87, for Non-ITS Switchgear (PCJ-CNTRL-5871)
Building 90, BOF Switchgear (PCJ-CNTRL-5911)
Cooling Tower Electrical Room (PCJ-CNTRL-5831)
NLD Pump House (PCJ-CNTRL-5541)



WTP Network Systems

Figure 1

Fig. 1

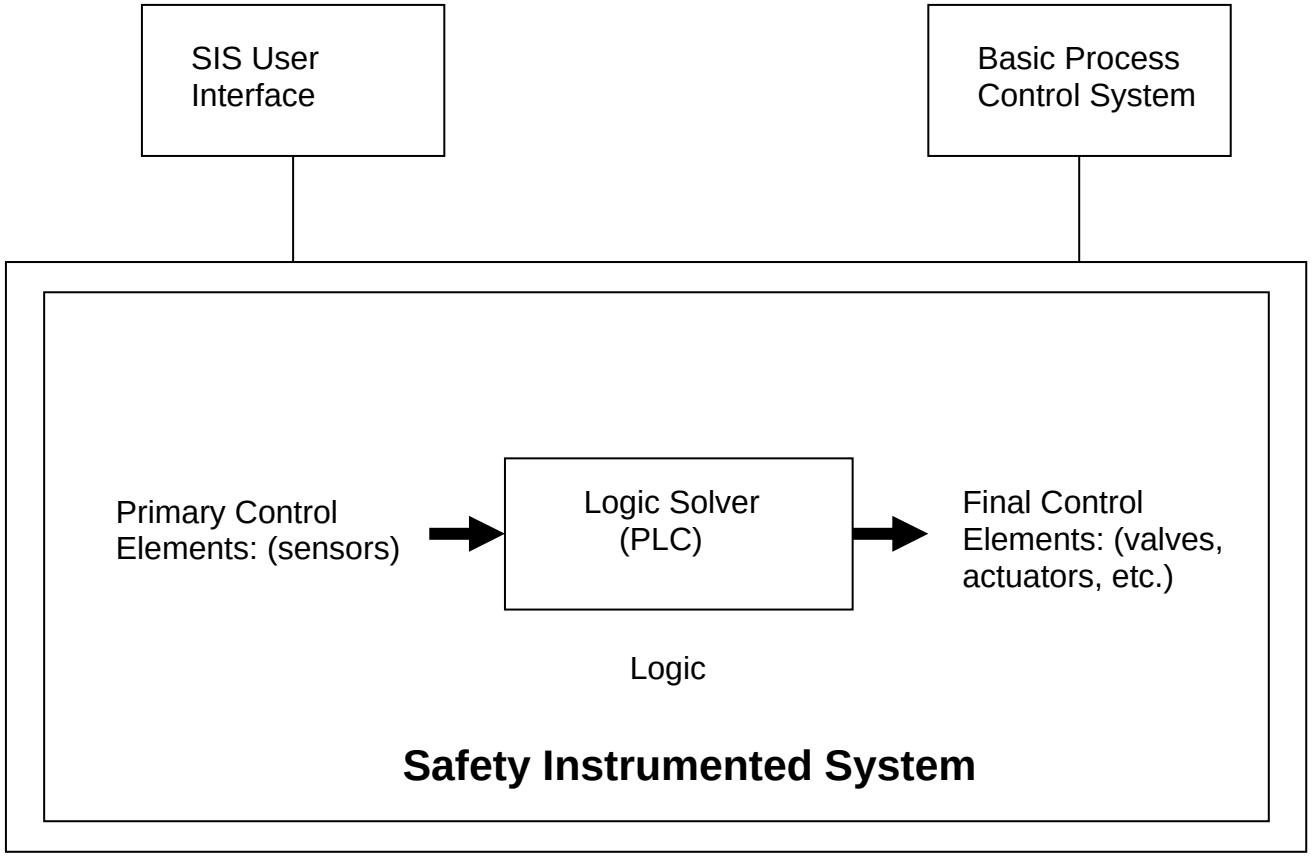


Figure 2

Fig. 2

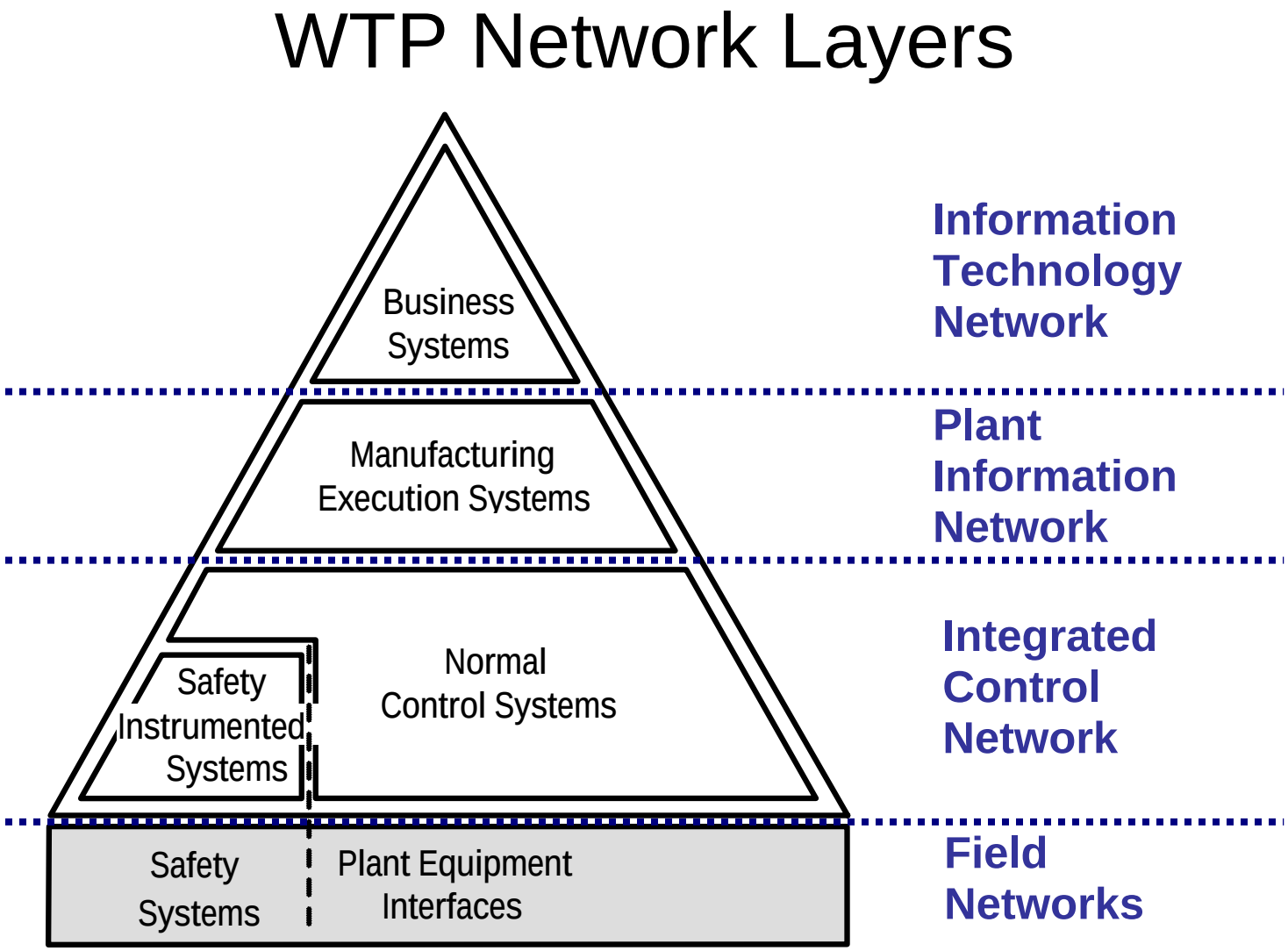


Figure 3

Fig. 3

Basic Control System Architecture

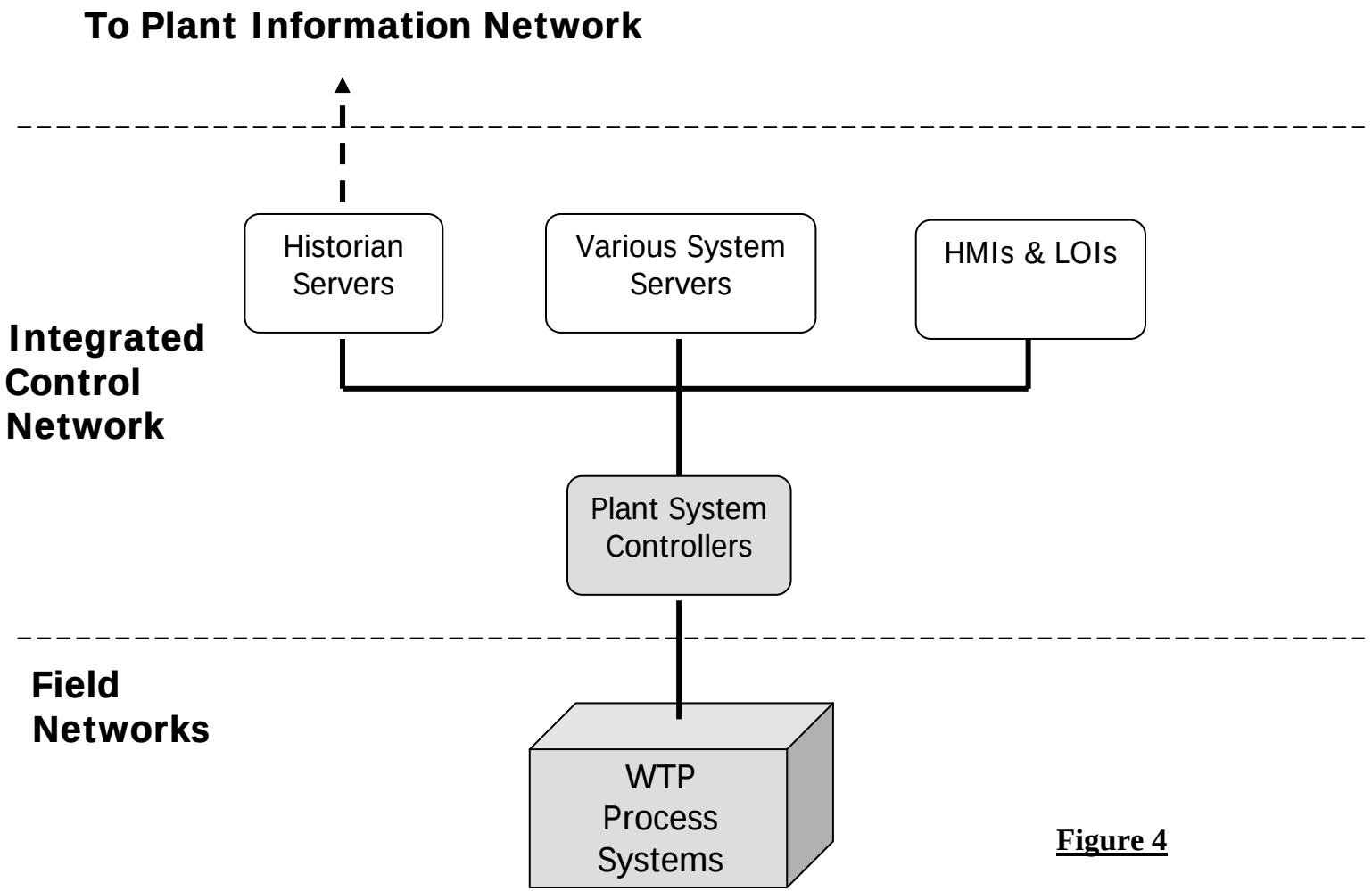


Figure 4

Fig. 4

WTP – Integrated Control Network

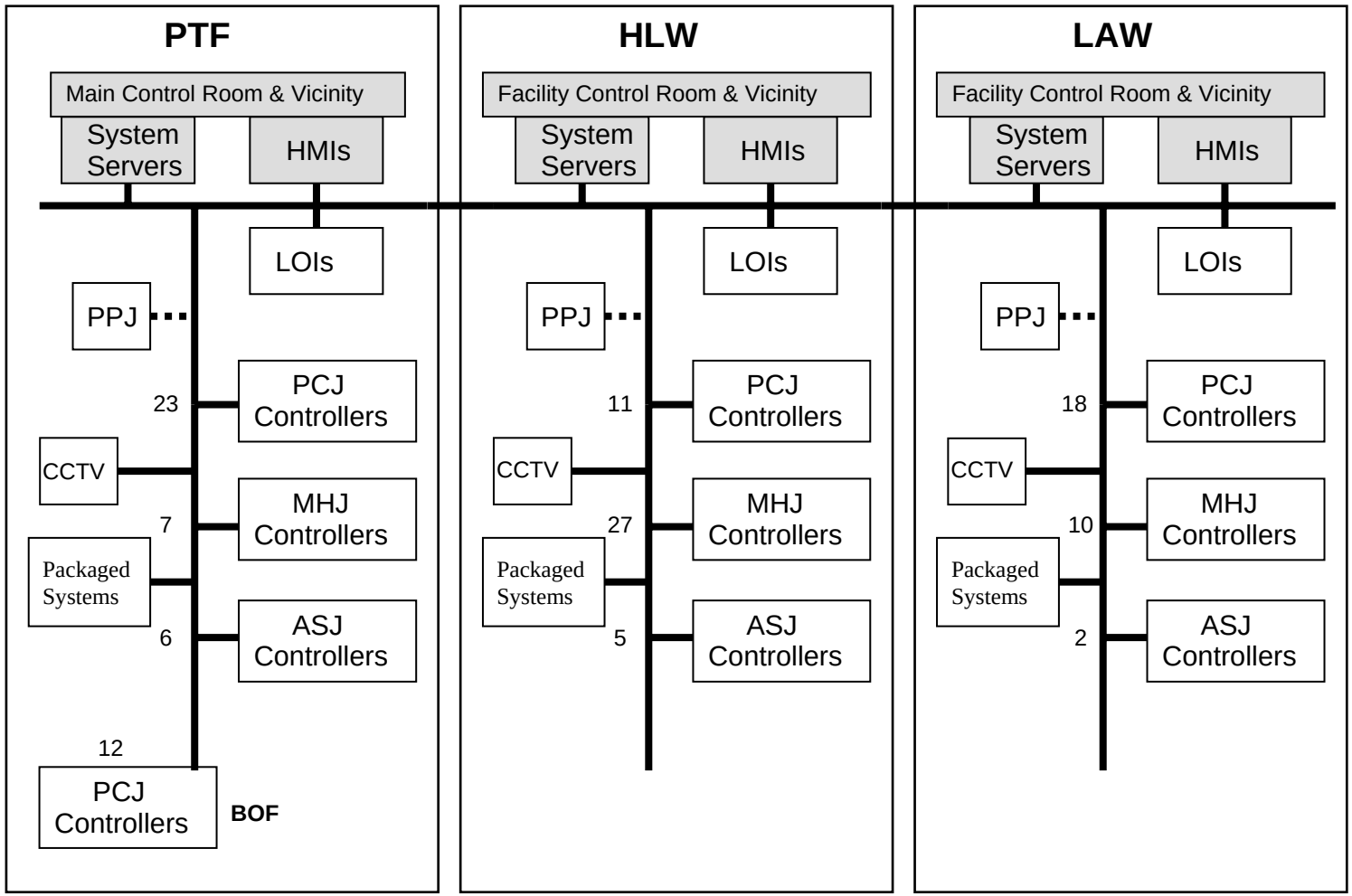


Figure 5

Fig. 5

Typical Field Network Arrangement

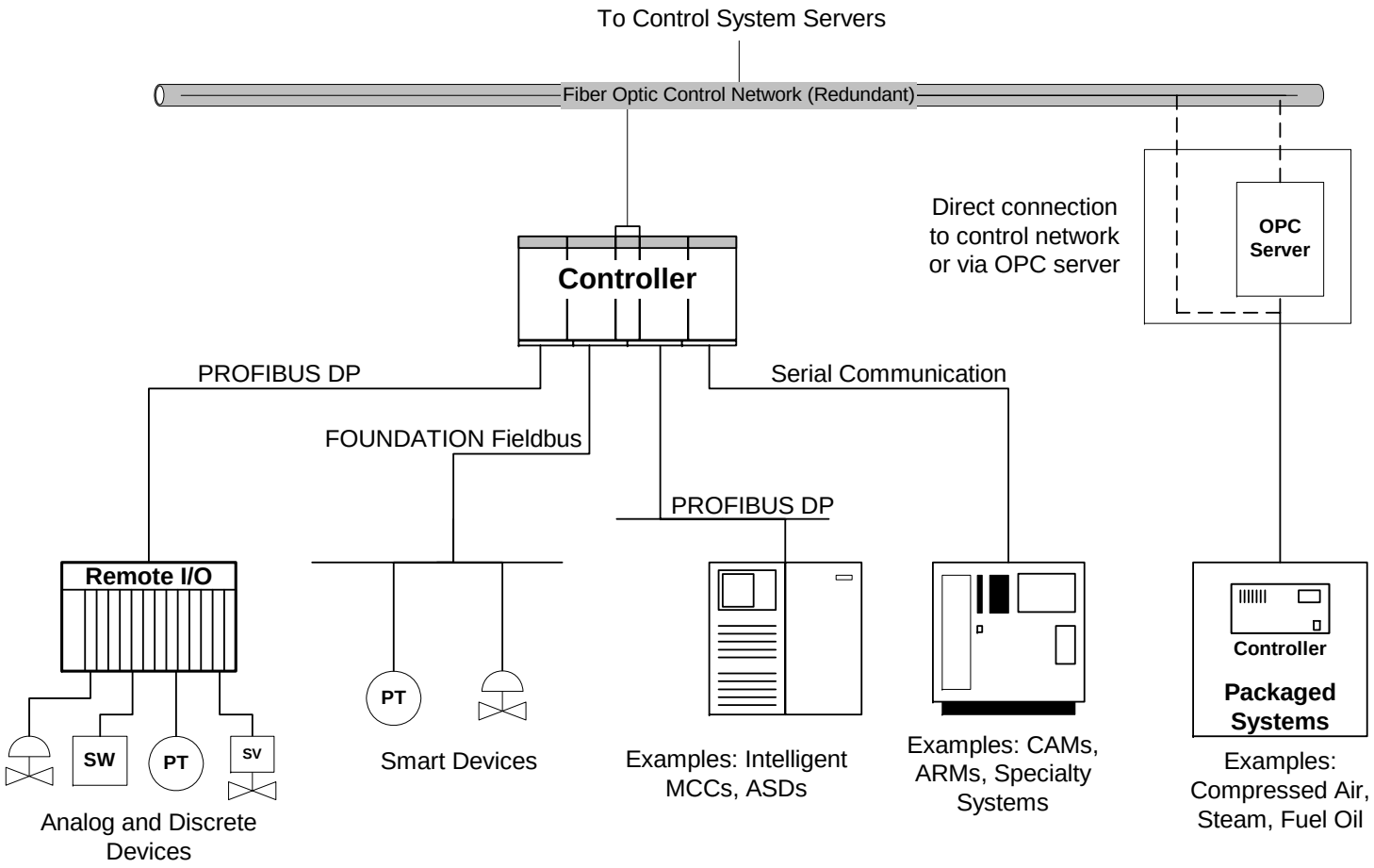


Figure 6

Fig. 6

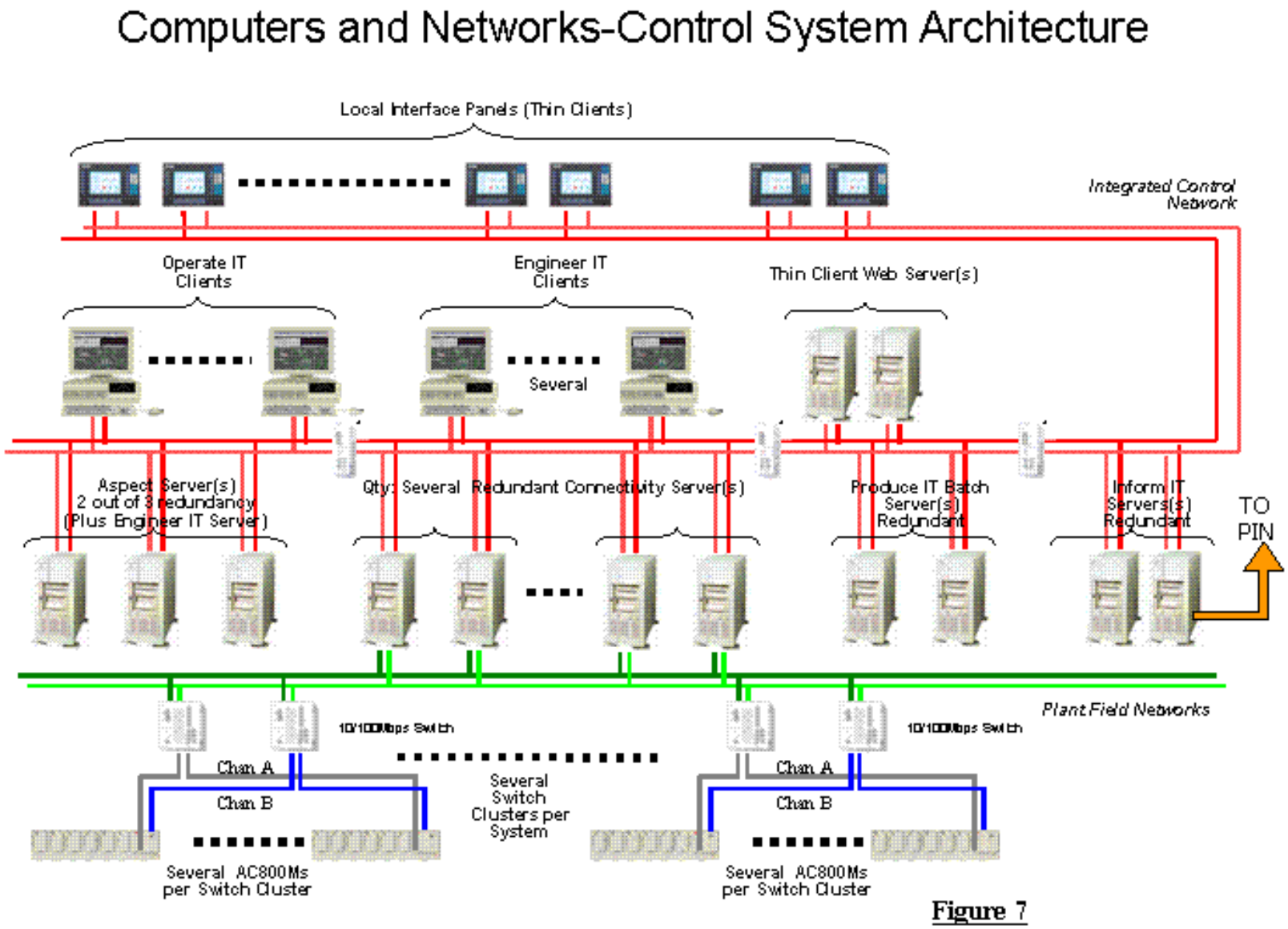

Computers and Networks-Control System Architecture
Local Interface Panels (Thin Clients)
Integrated Control Network
Operate IT Clients
Engineer IT Clients
Thin Client Web Server(s)
Several
Aspect Server(s)
2 out of 3 redundancy
(Plus Engineer IT Server)
Qty: Several Redundant Connectivity Server(s)
Produce IT Batch Server(s) Redundant
Inform IT Servers(s) Redundant
TO PIN
Plant Field Networks
10/100Mbps Switch
10/100Mbps Switch
Chan A
Chan B
Several Switch Clusters per System
Chan A
Chan B
Several AC800Ms per Switch Cluster
Several AC800Ms per Switch Cluster
Figure 7

Fig. 7

AC 800M Process Controller

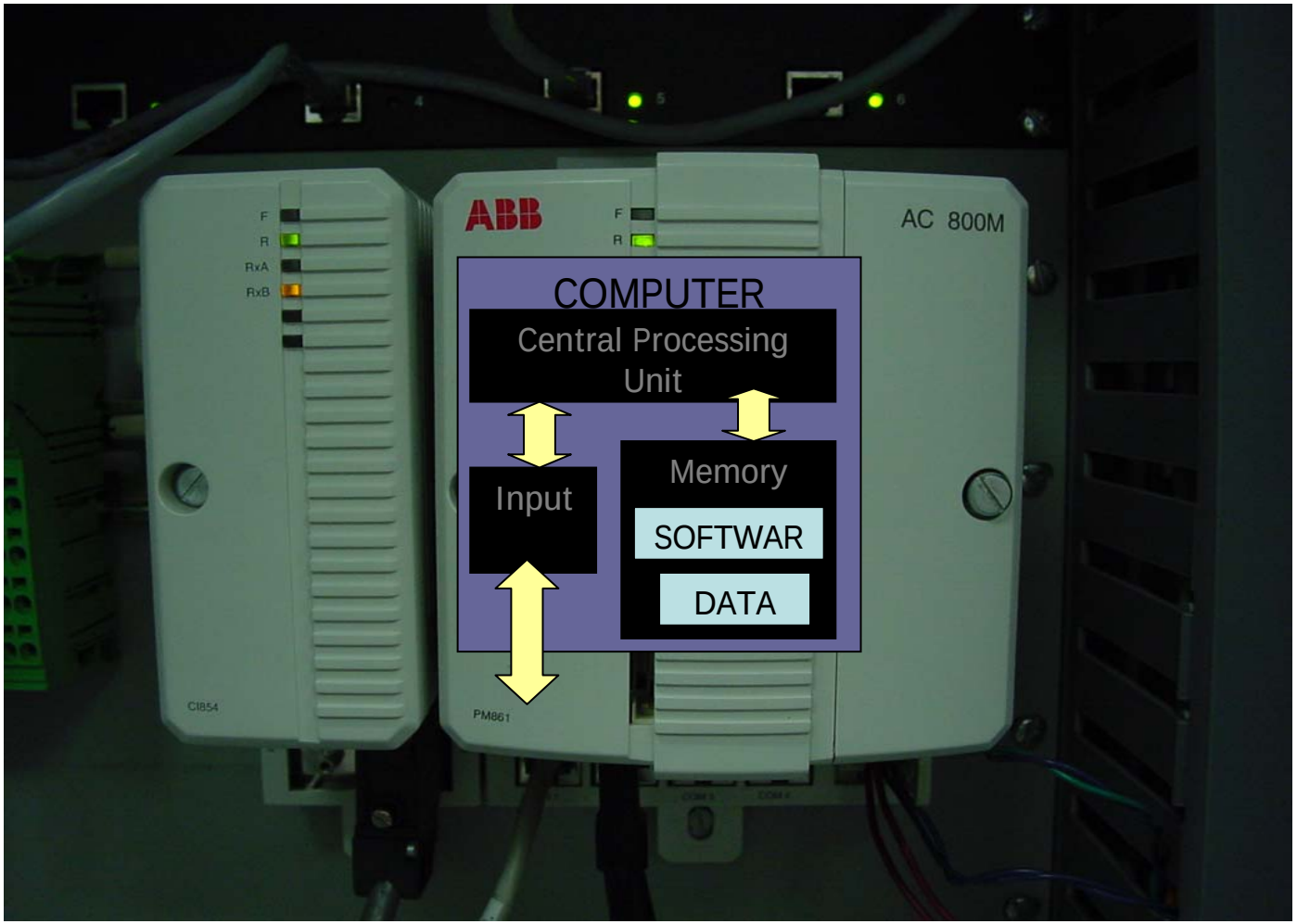


Figure 8

Fig. 8

ABB System General Arrangement

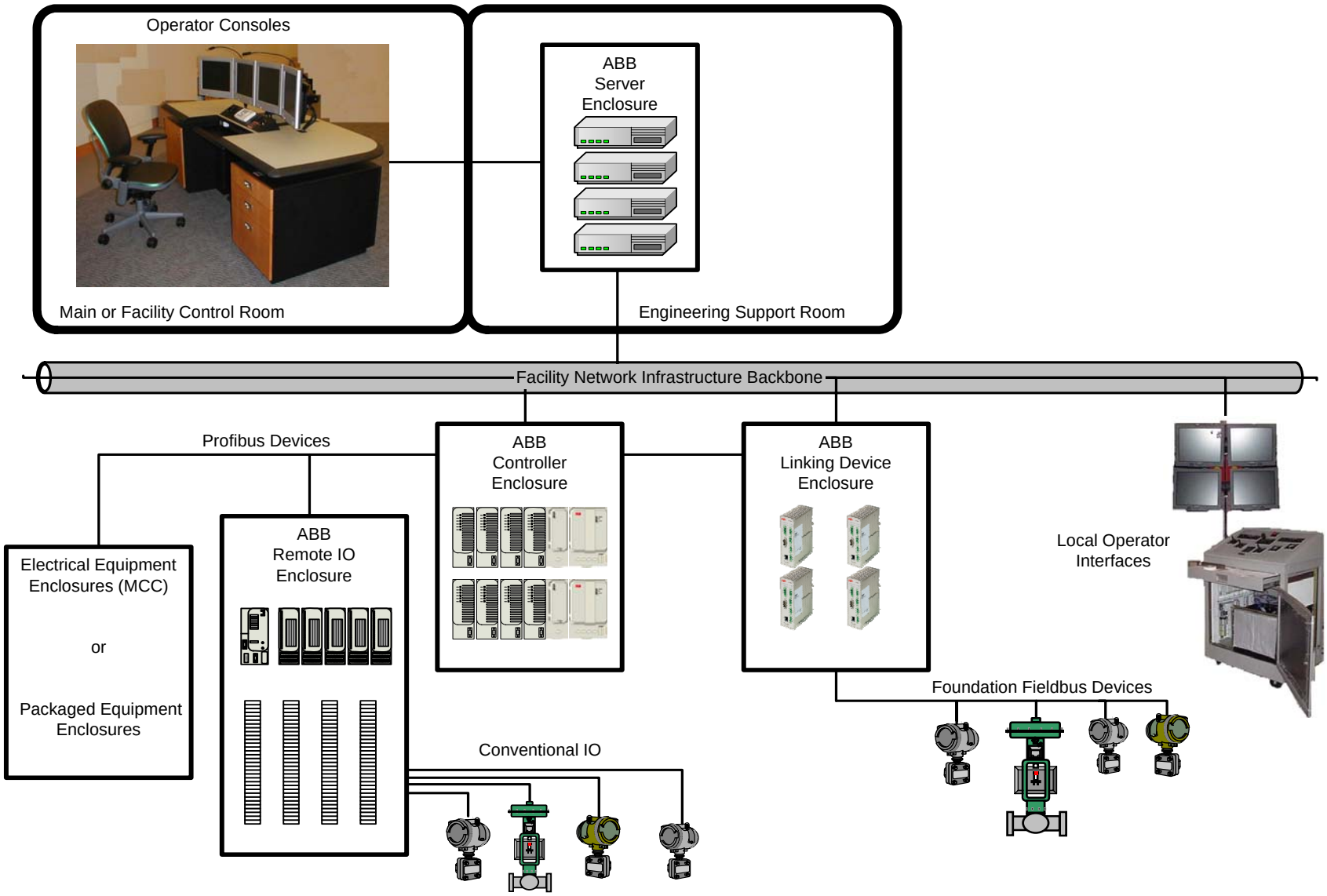


Figure 9

Fig. 9

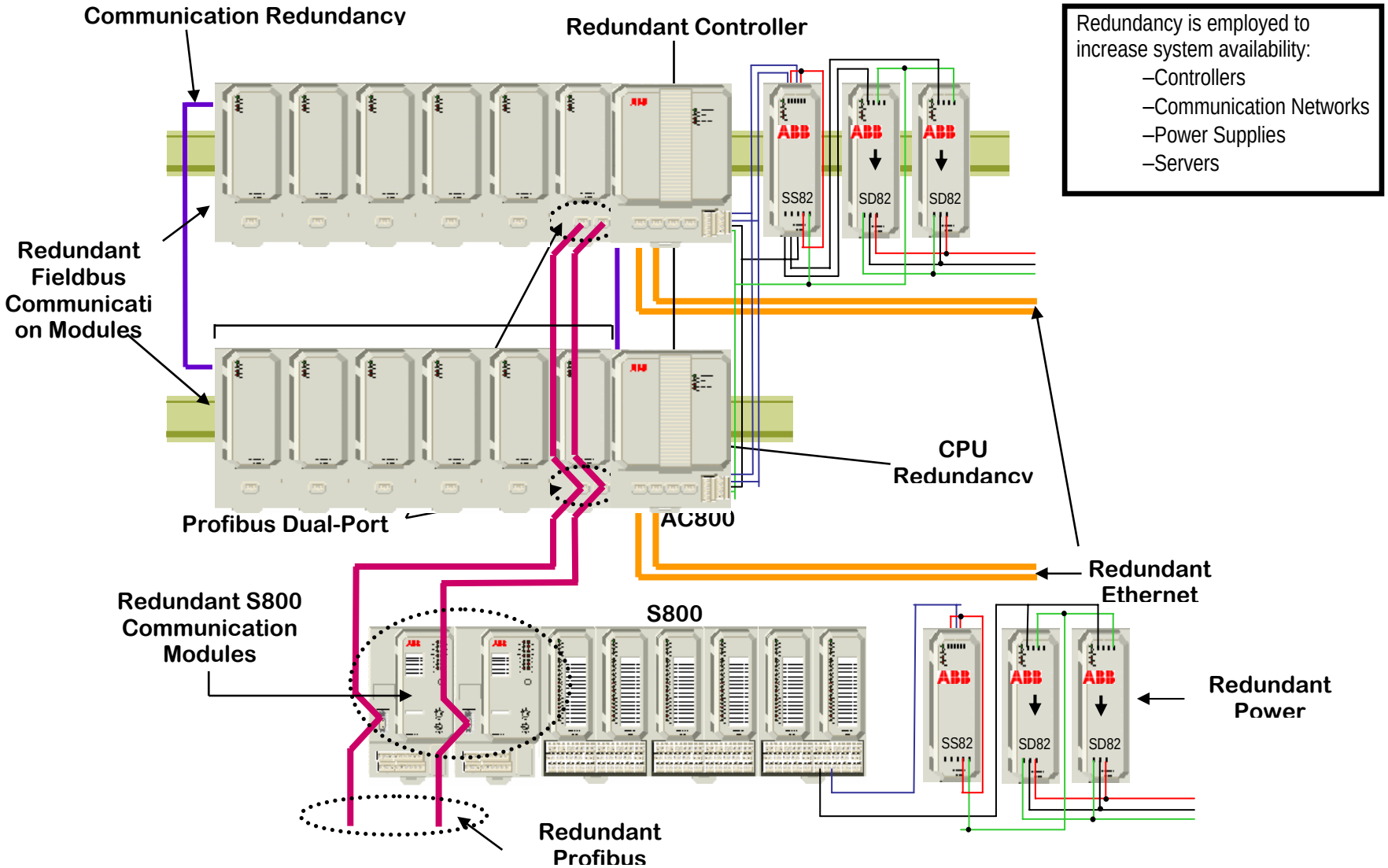


Figure 10

ABB Controller Redundancy

Fig.10

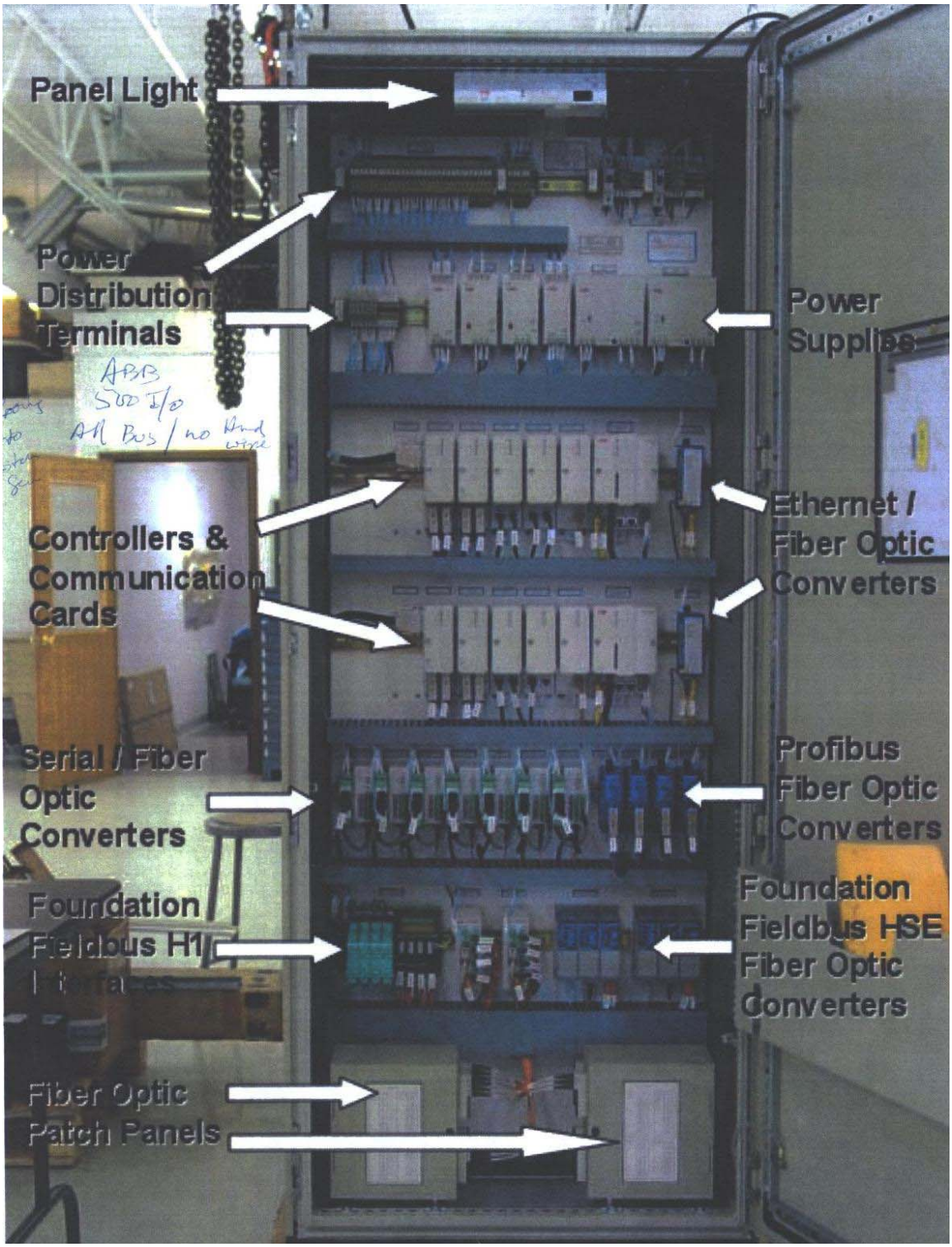

Panel Light
Power Distribution Terminals
Power Supplies
Controllers & Communication Cards
Ethernet / Fiber Optic Converters
Serial / Fiber Optic Converters
Profibus Fiber Optic Converters
Foundation Fieldbus H1
Foundation Fieldbus HSE Fiber Optic Converters
Fiber Optic Patch Panels

Fig. 11

Appendix A – Distributed Control System Features

The size and complexity of modern industrial processing plants require elaborate measures and means for monitoring and controlling a host of various chemical and physical processes. Such control is essential to ensure safe and cost effective plant operations. The current state-of-the-art for control of large complex plants like the WTP is by means of some kind of a Distributed Control System (DCS).

As the name implies, a DCS is an interconnected system of hardware and software components that are remotely located throughout plant processing entities. Distributing the means of control as close as possible to plant equipment is a desired objective in any DCS.

A DCS has three general qualities.

1. Control functions are distributed into small groups of semiautonomous subsystems that are connected by a high-speed communications network. Typical distributed functions are listed below.

    -Data Collection
    -Process Control
    -Presentation of Information
    -Process Analysis and Supervision
    -Information Storage and Retrieval
    -Reporting

2. A DCS accommodates the automation of diverse processes by integrating advanced regulatory control, logic and sequential control, procedural languages, and advanced system application packages. The latter would also include applications intended to meet business and management needs.

3. The DCS organizes and integrates many diverse elements and subsystems such that they exist and operate together as a single unified automated system. Examples of elements and subsystems are:

    -Process signal input and conditioning
    -Process actuator signal outputs
    -Various types of controls (regulatory, sequence, logic, etc.)
    -Readable process displays for process values, alarms, trends, etc.
    -Actions for setpoint changes, manual override and alarm handling
    -Process optimization and production support
    -Information storage systems
    -Communication systems

Appendix B – Controller Assignments

B-2 – HLW Controller Assignment

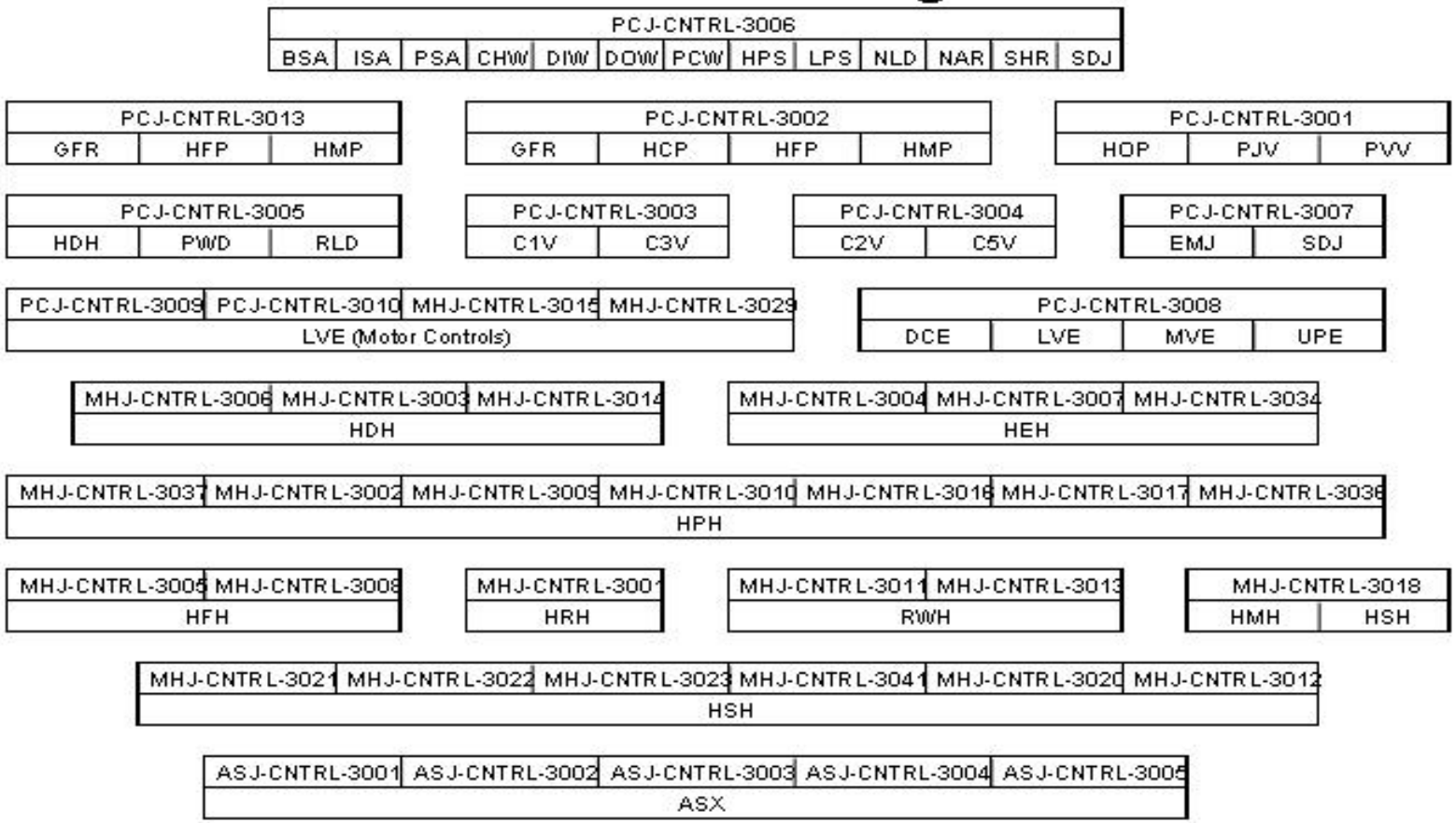
B-3 – LAW Controller Assignment

B-4 – PTF Controller Assignment

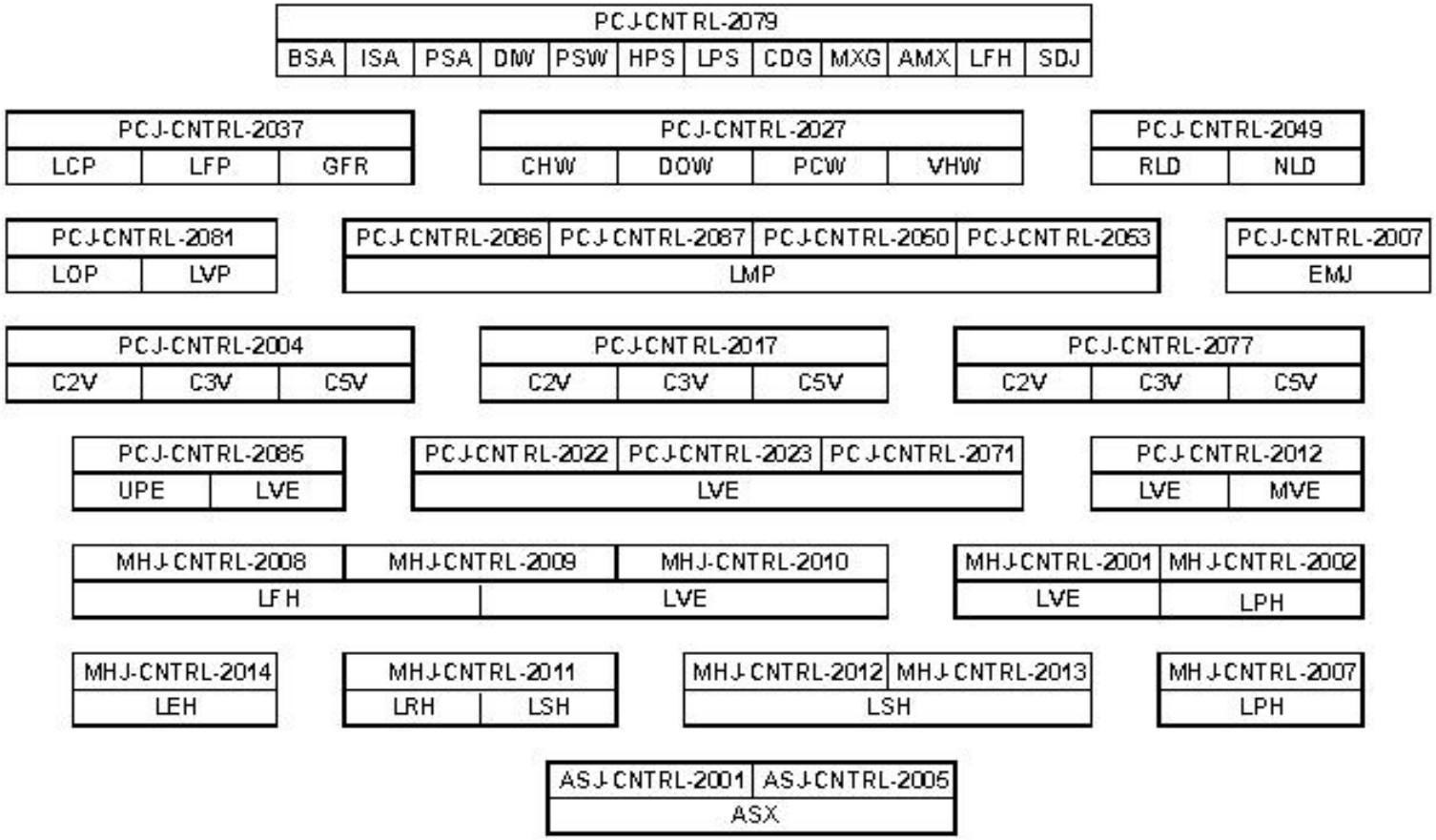
B-5 – BOF Controller Assignment

See 24590-WTP-RPT-ENG-02-009, *System Area Locators List and System Division of Responsibility,* to identify the three-letter system designations.

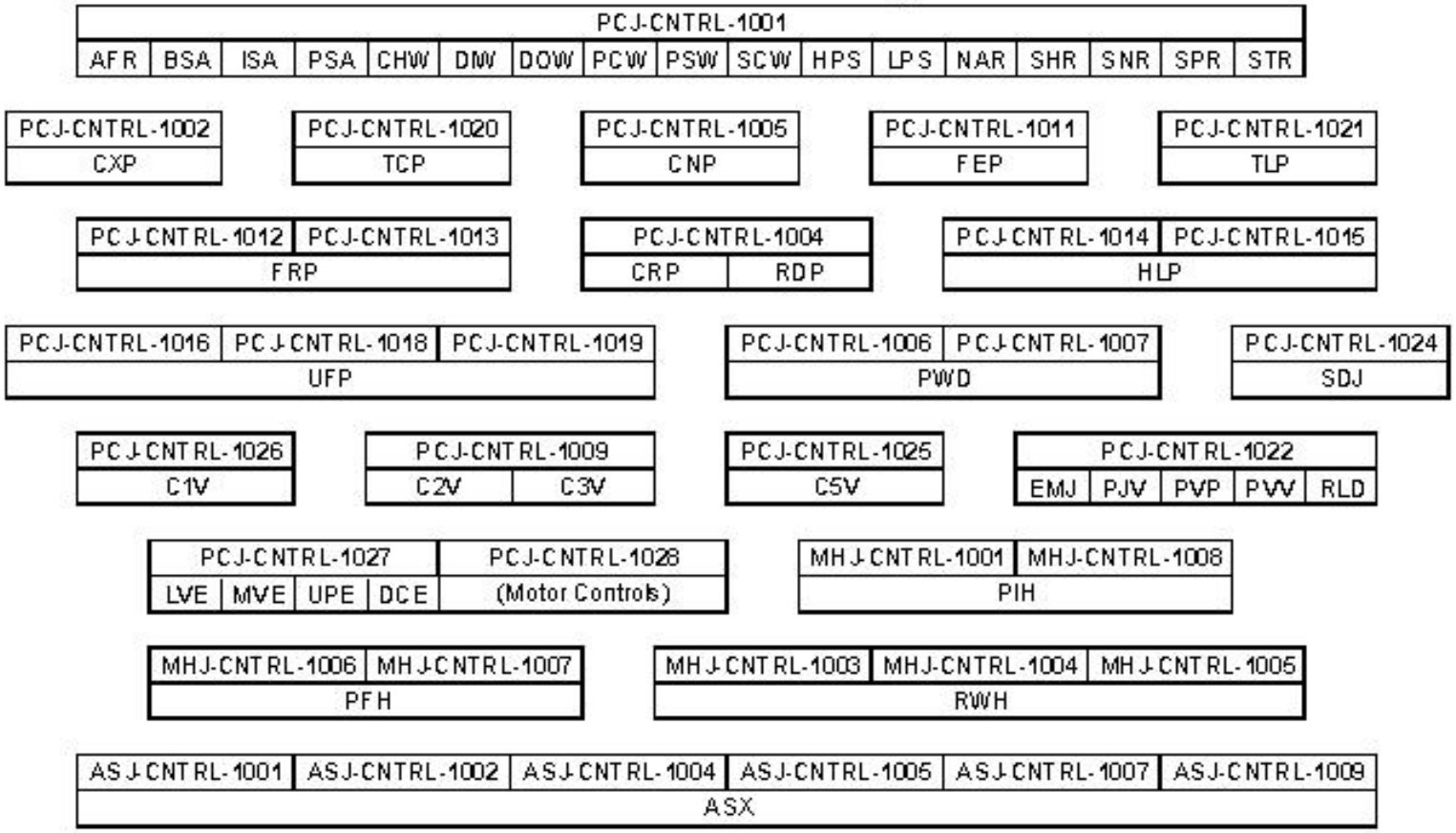
HLW Controller Assignments



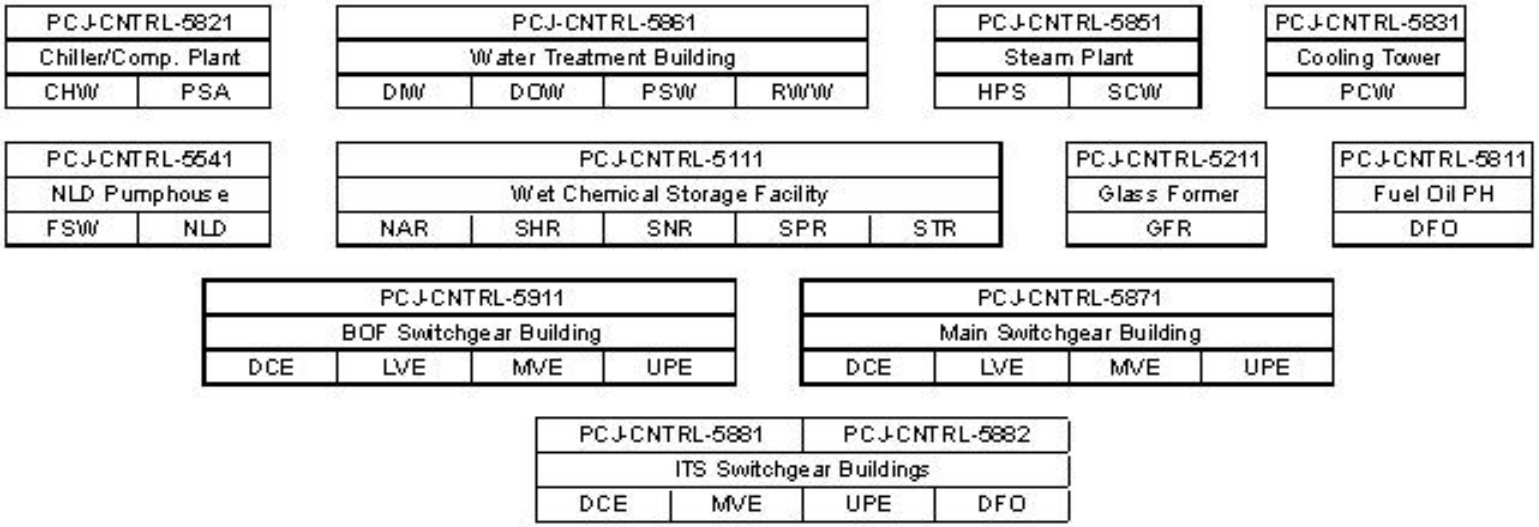
LAW Controller Assignments



PTF Controller Assignments



BOF Controller Assignments



Appendix C

Foundation Fieldbus and Profibus Characteristics

Characteristics	**Profibus DP/PA**	**FOUNDATION Fieldbus**
Technology Developer	Profibus User Organization	Fieldbus Foundation
Year Introduced	DP-1994, PA-1995	1995
Governing Standard	DIN 19245 part 3/4	ISA SP50/IEC TC65
Openness	Products from over 150 vendors	Chips/software from multiple vendors
Network Topology	Line, star & ring	Multidrop with bus powered devices
Physical Media	Twisted-pair or fiber	Twisted –pair
Maximum Devices (nodes)	127 nodes	240/segment, 65,000 segments
Maximum Distance	24Km (fiber)	1900m @ 31.25K or 500m @ 5Mbps
Communication Methods	Master/slave peer to peer	Client/server, publisher/subscriber, event notification
Transmission Properties	DP up to 12 Mbps, PA 31.25Kbps	31.25 Kbps, 1 Mbps, 2.5 Mbps
Data Transfer Size	244 bytes	16.6 M objects/device
Arbitration Method	Token passing	Deterministic centralized scheduler, multiple backup
Error Checking	HD4 CRC	16-bit CRC
Diagnostics	Station, module & channel diagnostics	Remote diagnostics, network monitors, parameter status
Performance: Cycle Time: 256, Discrete 16 nodes with 16 I/Os	Configuration dependent typically <2ms	100 ms @ 31.25K, <2 ms @ 2.5M
Performance: Cycle Time: 128, Analog 16 nodes with 8 I/Os	Configuration dependent typically <2 ms	600 ms @ 31.25K <8 ms @ 2.5M
Block transfer of 128 bytes, 1 node	not available	36 ms @ 31.25K 0.45 ms @ 2.5M

Appendix D – ABB Aspect Object

Section 3 System Topology and Architecture

3.1 Architectural Base - the Aspect Object

The Aspect Object architecture is a cornerstone of the Industrial^{IT} concept. It provides:

- A consistent, scalable, concept that integrates Process Control & Automation, Substation Automation, and Safety products.
- Information centric navigation – a consistent way to instantly access all information without having to know how and by which application the information is handled.
- Vertical integration as well as integration of e-Business in real time.
- Integration of autonomous applications. Very little awareness is required between applications.
- Easy integration of new aspect systems (new applications). A homogeneous base for all applications. Open standards make it possible also for users to integrate new aspect systems.
- High level of engineering efficiency through data integration between aspect systems.
- Extensive re-use during the life cycle. Copy/paste, definition of object types and solutions, etc.

A central problem in plant operations, as well as asset life cycle management. is the need to organize, manage, and have access to information for all different aspects of a great number of plant and process entities. These entities, or real world objects, are of many different kinds. They can be physical process objects, like a valve, or more complex, like a reactor. Other examples are products, material, batches, manufacturing orders, and customer accounts.

Each of these real world objects can be described from several different perspectives. Each perspective defines a piece of information, and a set of functions to create, access, and manipulate this information. We call this an *aspect* of the object.

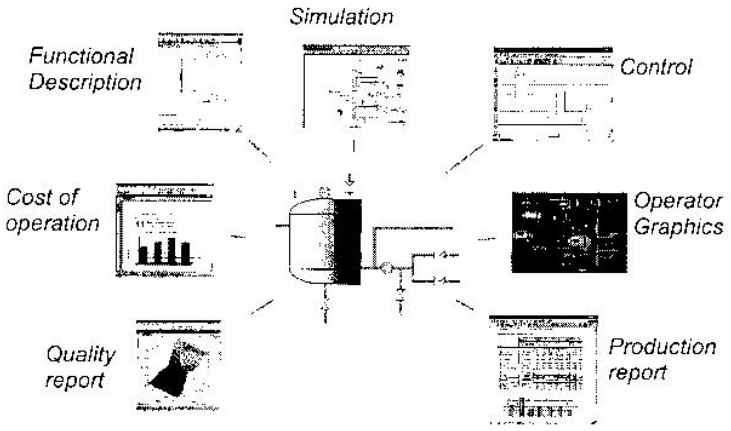


Figure 3-1. Examples of Different Aspects of an Object

3.1.1 Aspect Objects

It is necessary to be able to implement these aspects using many different applications, existing and new, from ABB, third parties and customers, both now and in the future. It is desirable to be able to do this without changes to the applications. It is not reasonable to require that all these different applications are aware of each other. Still, the applications must cooperate to provide an integrated view and functionality of the object.

Aspect Objects provide a solution to this problem. In this concept, rather than creating one single object or data model in the system to represent the real world object, each aspect is modeled separately. An Aspect Object is thus not an object in a strict sense, e.g. like a COM object, but rather a container of references to implementations of the different aspects.

3.1.2 The *Aspect Object Architecture*

The *Aspect Object architecture* defines a platform, which provides basic system functionality, and a framework, the Aspect Framework (Afw), for integration of various applications and connectivity components.

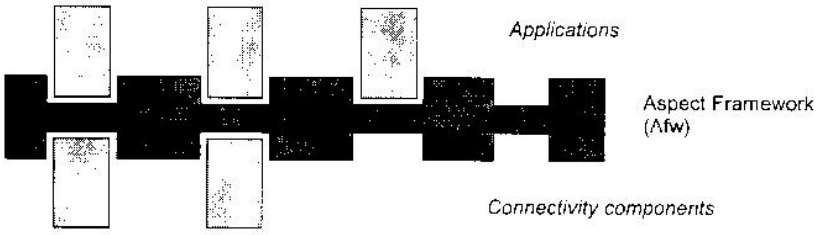


Figure 3-2. The Afw Aspect Framework

Connectivity components provide access to real time data, historical data, and/or alarm and event data from different types of controllers and devices.

Applications provide functionality to the system. They are implemented as services or client applications. The same application can act both as a service and as a client.

A service is an entity that provides a certain set of functions in the system. Services run in a server. A service manager initiates and supervises the execution of services.

Client applications are applications that utilize the functionality provided by one or more service, e.g. to present some information to a user. A client application can also support thin clients by providing an interface to an Internet Information Server.

A central feature of Industrial^{IT} is that information and functions are centered on Aspect Objects. To participate in Aspect Object operations, an application must present itself as an aspect system (or possibly as several aspect systems). In essence this means that the application provides COM objects called aspect system objects, which support certain framework defined interfaces, through which the application can initiate and participate in common operations on objects and aspects.

3.1.3 Aspect Integrator Platform

The Aspect Integrator Platform (AIP) is the base for many Industrial^{IT} products, and provides the following types of functionality:

- Basic platform functions
  Security, Installation, License Management, NLS, Event Logging, Error handling, Aspect Object management, Name services, Workplace management, OPC services,...
- Optional product functions
  Dynamic Graphics, Alarm and Event Handling, History collection and presentation, System Status

The Aspect Integrator Platform is a product in itself, although not directly "visible" to the user of standard software products. The platform is an integral part of the product, and relevant parts of it are installed at product installation.

The AIP is also provided as a platform product including development tools, across ABB and outside ABB, to build and integrate Aspect Systems.

3.1.4 Aspect Systems

Aspect systems provide the functionality that is defined for Aspect Objects; examples are Control, Process graphics, Alarm & Event, History, Reports, Simulation, Asset Optimization, Material Tracking, Production Scheduling.

Adding functionality to the workplace and server level, mainly involves adding new aspect types and aspect categories to existing aspect systems, or, when required, by adding new aspect systems. An aspect system may provide one or more user interfaces, implemented as an ActiveX, ASP/HTML page, Active Document, OLE Server, or Windows application.

Aspect systems can be more or less well integrated into the system depending on what function they provide, who supplies them, etc. To easily describe how an aspect system is integrated, different integration levels are defined. Core functions of the automation system, such as Operator Graphics, Historian, Engineering Tools, etc. have a high level of integration.

Attachment 2:

June 2003 Report

OPR Oversight Record of the BNI Bi-Monthly Design Overview – *Control Systems Software Functional Specification*

Summary

On June 26, 2003, BNI hosted and conducted the June Bi-Monthly Design Overview covering the topic of *Control Systems Software Functional Specification*.

This meeting focused on the process BNI is pursuing in the development of Software Functional Specifications (SFS) for 171 different WTP systems. SFS development follows a well-defined series of steps that lead directly to writing the specific code for the Distributed Control System (DCS) hardware programming. More detailed information regarding the meeting is provided in the BNI Meeting Minutes (See below.) **Note: This meeting did not address ITS systems accept in a general sense in response to questions.**

The presentation and the materials received during the Design Overview provide adequate indication of the product ORP may expect from BNI in the design of the WTP DCS. While these materials are still being studied by ORP, the general conclusion so far is: **The Distributed Control System being designed for the WTP is consistent with industry standards and appears to incorporate the latest developments in technology market trends.** ORP engineering staff will complete a more thorough report leading to this conclusion in September 2003. For further information contact Mark Ramsay, 376-7924.

Issues and Recommendations

There were no significant technical I&C issues raised by ORP during or after the Design Overview Meeting. In fact, the design approach and process BNI is employing appears to be quite logical and well thought out. However, there is concern regarding BNI's ability for timely execution of the tremendous workload yet ahead in the development of an SFS for each of the 171 different plant systems. This concern is based on the following two points. (1) BNI acknowledged that the process they're using to producing each SFS has not been done before. Therefore it is possible that BNI may have underestimated the work planning. (2) The SFS process is labor intensive and hinges on the production of Rev.0 P&IDs. BNI has a recent history of schedule problems due to late P&IDs.

Recommendation: In the BNI Monthly Progress Report, specific account should be made as to the status and progress of SFS developments. This is work that could become critical path at some time in the future and therefore, should be monitored until sustained success in the work execution is demonstrated.

Attendance, Attachments, and Materials

Specific attendance by ORP staff and the particular areas of oversight are listed in the table below:

ORP Participants	Area of Oversight
Wahed Abdul	Ops and Commissioning
John Clark	Project Management
Pete Furlong	Project Management
Brain Harkins	Facility Rep.
Lew Miller	Nuclear Safety
Bruce Nicoll	Project Management
John Orchard	Engineering
Mark Ramsay	Engineering (I&C Lead)
Ed Randklev	Engineering
Randy Unger	Engineering

Attachments to this record include:

- **(A) BNI Meeting Minutes.** These discuss:
  - Summary of the Presentation
  - Comments and Significant Discussion Items
  - Control Systems Overview
  - Software Lifecycle
  - Software Functional Specification (SFS)
  - Plant Training Simulator
  - Action Items

  The Meeting Minutes also include as attachments, the Meeting Agenda and the Meeting Attendance List.

  The Meeting Minutes were reviewed by several of the ORP personnel listed above and accepted as an adequate record of the Design Overview content and proceedings.

- **(B) OPR Listing of Suggested Topics.** This list contained suggested items for discussion at the Bi-Monthly meeting. These were submitted prior to the scheduled meeting in an effort to convey ORP expectations.

- **(C) BNI Response to Suggested Topics.** BNI were able to address several of the items recommended by ORP. Several items could not be addressed mainly because they were not part of the meeting scope.

Presentation materials were provided to ORP, which included hardcopies of the presentation slides and a CD with additional slides.

Attachment A: BNI Meeting Minutes

Attachment B: OPR Listing of Suggested Topics

Attachment C: BNI Response to Suggested Topics

Attachment 3:

July 2004 Report

WTP Distributed Control System Review

1 Objective and Scope of the Review:

The contractual scope is listed as:

> Review the WTP distributed control system planning, integration, functionality, testability, and maintainability, using documentation to be provided by BNI and DOE, as well as direct meetings and discussions with key BNI and DOE personnel.
> Identify significant vulnerabilities in the design or implementation of the distributed control system.
> Suggest areas for cost, schedule, or safety enhancement that appear to be readily achievable.
> Document assessment of project status related to the WTP DCS, observations, and recommendations in a brief (ten pages or less) written report upon completion of the assignment.

Conversation with John Eschenberg on July 8, 2004 clarified that his specific objectives included:

1. Check on the health & well being of the functional design and implementation of the DCS. Is it progressing at the pace needed to achieve schedule?

2. Check on the level of automation being applied – is the balance appropriate?

3. Produce a plan that tells the DOE what to look for as the system develops over the next three years.

Discussion with Lew Miller on July 8, 2004 emphasized the importance of safety and noted the need to check the arrangements or procedures used by Bechtel to:

1. Classify instrumentation functions as safety instrumented functions (SIF's), and
2. Define target safety integrity levels (SIL's) for these safety instrumented functions, and
3. Ensure that the control and instrumentation design and supply will satisfy these required integrity levels.

It was agreed with John Eshenberg, on July 14, that the work shall be undertaken in two stages, with the instrumentation safety analysis check delayed for a month or two, allowing the Bechtel design to mature through a particular critical phase.

This interim report therefore covers the first of these two areas of work, associated with the distributed control system status and the degree of automation that is being applied to plant and process control.

2 Check on the status of the functional design and implementation of the DCS.

2.1 General

The design of the hardware and system configuration / architecture of the WTP DCS appears good. The planning and quality control of the design flow and software implementation process, as outlined in figure 1, appears well thought out and well documented.

Schedules exist and, against the level 4 schedule, Bechtel appear to be on track. The current staffing level is currently over 20, the peak (plateau) occurring in just over 12 months time, is between 35 to 40, and may be lower in practice. Hence this appears achievable.

There are no apparent significant deficiencies in this area, and it is clear that some excellent work is in progress.

2.2 WTP DCS (Software) Related Concerns - Standardization

There are (as always) significant interfaces between and within overall control system design, the control of individual process areas, operational requirements and interactions, the achievement of throughput, safety criteria and so on. The design groups associated with the main areas of PT, LAW and HLW – plus B of F and Lab – are geographically dispersed. In the absence of centralized overall design, particularly C&I where the facility C&I and plant wide C&I groups are separated, extra effort need to be sustained. For example SFS's need to be kept synchronized and design philosophies have to be kept rationalized

This includes ensuring a standardized approach to control and operation. Differences in implementation or "look and feel" between process areas need to be avoided and inter-process transfers and interactions need to be managed.

2.3 WTP DCS (Software) Related Concerns – Process Design Uncertainty

There appears to be some uncertainty about the detail design of certain process functions or stages. The detail design considered here includes data sheets, system block diagrams and acceptance criteria.

This has been quoted as one reason for the postponement of the application of comprehensive, sequence or procedure based, automation. This needs to be fully explored so that the limits and areas of most risk are understood. Any high-risk areas need to be resolved, with software implementation delayed until design is more certain. Clearly work on the translated of the 'rev A' SFS's to the SDD's and software implementation should be prioritized to ensure work is not inappropriately channeled to uncertain areas.

2.4 WTP DCS (hardware & software) Related Concerns – Systemization

Each DCS controller and project system content has already been examined by Bechtel, aligned and agreed; which is a commendable 'systemization' practice.

As may be understood or expected the DCS system architecture shows examples where more than one DCS Controller can cover an overall process or service function. The example noticed was LAW C3 ventilation. Further, these 'functionally shared' controllers are in different areas / rooms / geographical locations.

Also, the routing of signals to / from a controller can be heavily influenced by geography, and there can be considerable cost advantage in routing to the nearest available controller. Is there a general criteria or policy that would over ride these types of considerations?

An open question is "Has systemization considerations been included on the design and management of all systems items, including the cabinet power supply arrangements?" This topic involves a critical principle that influences the ease or difficulties (and delays) experienced during commissioning.

2.5 WTP DCS Suggestions

1 Use selective 'prototypes'.

The project may see benefit in the identifying controllers, such as HLW PJ M (?), to bring forward, complete & test early. At least one such controller should be completed early from each major process area, see figure 2.

2 Enhance the use of simulation

The planned control room type of simulation does not appear to be targeted to test software or assist in the task analysis of operational activities. It may even have different configuration management.

It is suggested that the project develop selected (process or tank transfer) mathematical models, prove these models and then use them as a simulation basis, perhaps with speedup, in an integrated manner with the DCS software.

3 Review the use of the integrated OR model.

This is an uncertain area, not specifically included in the scope of this task and therefore without any formal discussion with the expert project staff. However in the course of the work undertaken, certain indications have caused some concern, including:

- Questions associated with the OR model providing throughput confirmation.
    - Are there different or sub divided models within the project, if so are they integrated and controlled?

- Questions associated with the base data being used by the OR model.
    - Comment that the crane info. is not fully loaded into the OR model ~ and there is an absence of resolvers on cranes.
    - Questions on the instrumentation (and valves) availability levels that will be achieved and if this has been reflected in the OR model assumptions.

- Questions on the automation assumptions that are imbedded in the OR model.
    - Has the OR model been run and rerun with and without the changed degree of automation that is being proposed?

- The need therefore to **formally** re-run the OR model, taking cognizance of the proposed changes to the basis of design.

4 WTP Software Implementation – The Tracking of Progress

Appropriate project controls are in place and working, and progress can be tracked on the Bechtel C&I Summary Schedule (level 3 or, in more detail, levels 4 & 5).

Progress trends are available, although currently there is insufficient planned or actual progress to allow these trends to be meaningful.

The DOE should undertake a monthly (or at least quarterly) check on the actual vs. planned progress of **SFS's** at rev 0. This should be sub-divided, at least, to the major areas of LAW, HLW, PT, B of F and Lab. Subsequently the progress achieved **on testing** should be monitored.

A bi-annual review should be scheduled, specific to software implementation progress.

5 The Potential Reduction in the Level of Automation:

At the start of this work, and almost immediately, it became clear that there is a currently advanced proposal to change the basis of design of the WTP. This change is summarized in the **draft** revision to the Basis of Design Document 24590-WTP-DB-ENG-01-001, Section 7 – Control Philosophy, sub section 7.1 'Summary':

Revision 1 states:

> *High levels of automation will be implemented, optimizing throughput and minimizing staffing where practical. Operator decisions may be necessary to maximize the throughput of WTP or meet product quality requirements. Extensive*

diagnostics for recognition and correction of conditions will be included to reduce downtime. Simple, common sense design of modes of operation will ease operability in both normal and abnormal situations.

It is proposed that this be deleted and replaced by:

Manual administrative control of the plant will be utilized to the extent practical. Automatic control will be used where timing requirements are too fast for manual action.

The above is a significant basic change in the basis of design of WTP.

Further insight into this change, complete with examples, can be found within the basis of design document proposed revision, including sections:

- Section 7.3.5 Control modes for Primary Control Types, where the revision changes:
  - "Process operations will be automated to minimize the number of stages requiring operator initiation."

  To
  - *"Process operations will be automated for basic control functions such as interlocks regulatory control, or sequences that require fast execution times.'*

  And
  - *"Most operations will be controlled manually via administrative procedures written by operations."*

- Section 7.3.5.2. Manual Mode, which has the addition that:
  - *The primary mode of operation in the WTP plant for batch operations will be manual execution of written procedures. Those systems that are designed to be operated in the manual mode will not have the option of being operated automatically."*

5.1 The Potential Reduction in the Level of Automation: Stated Reasoning.

The following, plus the section 5.2 content of this report, is derived from conversation with Ross Hamlett, Wednesday July 21, 2004:

- WTP is seen as a '1st Generation' facility, with significant design details not yet known well enough to automate.
- In DWPF, during commissioning, automation was stripped out, then fitted back as necessary when sufficiently understood.
- Therefore the view is that on WTP automation should be scaled back from the previously agreed level.

5.2 Potential Reduction in the Level of Automation: Stated Advantages.

The acceptance of the previously stated assertions can lead to the following reasoned advantages:

- Reduced testing:
- No need to test routes that are uncommon / irregular
- If automated procedures are present then project **has** to test these and by their very nature the tests are more complex ~ including the pre-checks, both start and termination, and the interlocks.
- Reduced control system logic rework, during commissioning, to accommodate changes in operational strategies.
- Significantly reduced commissioning scope.
- Reduced design work - at this point in the project.

- The alternative (to the above) carries a contractual risk of failure to achieve the project cost or schedule ~ commissioning is a critical path activities.

It was noted that the Commissioning & Test (C&T) team view is that:

> *"Procedural (batch) control vs. direct operator control does **not** alter staffing requirements for WTP facilities."*

5.3 An Alternative View on Staffing Levels.

It is considered that the removal of the automated procedural sequences applied to activities such as liquor transfers **will** result in increased burden upon the operational staff. In this example, the prospect of operators manually working through a listing of pre-checks and settings, confirming valves and pump status before initiation etc., is considered contrary to normal current practice.

These checks or pre-conditions are 'normally' interrogated by the DCS and the operator only has to accept the DCS confirmation. Further, when pumping is underway the DCS directs the operator to any state changes s/he needs to be aware of, rather than the operator being engaged 'full time' in tedious, long duration, tasks.

This difference of view, with respect to operational loading and adequacy of provisions (CCR consoles etc) and resources, can be resolved via task analysis.

At a burdened hourly rate of ca $40 / hr a **single** additional operator costs about $3M over the 40 year operational span. Hence if the change were to add just two operators, per shift, to each of the three major areas this would result in 8 additional operators per area, 24 in total, and a potential cost of $72M. A cost benefit analysis appears to be needed.

5.4 Potential De-Automation: The Effect on the Safety Case

Typically, credit is taken for automated actions that reduce the likelihood of a demand on the safety systems. Provided the appropriate quality control process is followed such automation is normally considered to be more reliable than operator action, less likely to making a mistake. A operator action, depending upon ergonomics, circumstances, complexity, checks and procedures has a typical likelihood of error of somewhere between one in a hundred to one on a thousand - per action.

It is unclear if the overall safety case work has been reviewed and revisited to take account of the proposed change in the basis of design statements on automation. It is unclear if a risk review has been undertaken to highlight areas of particular concern.

It is therefore recommended that the status of this work is checked and that these tasks be undertaken if necessary.

5.5 Potential De-Automation: The Effect on Commissioning Scope

It has been said that if, for example, a piped transfer is not normally used, and has no procedural sequence control, then commissioning tests will be restricted to flushing trials only. Whereas, if the automated checks and actions are present, then these and the full transfer system, need to be commissioned.

However – an alternative view is that, with or without automated sequences, if a pumped transfer routes exists it should be fully cold commissioned. Best endeavors should target the elimination of an unexpected problem during hot ops, however infrequent the use. This consideration is more associated with the commissioning strategy, rather than being restricted to an automation issue.

5.6 Degree of Reduction in Automation:

It is difficult to accurately determine and quantify the proposed level of de-automation. A figure of 14 % scale back is being circulated. The basis of this figure is not yet clear. Given that the standard controls (e.g.PID) are not at issue, the scale back % should simply be the 'before and after' ratio of procedural sequences (only). Comparing the Basis of Design rev 1 to the proposed rev 2 version produces the following table:

Facility	Area	Original Automatic Procedural	Revised Automatic Procedural	Revised (new) Manual Admin
Pretreatment	LAW Receipt & Evap			☐
Pretreatment	HLW Receipt & LAW / HLW Ultrafilitration		☐	☐
Pretreatment	Ion Exchange		☐	
Pretreatment	Liqid Effluents			☐
Vitrification (LAW & HLW)	Receipt & Blending	☐		☐
Vitrification	Melter Feed Prep	☐		☐
Vitrification	Melter	☐		☐
Vitrification	Melter pour, sampling & hndg	☐		☐
Vitrification	Product Can Handling	☐		☐
Vitrification	Product Can Weld	☐		☐
Vitrification	Product Can storage	☐		☐
Vitrification	Liquid Effluents			☐
Bal of Facilities	Liquid Effluents			☐
Bal of Facilities	Wet & Dry Receipt & Store	☐		☐

The above simplified representation suggests that all automatic procedural controls that were originally listed in the Basis of Design document have been replaced by manual administrative controls. Hence the comment that the 14% figure needs to be properly understood.

5.6 Observation on the Basis of Reasoning

C&T stated that *"In DWPF, during commissioning, automation was stripped out, then fitted back as necessary when sufficiently understood."* How much was back fitted wasn't quoted. It is clear that the DWPF experience is a significant influence on the design, construction and commissioning of WTP.

According to the SRS Fact sheet[1]

- DWPF construction began in 1983
- System testing began in 1990
- Non- rad simulated tests were completed in 1993
- Operations commenced in 1996

Simply and only from the above a concern is that relatively old technology and experience is overly influencing a 21st century plant design. The relevance / degree of truth of the above will be known better by those controlling the Project.

5.7 Potential Reduction in the Level of Automation: Final Comment

In my experience, it is unusual for an Operational team to pressurize the C&I Team to **reduce** the level of automation, normally the Operations team want a plant with comprehensive automation.

Coupled to the above is the fact that there has also been reference to the expectation that this 'de-automation' will help the contractor achieve the cost / schedule project demands. What follows, therefore, is pure speculation:

Observations:

- The contract scope is design, build and prove.
- The contract does not cover operations beyond the proof of throughput stage.
- The existing schedule shows cold and hot commissioning as critical path.
- A GAO[2] report shows that the cold and hot commissioning time duration has been substantially reduced, see figure 3.
- All of the above provides pressure for reducing critical path activity scope and complexity.

The above, coupled to the saving of design costs associated with automation provision, is a powerful driver.

---

[1] (http://www.srs.gov/general/news/newpub- rel/factsheets/dwpf.pdf):

[2] Source: GAO-04-611 Hanford Waste Treatment Project. Page 18

Summary & Recommendations

On the topic of the DCS Software Implementation:

There are no apparent significant deficiencies in the implementation of the DCS software and it is clear that some excellent work is in progress.

It is suggested that to reduce risk further consideration be given to:

- The selective use 'prototypes'.
- Enhance the use of simulation.
- Review the use of the integrated OR model.

These recommendations are described further in the text of this report. The report provides guidance on monitoring progress in the future.

On the topic of degree of automation applied to process control:

This is seen as an area of particular and urgent concern. The report documents areas of perceived risk and provides suggestions or recommendations to test or quantify such risks. This report suggests:

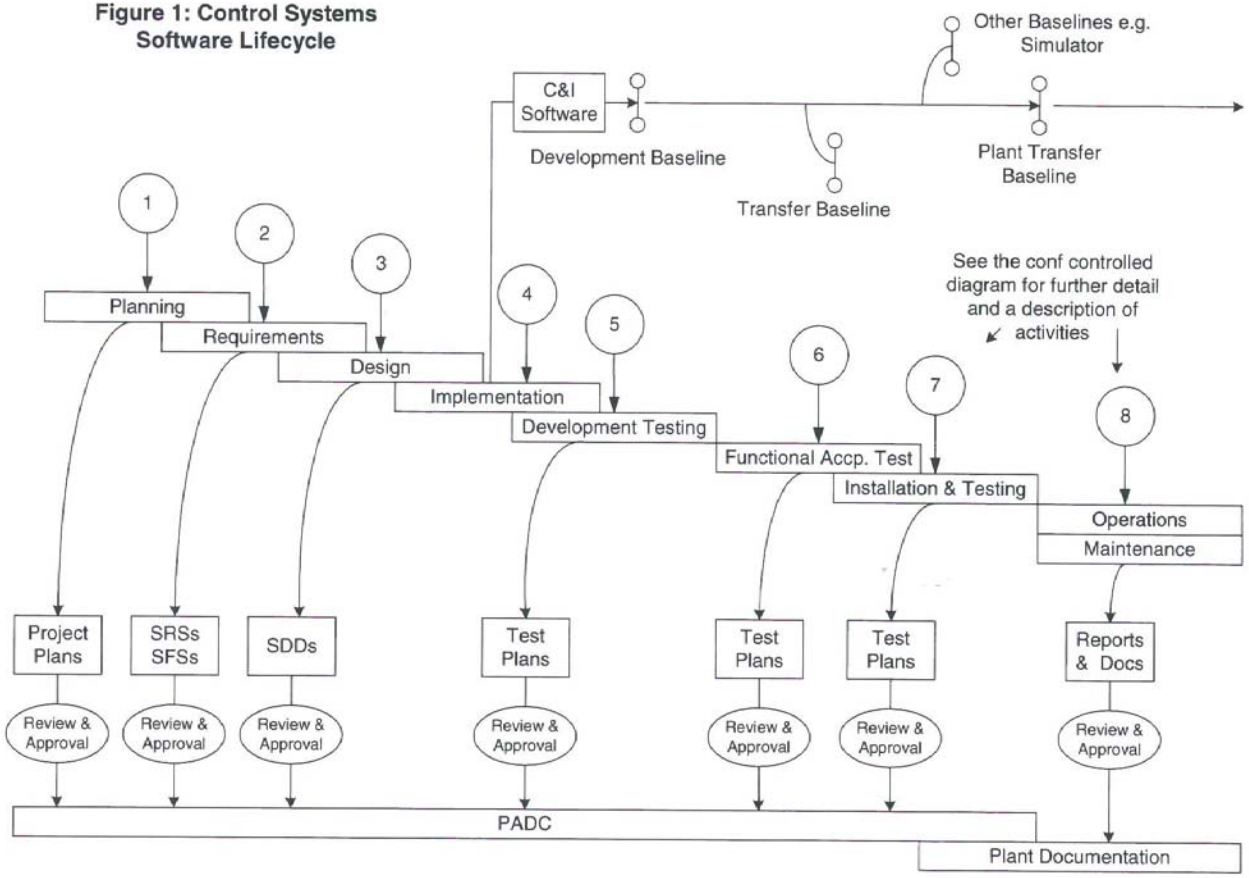
- A lifetime cost benefit analysis be done on the proposed change to the basis of design.
- A risk analysis is undertaken covering any impacts of the proposed change to the basis of design.
- A task analysis is completed showing the effect of the proposed change to the basis of design on operational burden and staffing levels.
- The safety case work be reviewed to determine if there is any effect of the proposed change to the basis of design,
- The above should include a technical examination of potential reliability / availability aspects and feed such results back into the OR model for a check on throughput.

All of the above should be managed by DOE or an independent party

G Harrop

July 22, 2004

Figure 1: Control Systems Software Lifecycle



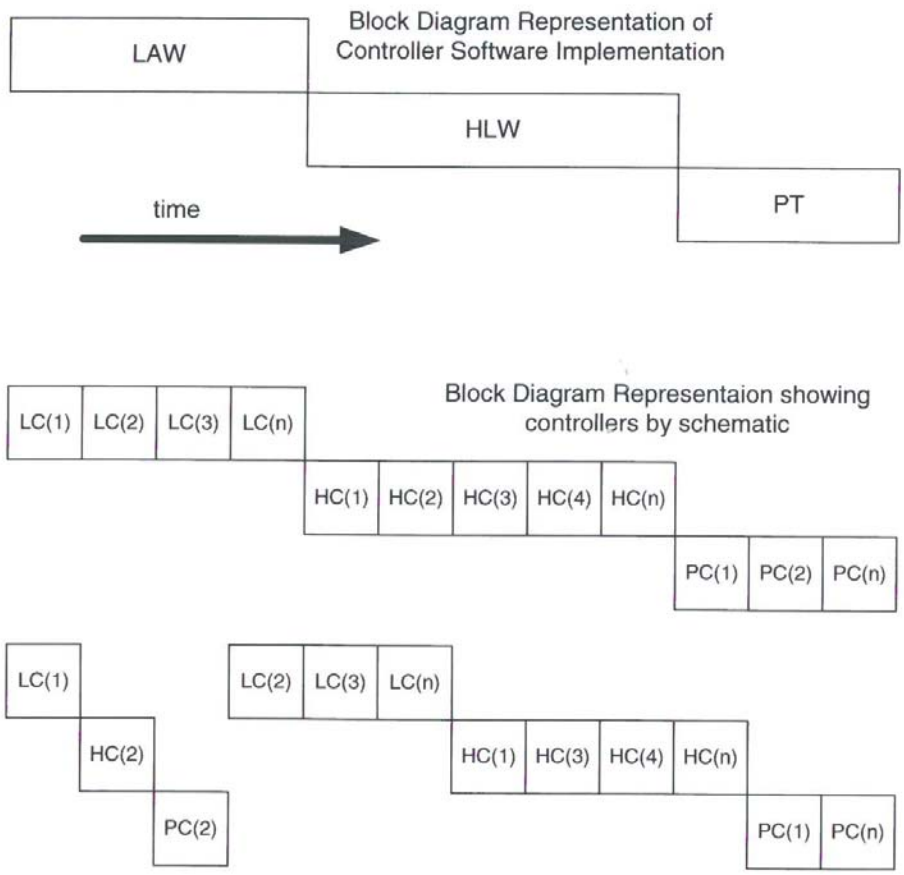
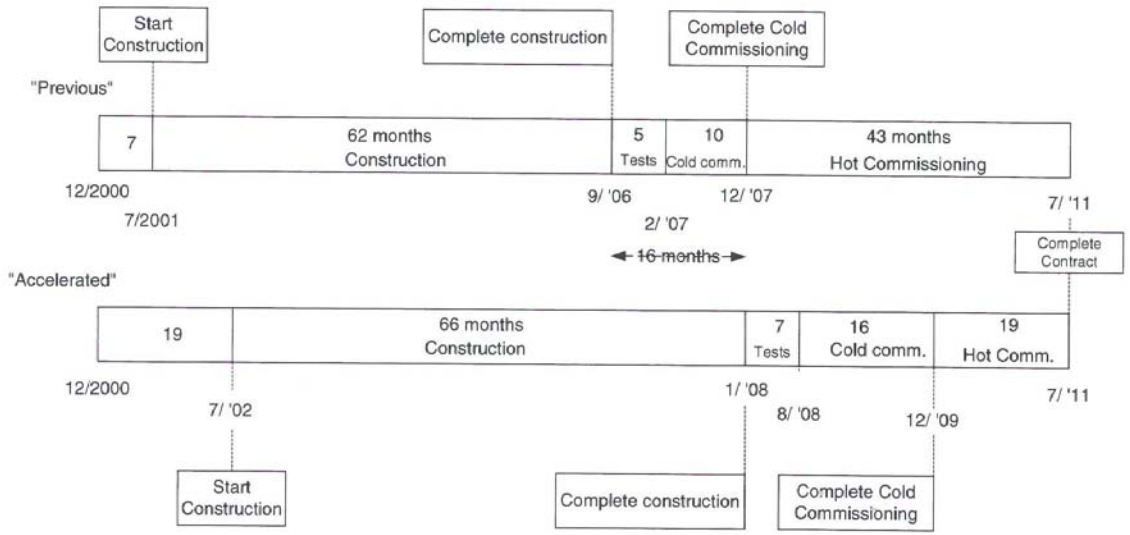


Figure 2: Simplified picturial representation of 'prototype' tactics.

Figure 3. Key Project Dates: Previous & 'Accelerated' Schedule Approach



Source: GAO-04-611 Hanford Waste Treatment Project. Page 18