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

MAY 1 3 2005

05-WED-020

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

Dear Mr. Henschel:

CONTRACT NO. DE-AC27-01RV14136 – U.S. DEPARTMENT OF ENERGY, OFFICE OF RIVER PROTECTION DESIGN OVERSIGHT ASSESSMENT REPORT ON THE PROGRAMMABLE PROTECTION SYSTEM (PPJ) (D-05-DESIGN-012)

This letter provides for your information the subject Design Oversight Assessment Report (Attachment) on the PPJ design developments. This assessment was conducted in April 2005 and evaluated the Bechtel National, Inc., methodology and processes for development of the PPJ design and documentation, as well as status to-date.

The assessment identified no Findings and at this time there are no open items or new actions identified for the Waste Treatment and Immobilization Plant (WTP) Contractor.

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,

for Roy J. Schepens
Manager

WED:WFH

Attachment

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

Attachment
05-WED-020

ORP Design Oversight Report

Waste Treatment Plant (WTP) Programmable Protection System (PPJ)

D-05-DESIGN-012

April 2005

WED:MLR
May 2, 2005

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

ORP Design Oversight Report

Waste Treatment Plant (WTP)
Programmable Protection System (PPJ)

D-05-DESIGN-012

April 2005

Performed:

Mark L. Ramsay, SSO
WTP Engineering Division
Office of River Protection

Concurrence:

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

Approved:

John R. Eschenberg, Project Manager
Waste Treatment Plant
Office of River Protection

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

ORP Design Oversight Report

Waste Treatment Plant (WTP)
Programmable Protection System (PPJ)

April 2005

Table of Contents

EXECUTIVE SUMMARY 3
INTRODUCTION AND BACKGROUND 4
SCOPE AND APPROACH 5
DISCUSSION 5
APPENDIX - SAFETY INSTRUMENTED SYSTEMS LISTINGS 14

Table of Tables

Table 1 - PTF Safety Instrumented Systems 14

Table 2 - HLW Safety Instrumented Systems 17

Table 3 - LAW Safety Instrumented Systems 18

Table of Figures

Figure 1 - SIS within the WTP Control System 20

Figure 2 - Typical SIS Life Cycle Document Flow 20

EXECUTIVE SUMMARY

This assessment (conducted in April 2005) evaluated the Waste Treatment and Immobilization Plant (WTP) Programmable Protection System (PPJ) design developments. Particular focus was on:

- Safety Instrumented System (SIS) definition;
- Document deliverables;
- Requirements implementation;
- Implementation of key standards;
- Software planning;
- Logic hardware; and
- Schedule and progress

Observations:

- The SIS development process (from SIS needs determination to final software implementation) is procedures driven and is well documented.

- ANSI/ISA S84.01, *Application of Safety Instrumented Systems for the Process Industries* is effectively implemented in Bechtel National, Inc. (BNI) documentation and in the SIS designs.

- Safety System Requirements Specifications (SSRS) are in the early stages of development but appear to meet requirements defined in the *Basis of Design* (BOD) and in the *Safety Requirements Document* (SRD).

- Software planning is well defined, but execution has hardly begun due to the immaturity of SSRSs.

- Logic hardware as represented by a test bed system (by Triconex) meets requirements defined in the BOD, and appears to represent the best logic solver technology currently available.

- Approximately 40 SISs are currently planned for development. These all appear to be scheduled and are in various stages of progress, mainly in terms of SSRS development.

Highlights

- ANSI/ISA S84.01 is used as an umbrella document for other implementing standards listed in the SRD and BOD. The BNI Design Guide formalizes and drives specific consideration and incorporation of these implementing standards as applicable in the SSRS development process.

- BNI streamlined the software development process to better utilize the SSRS by including not only SIS design requirements but also software requirements. This eliminated the need for an additional level of SIS software documentation.

- The SSRS documents evaluated exceed the requirements defined in ANSI/ISA S84.01 and provide excellent traceability to system safety basis. This is due primarily to a well formulated BNI *Design Guide for Safety Instrumented Systems Implementation.*

Conclusions

The PPJ design appears on course and the design process is well documented and focused on meeting requirements and incorporating appropriate industry standards. At this time there appear to be no weaknesses or vulnerabilities in the design methodology or in the usefulness and quality of the SSRSs, although these documents and the SIS development process in general, are only in the initial stages.

Future assessments will be aimed at: (1) the Integrated Safety Management (ISM) process for identifying the need for an SIS based on hazards analysis; non-SIS protection layers; and determination of the system Safety Integrity Levels (SIL determinations); (2) PPJ Software Design Documents; and (3) Functional Acceptance Tests leading to Revision 0 SSRSs.

INTRODUCTION AND BACKGROUND

Programmable Protection System

The PPJ for the WTP provides independent protection and control of systems, structures, and components (SSC) determined to be safety design class or safety design significant. The PPJ is independent from the normal plant control system referred to as the Integrated Control Network (ICN). The PPJ is designed to operate automatically and transparently without operator intervention to bring process systems to a safe state or maintain a safe state if and when the normal control systems fail to keep the processes within the safe operations envelope.

Each of the main WTP facilities (Pretreatment Facility [PTF], High-Level Waste [HLW], and Low-Activity Waste [LAW]) has a dedicated PPJ that is comprised of SIS. Each SIS is defined by a SSRS that addresses at least one safety instrumented function (SIF). Several SISs encompass more than one SIF. These systems and functions are listed by facility in the Appendix.

An SIS consists of field sensors, a Logic Solver (or hardwired logic) and final field elements (such as valves) that share logic to serve aggregate safety functions. SISs are considered active preventive or mitigative SSCs. A general system is shown in Figure 1. BNI will utilize the Tricon System developed by Triconex as the logic solver for SISs. A test bed system is currently being utilized.

SCOPE AND APPROACH

This review focused on the PPJ design developments to date and was conducted during April 2005. The following elements were addressed.

- Implementation of ANSI/ISA S84.01, *Application of Safety Instrumented Systems for the Process Industries* (S84);
- Review of selected SSRSs against guidance provided in 245090-WTP-GPG-J-015, Revision 0, *Design Guide for Safety Instrumented Systems Implementation* (Design Guide) and requirements in 24590-WTP-DB-ENG-01-001 *Basis of Design* (BOD) and *Safety Requirements Document Volume II* (24590-WTP-SRD-ESH-01-001-02);
- Software development planning;
- Evaluation of the Triconix System/Equipment;
- Current SISs listings; and
- Schedule progress.

A general review of design documents and criteria was performed and a crosswalk comparison was made of ANSI/ISA S84.01 with the BNI Design Guide. Selected SSRSs were reviewed against the Design Guide, BOD and SRD. The Triconix test bed equipment was also observed and vendor literature on the Tricon equipment was reviewed. The schedule was briefly considered, mainly regarding development of the SSRSs and selected BNI Control and Instrumentation (C&I) engineers were interviewed.

DISCUSSION

General review of design documents and criteria

SIS Design Criteria

SISs are engineered safety systems designed to meet safety criteria defined in *Safety Requirements Document Volume II* (24590-WTP-SRD-ESH-01-001-02). Safety Criterion (SC) 4.3-1 of the SRD states:

"Engineered safety systems shall be designed (1) to initiate automatically the operation of appropriate systems to assure that specified acceptable design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of Important to Safety systems and components. The ability to manually initiate engineered safety systems shall be provided."

The SRD requires that these SISs be designed in accordance with ANSI/ISA-S84.01, *Application of Safety Instrumented Systems for the Process Industries* (S84) to meet WTP safety system availability requirements. In addition, the design of the WTP SISs must meet general criteria defined in Section 9.10 of the BOD.

ANSI/ISA-S84.01-1996 (S84)

S84 is one of several implementing standards for SC 4.3-1, 4.3-4 and 4.4-2 defined in the SRD and also is an implementing standard for the following requirement (Appendix B, 2.5 in the SRD):

"Automatic systems should be provided that would place and maintain the facility in a safe state and limit the potential spread of radioactive materials when operating conditions exceed predetermined safety setpoints." (DOE/RL-96-0006, Section 4.1.1.5)

The objective of S84 is to define the requirements for SISs. S84 provides performance based criteria with very few prescriptive requirements. Hence, there is considerable flexibility as to the methods for meeting the criteria. BNI's implementation of this standard is most visible in their SIS Design Guide, which provides greater detail and specificity for design of the WTP SISs.

While S84 is used primarily to specify development of the SISs, BNI also utilizes this standard as an umbrella document to encompass other required implementing standards as listed in the SRD and BOD. This ensures that implementing standards are adequately addressed and, if applicable, incorporated into the safety systems design. This was confirmed in the review of the BNI Design Guide and selected SSRSs.

According to the SRD, the applicability of S84 is limited to Design and Construction phases of the WTP. Therefore, those elements of S84 dealing with Testing, Start-up and Commissioning phases are not specifically required for implementation. However, it is likely that the SIS design will be consistent with S84 in these areas as well. Also, regarding construction, S84 stipulates that "equipment shall be installed per the design." Given that this is the only construction requirement, S84 applicability is essentially limited to the *design* of the WTP SISs.

Design Guide

BNI has provided a *Design Guide for Safety Instrumented Systems Implementation* that provides a point-by-point response to Clauses 4 though 7 of the S84 standard. Clauses 1-3 (general scope, standard conformance, and definitions) are implemented in the course of addressing Clauses 4-7. Clauses 8 and on of S84 deal mainly with project phases other than Design and Construction and are not applicable, neither are they specifically addressed in the Design Guide.

The Design Guide sets forth the general flow process for development of each SIS. The steps are:

- Establishing a Safety Life Cycle process that addresses such activities as hazards analysis, the need for an SIS, non-SIS protection layers, determination of the SIL (e.g. safety system availability based on probability of failure values), and various other conceptual activities. The BNI ISM process provides these activities as inputs to SIS development;

- Development of the SSRS. Each SIS will have an SSRS that evolves through the project phases with input from the ISM process. SIS basis requirements are defined through the ISM process and documented in the facility-specific Preliminary Safety Analysis Reports. These requirements are also fully documented in the appropriate SSRS;

- Development of the SIS Conceptual Design;

- Development of the SIS Detailed Design; and

- Performance of Functional Acceptance Testing.

The Design Guide provides the details for each of these process steps.

SSRS

The SSRS is the product document from implementation of S84. The SSRS defines input requirements, safety functional requirements and safety integrity requirements resulting from conceptual and detailed design requirements and considerations set forth in S84. The SSRS is developed in concert with the BNI ISM process and establishes the basis upon which system hardware and software is developed.

In addition to the value that the SSRS provides for final system design, each SSRS provides traceability to the ISM documentation justifying the need for the SIS along with SIL determinations.

Software Project Plan

PPJ software is developed according to the *Software Project Plan for Programmable Protection System* (24590-WTP-PL-J-01-004). Figure 2 provides the document flow for the software document deliverables. Note that current work to-date has been limited to SSRS development. Hence, most of the software design is yet to be performed. Software design for a given SIS can begin no sooner than release of the associated Revision A SSRS.

Recently (January 2005) Revision 1 of the Software Project Plan for the PPJ was released. It represents a marked improvement over Revision 0 and reflects BNI's efforts to make the PPJ software development process consistent with the software process for the ICN. Also, in revising the PPJ Software Project Plan, BNI streamlined the overall process and eliminated the need for additional documentation to capture software requirements in SIS-specific Software Requirements Specifications. Software requirements are now adequately captured in the SSRSs.

Crosswalk of the Design Guide with S84

As mentioned above, S84 is only required for the *design* of SISs. Hence, project phases preceding or following design are not contractually amenable to compliance with S84. Those portions of S84 strictly applicable to the WTP design include Clauses 5 through 7. These clauses deal with development of the SSRS and conceptual and detailed design requirements respectively. However, the BNI Design Guide also addresses Clause 4 in S84 dealing with the Safety Life Cycle, though not as a commitment to implement the entire S84 life cycle but rather to clarify what is analogous within the ISM process to the S84 safety life cycle.

In this review, the Design Guide (Revision 0) was compared with the S84 standard. The summary results are described as follows.

The Design Guide was developed and formatted to specifically correspond to Clauses 4 through 7 of S84. Each element under these clauses was addressed point-by-point and as applicable, was incorporated into the Design Guide.

In addressing Clause 4 of the standard, the Design Guide provides appropriate response in terms of the ISM process and is more detailed than S84 in describing the safety scope relative to the ISM process. S84 describes a Safety Life Cycle concept. The WTP analog to this concept is the ISM process. The BNI C&I group uses the output of the ISM Process to perform design for SISs consistent with the Design Guide.

Also, BNI implemented under element 5.2.4 *Regulatory requirements impacting the SIS,* (*SSRS Input Requirements* section); requirements to address other standards listed in the BOD and the SRD, and as applicable incorporate these standards into the design. As verified from review of selected SSRSs, this process is being applied to SIS design and appears to be effective.

In instances where S84 lacked specificity, the Design Guide provided useful detail in various appendices particularly applicable to the actual development of an SSRS. However, the information in these appendices will soon be provided in another document. Revision 1 to the Design Guide is currently in process and according to C&I engineers, will reduce much of the detail currently provided in the appendices. This detail will be placed in a desktop instruction (GPG document) that will be expanded to include more detailed information for greater clarity in SSRS development. It was stated that the revision will not reduce or undermine the degree of S84 incorporation.

General Review of Selected SSRSs

According to the SIS listings in the Appendix, there will be about 40 SISs, each requiring an SSRS. (Note: This number may change as the project design evolves and the ISM process determines a given SIS is no longer necessary or that a new SIS should be added.) The SSRSs are currently in various stages of development and none have yet been issued Revision 0. (Revision 0 SSRSs are issued following Functional Acceptance Testing. See Figure 2.) A few Revision A or draft Revision A SSRSs were provided by BNI for this review.

The main objective for this SSRS review was to determine that these documents will likely meet requirements set forth in the BOD and the SRD as well as be consistent with the BNI Design Guide, which implements S84. This review is summarized below.

Selected SSRSs appear to meet BOD Requirements:

The specific BOD requirements for the SIS designs are listed as bullets in Section 9.10 of the BOD. Observations with respect to each applicable bullet (#1, #2 etc.) are stated below.

#1- As evident from SIF process graphics and configuration diagrams within the SSRSs, the SISs will provide only status information to the ICN system without compromising PPJ isolation from the ICN.

#2 & #3 - Dedication of sensors and final control elements to the SISs is generally apparent from review of the SSRSs. However, because changes in the designs and documentation are still in process (only draft Rev A SSRSs) some inconsistencies show up. For example, in one SSRS, an ITS radiation monitor provided both a safety function and a normal process function. In other words, the radiation sensor was not dedicated strictly to the SIS. This point was discussed with the C&I engineer who indicated that this issue had already been addressed and review of the associated meeting minutes confirmed the issue had been resolved to ensure the dedication of the monitor to the safety system. Similar clarification was made regarding dedicated final control elements which appear on process diagrams as having both a non-safety function control and a safety function control. BNI indicated that careful consideration to the BOD requirements was driving ongoing efforts and changes to ensure isolation and separation of SIS elements. Generally, to maintain the integrity of the PPJ system, devices wired to the PPJ will be properly isolated or treated as associated circuits and purchased and installed to meet the requirements of the associated safety function. In some instances, in order to maintain the integrity of a safety function, detection, logic, and action of a process function will be completed through the PPJ.

#5 - Under the Input Requirements portion of the SSRS, the safety function of a given SIF is defined and control strategy documentation is referenced.

#6 - Redundancy, independence and physical separation requirements applicable to SISs are implemented in accordance with IEEE standards identified in the SSRS for each SIS as *Input Requirements* under the *Regulation* heading.

#10 - As indicated from the SSRS process drawings, safety function devices are deenergized to trip. Hence, loss of instrument air or electrical power will cause final control elements to trip to the safety state. Trip actions are specifically addressed in the SSRSs. Also, *Spurious Trips* are addressed under *Safety Integrity Requirements* in the SSRS and the control actions are consistent with the BOD requirements.

#11 - The SSRSs address testing for each SIS under *Safety Integrity Requirements,* specifically, *Safety Testing.* Specific test requirements are still being defined in some of the SSRSs.

Selected SSRSs appear to meet SRD Requirements:

Generally, the SSRSs specifically site applicable SC from the SRD.

From narrative descriptions and the configuration diagrams provided in each SSRS considered, the respective SIS designs will provide automated operation of safety system equipment and sensing capability for accident conditions, as required by SC 4.3-1. Also, capability for manual activation of safety systems (SC 4.3-1) will be provided from Human Machine Interfaces (HMI).

It was also evident from the SSRSs that the SIS designs will provide ITS instruments and controls to monitor critical process variables such as vessel liquid levels, radiation levels, seismic activity, etc., with the ability to detect off-normal conditions and take appropriate actions to place the facility in a safe state per SC 4.3-4.

At least one of the SSRSs indicated that ITS instrumented functions are designed with periodic safety testing, maintenance and calibration requirements; consistent with SC 4.4-2. Other SSRSs have not yet defined the testing and maintenance requirements but this work is in progress and the SSRS requirements as defined by S84 address testing and maintenance.

Selected SSRSs appear to follow the BNI Design Guide:

The format and content of each SIF within an SSRS follows the specific content of Section 5 of the Design Guide (Clause 5 in S84). The general headings are:

- Input Requirements;
- Functional Requirements; and
- Safety Integrity Requirements.

Consistent with the Design Guide, Section 4.0, *The ISM Process and Safety Life Cycle for SIS,* and the safety life cycle concept in Clause 4 of S84, the SSRS includes necessary information from the ISM process in order to derive SSRS Input Requirements (safety functions, SIL determinations, etc.). These requirements provide the basis for the conceptual design of the SIS and are clearly delineated in the SSRSs documents evaluated.

Section 6 of the Design Guide provides conceptual design requirements and design considerations to meet SIL requirements. These requirements and considerations were addressed as evident from the SSRS Input Requirements, particularly in regard to common cause failure considerations and regulatory requirements, which involves a determination of the applicability of other implementing standards.

Functional Requirements and Safety Integrity Requirements in the SSRSs are determined based on the detailed design requirements described in Section 7 in the Design Guide. The SSRSs reflect reasonable consideration of Section 7.

Verification of the Tricon Logic Solver System

The Engineering Specification for the PPJ (24590-WTP-3PS-JD03-T0002) was issued for purchase in January 2003. Subsequently, a contract was awarded to Triconex to provide equipment, training, and services associated with development of the PPJ. For the equipment to be purchased, Triconex was required to provide a test bed system comprised of Tristation 1131 hardware and Sequence of Event Software. This system now resides within the BNI C&I group for training and testing purposes by the C&I engineers responsible for developing the system software for the PPJ.

Additional information regarding Triconex and their equipment was obtained at the Triconex web site. Highlights from this information are provided below.

About Triconex:

- In 1986, the Tricon fault tolerant control system was introduced. This system was designed around a triple modular redundant (TMR) architecture and was the first of its kind to be completely triple redundant, dependable and cost effective.

- Triconix has installed over 5,000 TMR systems throughout the world in a wide range of industries and applications.

- Recently, Triconex completed a nuclear class 1E audit by the Nuclear Regulatory Commission. As a result, the Tricon controller has become the first off-the-shelf digital controller certified for nuclear class 1E applications. This is explained further below.

In December 2001, the Nuclear Regulatory Commission (NRC) completed an extensive safety evaluation of the Tricon Programmable Logic Controller (PLC) system. The summary conclusion reached by the NRC in its evaluation of the Tricon system states:

"...when properly installed and used, the Tricon PLC system is acceptable for safety-related use in nuclear power plants."

"...the Tricon PLC system meets the requirements of 10 CFR 50.55a(a)(1) and 55a(h). It also meets GDC 1, 2, 4, 13, 20-24, and 29, and IEEE Std 603 for the design of safety-related reactor protection systems, engineering safety features systems, and other plant systems, and the guidelines of RG 1.152 and supporting industry standards for the design of digital systems."

> 10 CFR 50.55a(a)(1) and 55a(h) are federal regulations allocated to the oversight of the NRC with respect to *Domestic Licensing of Production and Utilization Facilities* (part 50) specific to *Conditions of Construction Permits* (50.55).
>
> GDC refers to General Design Criteria described in 10 CFR 50 - Appendix A
>
> IEEE Std 603 - *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.*
>
> RG 1.152 is the NRC Regulatory Guide 1.152 – *Criteria for Digital Computers in Safety Systems of Nuclear Power Plants*

The significance of the NRC evaluation as it applies to the WTP is the determination that the Tricon system meets the requirements defined in IEEE Std 603, which references many of the WTP implementing standards listed in the SRD.

About Triple Modular Redundant (TMR) architecture:

The Tricon system achieves fault tolerance through a TMR architecture. TMR is a simple method of packaging a set of triple redundant safety system components into a 2 out of 3 (2oo3) voting system that is engineered and programmed as if it were a single device.

The Tricon is designed with fully triplicated circuitry throughout—from the input modules, through the Main Processors, to the output modules. Every I/O module contains the circuitry for three independent legs. Each leg on the input modules reads the process data and passes that information to its respective Main Processor. The three Main Processors communicate with each other over a high-speed bus system called the Tribus. Once per scan, the three Main Processors synchronize and communicate with their two neighbors over the Tribus. The three sets of input data are interrogated and decided upon (a process called voting). The Main Processors execute the control program and send outputs generated by the control program to the three output modules. In addition to voting the input data, the Tricon votes the output data. This is done on the output modules as close to the field as possible, to detect and compensate for any errors that could occur between the Tribus voting and the final output driven to the field.

This architecture provides error-free, uninterrupted control in the presence of either hard failures of components, or transient faults from internal or external sources.

Key benefits and features of the Triconex TMR approach are:

- **No single point of failure** - The failure of any single component will not affect the correct operation of the Tricon system;

- **Very high safety integrity** - With the TMR architecture and high diagnostic coverage, the Tricon system achieves SIL 3 as defined in S84, representing highest level of safety system integrity. (Most of the WTP SIFs will be SIL 2);

- **High availability** - The Tricon TMR system can operate with one, two or three functional Main Processors. Faulted modules can be replaced while the system is operational for continuous uninterrupted control. A typical system has an Mean Time to Facility (MTTF) - spurious of greater than 200 years using the Military Standard failure rates. ***Using actual failure rates based on 1994 Triconex field repair records; the MTTF-spurious of a typical system exceeds 1,000 years;***

- **Low maintenance costs** - Highly skilled technicians are not required because extensive built-in diagnostics automatically pinpoint faults to field replaceable modules. (Alarms, PPJ status, and Tricon controller diagnostics will be fully communicated to the WTP Facility Control Rooms at the respective annunciators and HMI consoles.); and

- **Transparent triplication** - The Tricon TMR system has three isolated, parallel control systems integrated into one set of hardware. Two out of three (2oo3) voting provides high integrity, error-free, uninterrupted process operation. The Tricon appears to the user as one set of hardware, not three, allowing one control program for the application logic to be developed and downloaded to the three Main Processors. Field sensors connect to input points on the field termination panels. These signals are then separated into three isolated paths on the input modules and the data is sent over separate communication paths to the three Main Processors. After the control logic has been executed, output modules perform a 2oo3 vote of the output data received from the three Main Processors and sends the result to the output termination panels and the final field elements.

The following observations were also made regarding the Tricon hardware and are specific to the BOD requirements:

#4 - The test bed processing and logic circuitry is currently housed in a dedicated enclosure. Identical hardware for the plant systems will contain processing and logic circuitry in dedicated seismically qualified enclosures;

#7 - There is also dedicated cabling for the Tricon modules;

#8 - Provisions exists for manually resetting trips; and

#9 - The Test Bed hardware (controller) also includes system keyed locks to provide the administrative control for access to configurable parts.

Current Listings of SIS's by Facility

The listings of current SISs are provided in the Appendix. These are also listed in the Software Project Plan. Each SIS will have a dedicated SSRS. Current work associated with the SIS systems is mainly associated with SSRS development.

Schedule

The Level 4 schedule was briefly considered mainly to see what SSRS work activities were scheduled and that progress was being made, which was affirmed and verified by the SSRS evaluations and interviews. Critical evaluation of schedule performance was not part of this review mainly due to that fact that BNI is currently in process of establishing a revised schedule for PPJ work elements.

APPENDIX - SAFETY INSTRUMENTED SYSTEMS LISTINGS

Table 1 - PTF Safety Instrumented Systems

SSRS DOC	SSRS TITLE	FUNCTION TITLE	SAFETY FUNCTION
24590-PTF-3PS-PPJ-T0002	SSRS for C5 Cell Depression	C5 Fan Interlocks	Low flow set fan to set speed. Low low flow start Train if not running
24590-PTF-3PS-PPJ-T0003	SSRS for Pressurization of FEP Wash Rack	FEP Wash Rack pressurization	Prevent simultaneous opening of two pairs of valves
24590-PTF-3PS-PPJ-T0004	SSRS for Forced Purge	Hydrogen purge of Separator/Evaporators	If individual flows below setpoint open valve
24590-PTF-3PS-PPJ-T0004	SSRS for Forced Purge	Hydrogen purge of high consequence vessels	Low flow alarm only; operator action
24590-PTF-3PS-PPJ-T0004	SSRS for Forced Purge	Hydrogen sparge of non-Newtonian vessels	Low flow alarm only; operator action
24590-PTF-3PS-PPJ-T0005	SSRS for Seismic Isolation	Seismic Isolation	Manual activation to close approximately 20 valves
24590-PTF-3PS-PPJ-T0006	SSRS for PVV HEPAs	PVV HEPA Bank	Protect PVV HEPAs
24590-PTF-3PS-PPJ-T0008	SSRS for LAW Gamma Monitor Interlock for TCP-VSL-00001	LAW Concentrate Vessel Gamma Monitor and interlock	High gamma close 2 valves
24590-PTF-3PS-PPJ-T0009	SSRS for Cs IX H2 system	H2 system for Cs IX Column 1, 2, 3, and 4	Gas or liquid / gas for set time to open two valves
24590-PTF-3PS-PPJ-T0010	SSRS for Safety Design Class Electrical Power	Emergency Diesel Generator Load Sequence	Maintain electrical power to ITS equipment
24590-PTF-3PS-PPJ-T0012	SSRS for ITS Air Supply	ITS Air Supply	Maintain ITS power supply
24590-PTF-3PS-PPJ-T0013	SSRS for Cs IX Columns Emergency Elution (Temperature)	Cs IX Columns Elution Initiation Detection and Alarm for Column 1,2,3, & 4	Prevent a resin bed fire

Table 1 - PTF Safety Instrumented Systems

SSRS DOC	SSRS TITLE	FUNCTION TITLE	SAFETY FUNCTION
24590-PTF-3PS-PPJ-T0014	SSRS for Pretreatment Accident Monitoring	Pretreatment Accident Monitoring	Indication of variables required for safe shut down monitoring
24590-PTF-3PS-PPJ-T0016	SSRS For evaporator and separator level interlocks	Evaporator high level interlocks	Prevent overflow by shutting off significant sources (high level close inlet valves - 9 off)
24590-PTF-3PS-PPJ-T0016	SSRS For evaporator and separator level interlocks	Separator High level interlocks	Prevent overflow by shutting off significant sources (high level close two inlet valves)
24590-PTF-3PS-PPJ-T0018	SSRS For solids mixing	PJM mixing of hydrogen generating vessels	Prevent headspace H2 concentration from reaching LFL
24590-PTF-3PS-PPJ-T0018	SSRS For solids mixing	Evaporator / Separator recovery	Drain vessels to maintain H2 concentration from reaching LFL
24590-PTF-3PS-PPJ-T0021	SSRS for Ultimate Overflow vessel High-High Level alarm	Ultimate Overflow High Level Alarm	High level alarm - operator response is to activate manual activation of transfer piping and process piping interlocks
24590-PTF-3PS-PPJ-T0023	SSRS for Cx IX backflow	Isolation of high activity from Cs IX 1,2, 3, and 4 into C3/R3 areas	Prevent radiation exposure to facility worker
24590-PTF-3PS-PPJ-T0024	SSRS for Cesium Ion Exchange Treated LAW Collection Vessels Gamma Monitor and Interlock	Cesium Ion Exchange LAW Collection Gamma Interlock	Prevent radiation exposure to facility worker
24590-PTF-3PS-PPJ-T0025	SSRS for UFP Pulse Pot	UFP Backflow Prevention	Prevent radiation exposure to facility worker

Table 1 - PTF Safety Instrumented Systems

SSRS DOC	SSRS TITLE	FUNCTION TITLE	SAFETY FUNCTION
24590-PTF-3PS-PPJ-T0026	SSRS for Over pressurization of PVP (C5 TO C3 contamination)	SSRS PVP overpressurization	Prevent contamination migration while PVV is not operating. (High pressure in scrubber closes 6 inlet valves)
24590-PTF-3PS-PPJ-T0027	SSRS for Non-Newtonian Overflow	non-Newtonian high level interlocks	Prevent non-Newtonian from overflowing into vessels that are not able to mix non-Newtonian waste
24590-PTF-3PS-PPJ-T0028	SSRS for Anti-foam addition	Anti foam addition	Add anti-foam to non-Newtonian waste. (To allow manual activation after seismic event to open 2 valves for 5 vessels)
24590-PTF-3PS-PPJ-T0029	SSRS for C1V Flow	Maintain Control room pressurized	Maintain control room pressurized
24590-PTF-3PS-PPJ-T0029	SSRS for C1V Main Control Room Cooling water (temp)	Main Control Room Ventilation Systems	Maintain control room habitable

Table 2 - HLW Safety Instrumented Systems

SSRS DOC	SSRS TITLE	FUNCTION TITLE
24590-HLW-3PS-PPJ-T0001	SSRS for C5 Area Ventilation Exhaust	C5V Fan Flow Interlocks to Maintain Cascade Ventilation
24590-HLW-3PS-PPJ-T0001	SSRS for C5 Area Ventilation Exhaust	C5V HEPA Filter High Differential Pressure Protection Interlocks
24590-HLW-3PS-PPJ-T0002	SSRS for C3 Canister Storage Area Ventilation	C3V Canister Fan Flow Interlocks
24590-HLW-3PS-PPJ-T0003	SSRS for Hydrogen Mitigation Purge and Sparge	RLD-VSL-00008, Melter Feed and Melter Feed Preparation Vessels Hydrogen Purge Flow
24590-HLW-3PS-PPJ-T0003	SSRS for Hydrogen Mitigation Purge and Sparge	Melter Feed and Melter Feed Preparation Vessels Sparge on Loss of Agitator Mixing
24590-HLW-3PS-PPJ-T0004	SSRS for EDG HLW Load Sequencing	HLW Electrical Load Sequencing of Emergency Diesel Generator Power
24590-HLW-3PS-PPJ-T0005	SSRS for Mechanical Interlocks	Canister Export Handling: Hatch HEH-HTCH-00002 Gamma Interlock
24590-HLW-3PS-PPJ-T0005	SSRS for Mechanical Interlocks	Radioactive Solid Waste Handling: Hatch RWH-HTCH-00001 and Horizontal Shield Door RWH-DOOR-00004 Door and Gamma Interlocks
24590-HLW-3PS-PPJ-T0006	SSRS for Posting Ports	Posting Port Door Interlocks for HDH-TWDVC-00002, HPH-TWDVC-00009, HSH-TWDVC-00001, HSH-TWDVC-00002 and RWH-SMPLR-00001
24590-HLW-3PS-PPJ-T0007	SSRS for High-High Liquid Level Control	Autosamplers High-High Liquid Level Feed Pumps Interlocks
24590-HLW-3PS-PPJ-T0007	SSRS for High-High Liquid Level Control	Melter Feed Preparation Vessels High-High Liquid Level Feed Interlock
24590-HLW-3PS-PPJ-T0008	SSRS for Offgas Treatment System	HOP Fan Automatic Switchover
24590-HLW-3PS-PPJ-T0008	SSRS for Offgas Treatment System	HOP HEPA Filter Preheater Interlocks
24590-HLW-3PS-PPJ-T0008	SSRS for Offgas Treatment System	Carbon Bed Fire Protection
24590-HLW-3PS-PPJ-T0009???	SSRS for HLW Accident Monitoring	HLW Accident Monitoring

Table 3 - LAW Safety Instrumented Systems

SSRS DOC	SSRS TITLE	FUNCTION TITLE
24590-LAW-3PS-PPJ-T0001	SSRS for Melter Plenum Pressure Interlocks	Melter 1 pressure interlocks
24590-LAW-3PS-PPJ-T0001	SSRS for Melter Plenum Pressure Interlocks	Melter 2 pressure interlocks
24590-LAW-3PS-PPJ-T0002	SSRS for LAW Wet Electrostatic Precipitator High Level Interlocks	Melter 1 Wet electrostatic precipitator high level interlock
24590-LAW-3PS-PPJ-T0002	SSRS for LAW Wet Electrostatic Precipitator High Level Interlocks	Melter 2 Wet electrostatic precipitator high level interlock
24590-LAW-3PS-PPJ-T0003	SSRS for LAW Submerged Bed Scrubber Level Instrumentation	Melter 1 scrubber high level interlocks
24590-LAW-3PS-PPJ-T0003	SSRS for LAW Submerged Bed Scrubber Level Instrumentation	Melter 1 scrubber low level interlocks
24590-LAW-3PS-PPJ-T0003	SSRS for LAW Submerged Bed Scrubber Level Instrumentation	Melter 2 scrubber high level interlocks
24590-LAW-3PS-PPJ-T0003	SSRS for LAW Submerged Bed Scrubber Level Instrumentation	Melter 2 scrubber low level interlocks
24590-LAW-3PS-PPJ-T0004	SSRS for LAW Caustic Scrubber Differential Pressure Interlocks	Caustic scrubber high differential pressure interlock
24590-LAW-3PS-PPJ-T0005	SSRS for LAW Catalytic Oxidizer/Reducer	Catalytic Oxidizer/Reducer differential pressure interlock
24590-LAW-3PS-PPJ-T0006	SSRS for Mercury Abatement Skid Interlocks	Mercury Abatement High temperature interlock
24590-LAW-3PS-PPJ-T0006	SSRS for Mercury Abatement Skid Interlocks	Mercury Abatement High Differential pressure interlock
24590-LAW-3PS-PPJ-T0006	SSRS for Mercury Abatement Skid Interlocks	Mercury Abatement Carbon monoxide and dioxide interlocks
24590-LAW-3PS-PPJ-T0006	SSRS for Mercury Abatement Skid Interlocks	Mercury Abatement High level interlock

Table 3 - LAW Safety Instrumented Systems

SSRS DOC	SSRS TITLE	FUNCTION TITLE
24590-LAW-3PS-PPJ-T0007	SSRS for Melter Off Gas System: HEPA Preheater and HEPA filters	Loss of temperature differential across HEPA preheaters sets melter 1 and 2 to idle
24590-LAW-3PS-PPJ-T0007	SSRS for Melter Off Gas System: HEPA Preheater and HEPA filters	High differential across HEPA filters
24590-LAW-3PS-PPJ-T0008	SSRS for Melter Off gas System Reconfiguration Interlocks	Melter offgas reconfiguration on loss of power
24590-LAW-3PS-PPJ-T0009	SSRS for Ammonia	Ammonia Supply system high pressure interlocks
24590-LAW-3PS-PPJ-T0009	SSRS for Ammonia	Ammonia supply tank fill interlocks
24590-LAW-3PS-PPJ-T0010	SSRS for LAW Accident Monitoring	Required monitoring after accident in LAW facility

Figure 1 - SIS within the WTP Control System

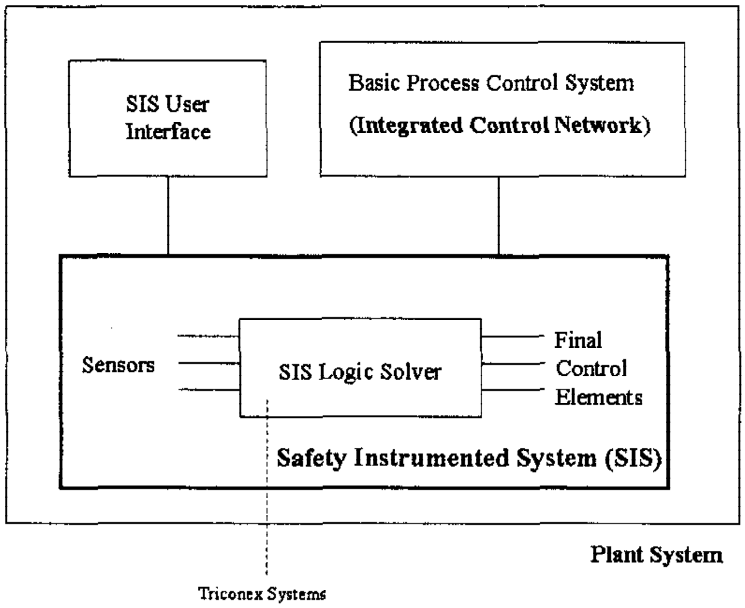
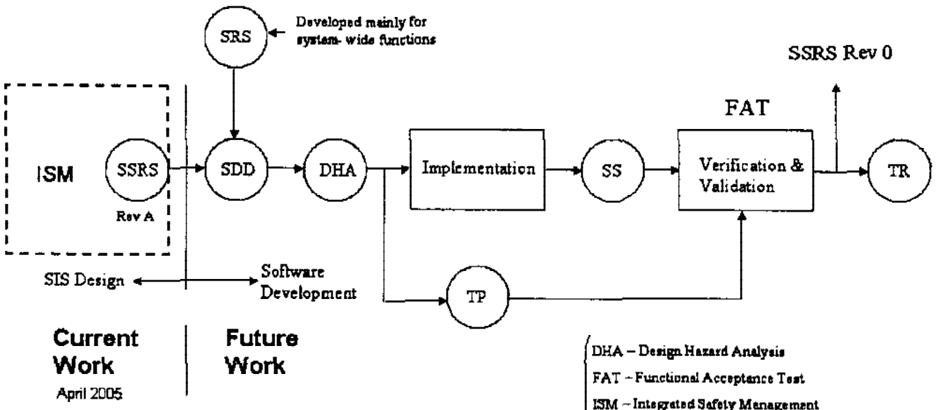


Figure 2 - Typical SIS Life Cycle Document Flow



SSRS Development is defined according to *Design Guide for Safety Instrumented Systems Implementation* (24590-WTP-GPG-J-015)

Software Development is defined according to *Software Project Plan for Programmable Protection System* (24590-WTP-PL-J-01-004)

DHA – Design Hazard Analysis
FAT – Functional Acceptance Test
ISM – Integrated Safety Management
SDD – Software Design Document
SIS – Safety Instrumented System
SRS – Software Requirements Specification
SS – System Software
SSRS – Safety Systems Requirements Specification
TP – Test Plan
TR – Test Report

Task# ORP-WTP-2005-0120

E-STARS^{TM} Report
Task Detail Report
05/13/2005 0859

TASK INFORMATION

Task#	ORP-WTP-2005-0120		
Subject	CONCUR: (05-WED-020) DOE ORP DESIGN OVERSIGHT ASSESSMENT REPORT ON THE PROGRAMMABLE PROTECTION SYSTEM (PPJ) (D-05-DESIGN-012)		
Parent Task#		**Status**	CLOSED
Reference	05-WED-020	**Due**	
Originator	Almaraz, Angela	**Priority**	High
Originator Phone	(509) 376-9025	**Category**	None
Origination Date	05/02/2005 1303	**Generic1**	
Remote Task#		**Generic2**	
Deliverable	None	**Generic3**	
Class	None	**View Permissions**	Normal
Instructions	Hard copy of the correspondence is being routed for concurrence. Once you have reviewed the correspondence, please approve or disapprove via E-STARS and route to the next person on the list. Thank you. bcc: MGR RDG File WTP OFF File J. J. Short, OPA W. F. Hamel, WED M. L. Ramsay, WED J. R. Eschenberg, WTP		

ROUTING LISTS

1	Route List	Inactive

- Ramsay, Mark L - Review - Concur with comments - 05/11/2005 1616
  Instructions:
- Hamel, William F - Review - Concur with comments - 05/11/2005 1617
  Instructions:
- Eschenberg, John R - Review - Concur with comments - 05/11/2005 1617
  Instructions:
- Schepens, Roy J - Approve - Approved with comments - 05/13/2005 0812
  Instructions:
- Miller, Lewis F - Review - Concur with comments - 05/11/2005 1618
  Instructions:

ATTACHMENTS

Attachments

1. 05-WED-020.MLR.Attach PPJ Assessment Rpt.doc
2. 05-WED-020.MLR.Design Oversight Rpt D-05-DESIGN-012.doc

COLLABORATION

COMMENTS

Task# ORP-WTP-2005-0120

Poster	Ramsay, Mark L (Almaraz, Angela) - 05/11/2005 0405
	Concur
	Mark signed the hard copy on 5/2/05.
Poster	Hamel, William F (Almaraz, Angela) - 05/11/2005 0405
	Concur
	Bill signed the hard copy on 5/2/05.
Poster	Eschenberg, John R (Almaraz, Angela) - 05/11/2005 0405
	Concur
	John signed the hard copy on 5/11/05.
Poster	Miller, Lewis F (Almaraz, Angela) - 05/11/2005 0405
	Concur
	Lew signed the hard copy on 5/10/05.
Poster	Schepens, Roy J (Poynor, Cathy D) - 05/13/2005 0805
	Approve
	signed by Shirley Olinger for Roy Schepens

TASK DUE DATE HISTORY

No Due Date History

SUB TASK HISTORY

No Subtasks

-- end of report --

Task# ORP-WTP-2005-0120

E-STARS™ Report
Task Detail Report
05/09/2005 1246

TASK INFORMATION

Task#	ORP-WTP-2005-0120		
Subject	CONCUR: (05-WED-020) DOE ORP DESIGN OVERSIGHT ASSESSMENT REPORT ON THE PROGRAMMABLE PROTECTION SYSTEM (PPJ) (D-05-DESIGN-012)		
Parent Task#		**Status**	Open
Reference	05-WED-020	**Due**	
Originator	Almaraz, Angela	**Priority**	High
Originator Phone	(509) 376-9025	**Category**	None
Origination Date	05/02/2005 1303	**Generic1**	
Remote Task#		**Generic2**	
Deliverable	None	**Generic3**	
Class	None	**View Permissions**	Normal

Instructions

Hard copy of the correspondence is being routed for concurrence. Once you have reviewed the correspondence, please approve or disapprove via E-STARS and route to the next person on the list. Thank you.

bcc:
MGR RDG File
WTP OFF File
J. J. Short, OPA
W. F. Hamel, WED
M. L. Ramsay, WED
J. R. Eschenberg, WTP

ROUTING LISTS

1	Route List	Active

- Ramsay, Mark L - Review - Awaiting Response
  Instructions:
  See previous concurrence
- Hamel, William F - Review - Awaiting Response
  Instructions:
  See previous concurrence
- Eschenberg, John R - Review - Awaiting Response
  Instructions:
  8/11 OL
- Schepens, Roy J - Approve - Awaiting Response
  Instructions:
  for SDO 5/12
- Miller, Lewis F - Review - Awaiting Response
  Instructions:
  5-10-05

ATTACHMENTS

Attachments
1. 05-WED-020.MLR.Attach PPJ Assessment Rpt.doc
2. 05-WED-020.MLR.Design Oversight Rpt D-05-DESIGN-012.doc

COLLABORATION

COMMENTS

Task# ORP-WTP-2005-0120

E-STARS^{TM} Report
Task Detail Report
05/02/2005 0108

TASK INFORMATION

Task#	ORP-WTP-2005-0120		
Subject	CONCUR: (05-WED-020) DOE ORP DESIGN OVERSIGHT ASSESSMENT REPORT ON THE PROGRAMMABLE PROTECTION SYSTEM (PPJ) (D-05-DESIGN-012)		
Parent Task#		**Status**	Open
Reference	05-WED-020	**Due**	
Originator	Almaraz, Angela	**Priority**	High
Originator Phone	(509) 376-9025	**Category**	None
Origination Date	05/02/2005 1303	**Generic1**	
Remote Task#		**Generic2**	
Deliverable	None	**Generic3**	
Class	None	**View Permissions**	Normal

Instructions

Hard copy of the correspondence is being routed for concurrence. Once you have reviewed the correspondence, please approve or disapprove via E-STARS and route to the next person on the list. Thank you.

bcc:
MGR RDG File
WTP OFF File
J. J. Short, OPA
W. F. Hamel, WED
M. L. Ramsay, WED
J. R. Eschenberg, WTP

ROUTING LISTS

1 Route List Active

- Ramsay, Mark L - Review - Awaiting Response
  Instructions:
  5/2/05
- Hamel, William F - Review - Awaiting Response
  Instructions:
  5/2/05
- Eschenberg, John R - Review - Awaiting Response
  Instructions:
  5-3-05
- Schepens, Roy J - Approve - Awaiting Response
  Instructions:

ATTACHMENTS

Attachments
1. 05-WED-020.MLR.Attach PPJ Assessment Rpt.doc
2. 05-WED-020.MLR.Design Oversight Rpt D-05-DESIGN-012.doc

COLLABORATION

COMMENTS

No Comments

TASK DUE DATE HISTORY