INL/EXT-05-00810

US-CERT Control System Center Input/Output (I/O) Conceptual Design

David G. Kuipers

February 2005

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-05-00810

US-CERT Control System Center Input/Output (I/O) Conceptual Design

David G. Kuipers

February 2005

US-CERT Control Systems Security Center
Idaho Falls, Idaho 83415

Prepared for the
U.S. Department of Homeland Security
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

US-CERT Control System Center

I/O Conceptual Design

February 2005

Approved by:

David G. Kuipers, Author Critical Infrastructure Assurance BEA	Date
Fred C. Cowart, Program Manager Control Systems Security and Test Center BEA	Date
Julio G. Rodriguez, Department Manager Critical Infrastructure Assurance BEA	Date

Input/Output (I/O) Conceptual Design

Introduction

This document was prepared for the US-CERT Control Systems Center of the National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS). DHS has been tasked under the Homeland Security Act of 2002 to coordinate the overall national effort to enhance the protection of the national critical infrastructure. *Homeland Security Presidential Directive HSPD-7* directs the federal departments to identify and prioritize critical infrastructure and protect it from terrorist attack. The *US-CERT National Strategy for Control Systems Security* was prepared by the NCSD to address the control system security component addressed in the *National Strategy to Secure Cyberspace* and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. The *US-CERT National Strategy for Control Systems Security* identified five high-level strategic goals for improving cyber security of control systems; the I/O upgrade described in this document supports these goals.

The vulnerability assessment Test Bed, located in the Information Operations Research Center (IORC) facility at Idaho National Laboratory (INL), consists of a cyber test facility integrated with multiple test beds that simulate the nation's critical infrastructure. The fundamental mission of the Test Bed is to provide industry owner/operators, system vendors, and multi-agency partners of the INL National Security Division a platform for vulnerability assessments of control systems.

The Input/Output (I/O) upgrade to the Test Bed (see Work Package 3.1 of the FY-05 Annual Work Plan) will provide for the expansion of assessment capabilities within the IORC facility. It will also provide capabilities to connect test beds within the Test Range and other Laboratory resources. This will allow real time I/O data input and communication channels for full replications of control systems (Process Control Systems [PCS], Supervisory Control and Data Acquisition Systems [SCADA], and components). This will be accomplished through the design and implementation of a modular infrastructure of control system, communications, networking, computing and associated equipment, and measurement/control devices.

The architecture upgrade will provide a flexible patching system providing a quick "plug and play" configuration through various communication paths to gain access to live I/O running over specific protocols. This will allow for in-depth assessments of control systems in a true-to-life environment.

The full I/O upgrade will be completed through a two-phased approach. Phase I, funded by DHS, expands the capabilities of the Test Bed by developing an operational control system in two functional areas, the Science & Technology Applications Research (STAR) Facility and the expansion of various portions of the Test Bed. Phase II (see Appendix A), funded by other programs, will complete the full I/O upgrade to the facility.

Phase I Project Description

The Phase I activity supports expansion of two portions of the Test Bed, the STAR Facility, and the Test Bed at the IORC.

- STAR Facility

  Improvements are in-process at the STAR Facility to add I/O and advanced testing capability to multiple process control sector-specific applications. Communications have been established between the IORC and STAR facilities and will be expanded in Phase I to incorporate a representative business and control system network, and a sector-specific process mockup providing a complete and flexible test environment.

- Test Bed at the IORC

  Improvements will support SCADA applications related to power generation, transmission, and distribution configurations. In the test bays, process or SCADA control systems can be connected to various types and brands of controllers (RTUs, PLCs, and IEDs) using a variety of communications systems and protocols. This activity will include installation of modem (leased-line) and direct-link serial communications and various LAN configurations for Ethernet with multiple protocols available as needed.

Upon completion of Phase I, the increased capabilities at the IORC Test Bed will allow for the mock-up of a complete infrastructure that is configured to represent a SCADA implementation. The network design architecture (specific for control systems) will have a point of presence on the internet that is protected via a firewall. Behind the firewall will be the business/corporate network that has a directly connected SCADA network, also secured via a firewall. With this infrastructure in place, validation assessments of a specific system can be conducted using the security objectives defined in the control systems security framework. The STAR Facility will also be utilized to conduct system mock-ups for US-CERT support.

STAR Facility Description

The STAR Facility provides a flexible control system infrastructure for mockup and configuration of various sector-specific process systems for meeting cross-sector testing requirements. Currently available at the STAR Facility are extensive instrumentation and control elements as a state-of-the-art control and data acquisition system from Rockwell Automation.

The design of the existing STAR Facility pilot plant process and control system is modular, which ensures that it can be reconfigured quickly both in scale and function to meet a wide variety of testing needs. Using the existing infrastructure of the Test Bed and parts that have been salvaged from the INL site, as well as new or donated equipment, the STAR Facility has the ability to rapidly mock-up working systems for a variety of cross-sector applications.

The Mix/Feed Tanks unit operation will be reconfigured so that it can support both the existing function it serves as part of the fluidized bed pilot plant, and a new process that incorporates batch mixing with tank-level pump control. The Mix/Feed Tanks unit operation will become a "plug and play" process that can be used with almost any control system to perform a specific set of operations using defined instrumented inputs and controlled outputs, as well as specified control logic and operator interface screens. This "plug and play" system will provide a controlled and repeatable environment for conducting cyber vulnerability assessments of different control systems.

Figure 1 provides a process flow diagram for the entire fluidized-bed pilot plant as configured for a waste treatment operation.

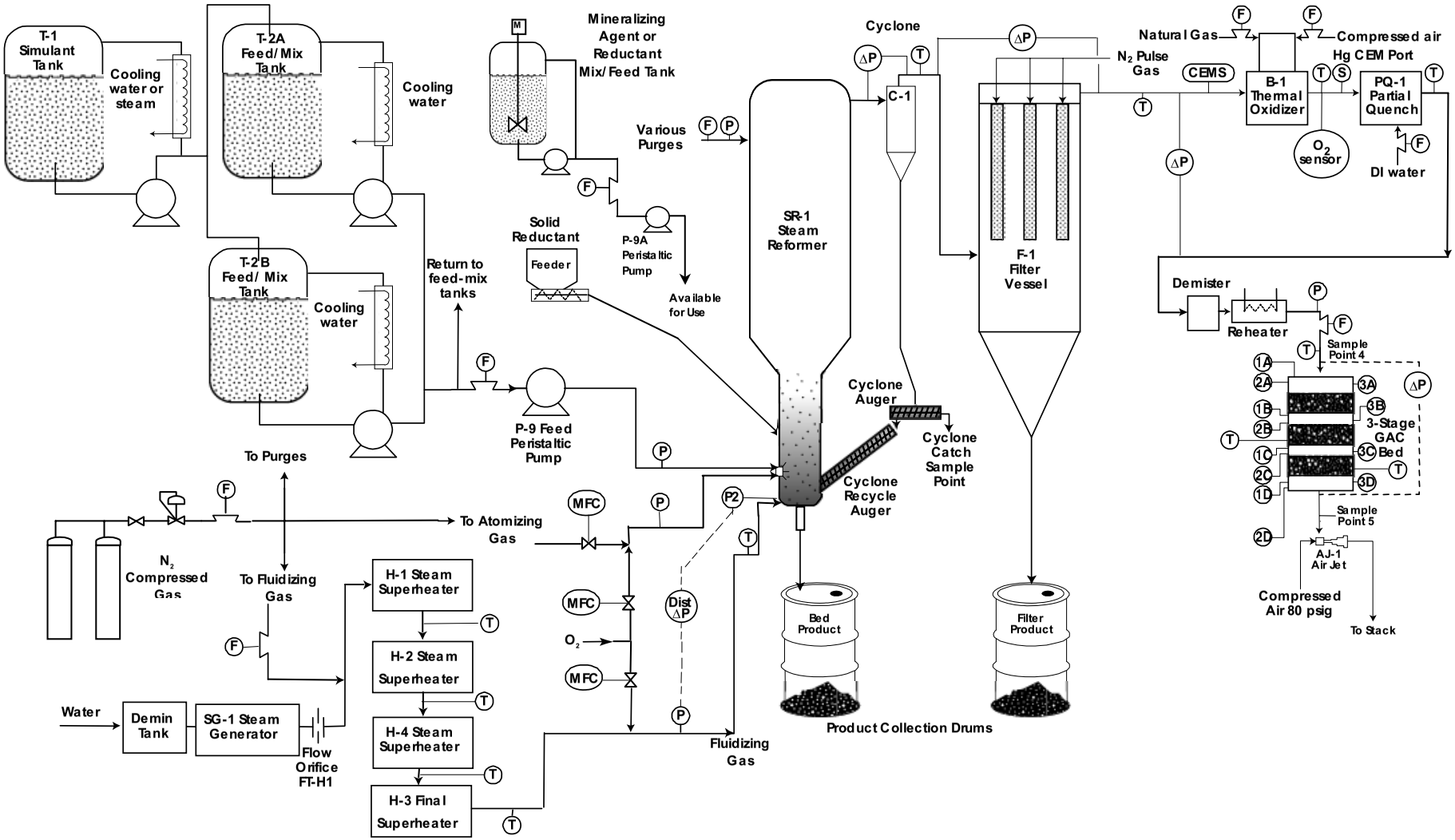

Figure 1. Entire fluidized-bed pilot plant as configured for a waste treatment operation.

Figure 2 is a simplified process flow diagram that shows just the Mix/Feed Tanks unit operation of the overall fluidized-bed pilot plant as configured for a waste treatment operation. In this configuration, the Mix/Feed Tanks unit operation consists of three stainless steel tanks with electronic level indication that are used for waste simulant storage and make-up. Three manually controlled pumps are used to recirculate the simulant and transfer it to the peristaltic feed pump system.

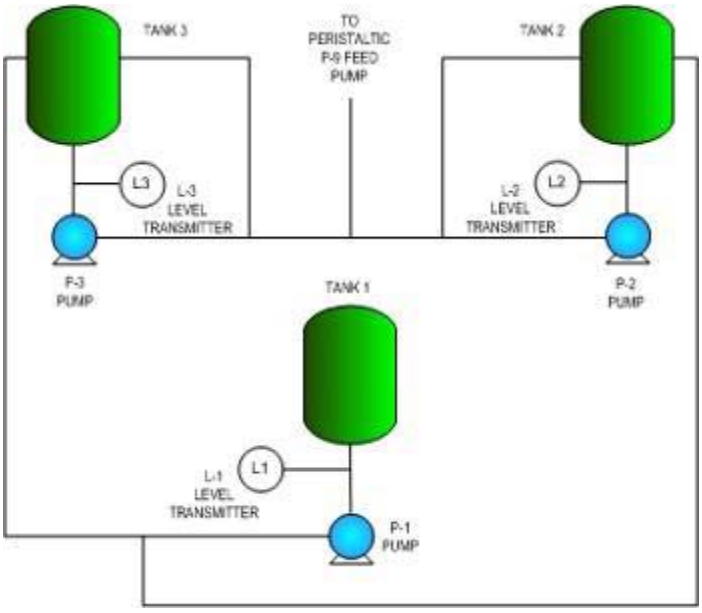

Figure 2. Mix/Feed Tanks unit operation as configured for a waste treatment operation.

Figure 3 is a simplified process flow diagram that shows just the Mix/Feed Tanks unit operation of the overall fluidized-bed pilot plant as configured for a process that incorporates batch mixing with tank-level pump control. This requires the addition of remote controlled motor starters for the three pumps, two flow meters, two control valves, and a remote actuated three-way valve. The control and data acquisition system from Rockwell Automation will be used to generate a control program for the process that will incorporate an automatic sequential batch process, safety and equipment protection interlocks, and a manual operation mode.

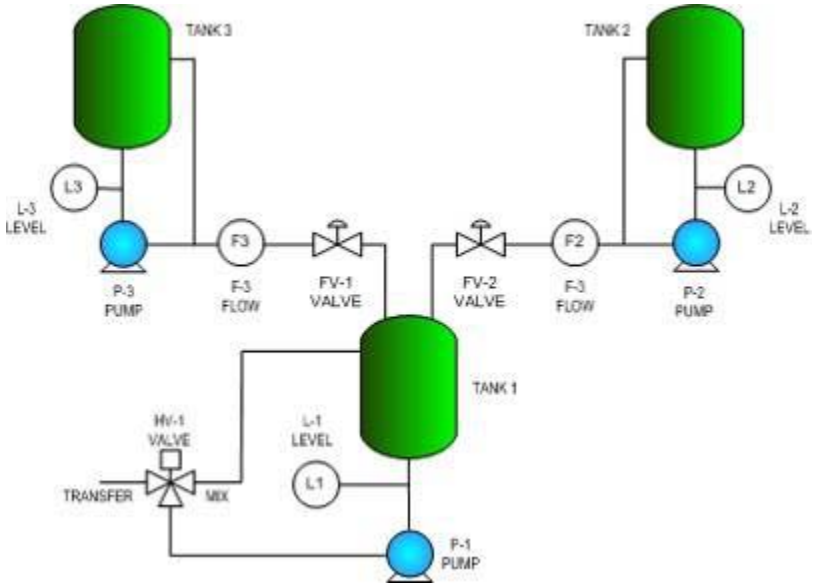

Figure 3. Mix/Feed Tanks unit operation as configured for a batch mixing test operation.

To make the system “plug and play,” the following features have been incorporated:

- The Mix/Feed Tanks unit operation will be isolated from the rest of the system so that it can be operated independently.
- The instrumentation and control elements for the Mix/Feed Tanks unit operation will be wired so that different controller hardware can be easily hooked up.
- A standard package of documentation will be generated that includes drawings, equipment protection/operational limits, control logic and interlocks, the Human Machine Interface, and a System Operability Test.

Test Bed at the IORC Description

The IORC Test Bed test area provides a testing environment for component and system-level testing. The emulators currently installed and being added by this activity provides a diverse testing environment in support of the several sectors (e.g., electrical utility) and Test Bed activities. The communications configuration can be configured for either SCADA or process-oriented control system applications using the same types of communications architectures. The configuration provides the flexibility to modify the communications scheme as needed for customer-specified application requirements.

Modular communications patch panels will be installed in four test cubicles at the IORC facility. The patch panels will be fitted with serial and Ethernet connection modules. The patch-panel modules will be hardwired to a new Front End Communications Panel (see Figure 4).

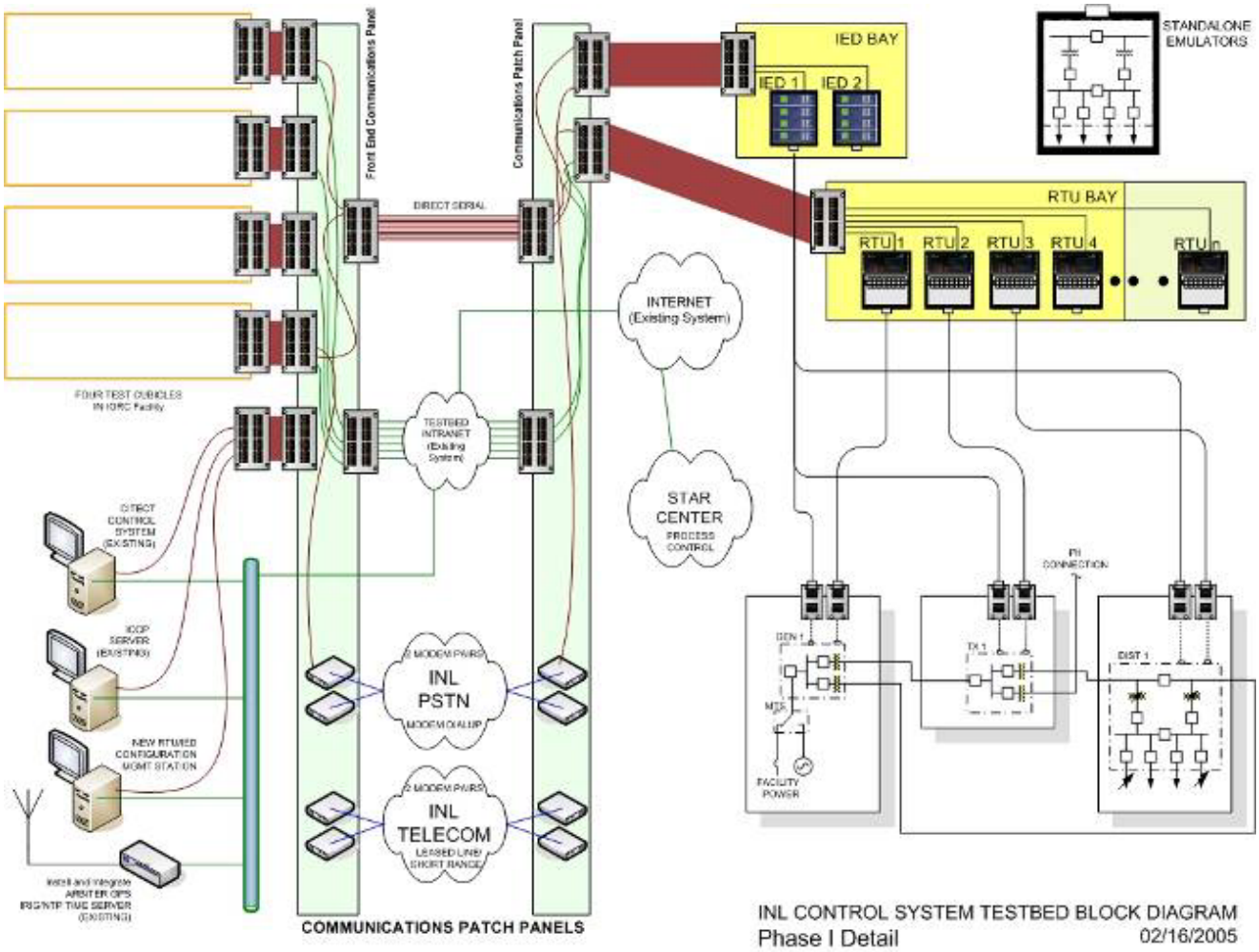

Figure 4. Phase I IORC Configuration.

An emulator system is provided by three interconnected emulator units. The electrical utility emulators include an electrical power generation unit, a power distribution unit, and a power transmission unit. These emulation units provide remote and local status and control as well as analog metering data specific to the subsystems. A standalone emulator unit will provide remote and local operation and status of a typical electrical distribution substation. Test Center cubicles may also communicate with STAR Facility process control system equipment. For Phase I, test cubicles will be available at the STAR Facility to provide high-speed local communications with the process control system assets.

Three existing RTU controllers will be mounted into new modular housings with associated I/O interface configuration hardware installed with this activity. A test customer may utilize communications to an existing IED test bay directly for analog monitoring of the connected emulator unit or access analog data via an RTU or other type of new or existing controller unit. The IED test bays will be modified to improve the plug-and-play capability with the new emulation units.

An existing ICCP server will be integrated with the Test Center communications systems to allow communications with multiple cubicles and an existing Citect control system. Additional Test Center computing system assets will be integrated as needed to accomplish specific testing configurations. The existing Citect Control System will also be integrated into the Test Center to support ICCP system communications and data sourcing, additional test system data generation and control applications, and other test objectives. The Citect system will be used to support process control and SCADA applications as needed. The system can be configured to support multiple configurations simultaneously. The Citect application provides native driver support for many protocols used across multiple sectors.

Schedule

The Phase I activity includes two milestones as defined in the FY-05 Annual Work Plan. The first deliverable is this conceptual design.

The second milestone is the completion of the Phase I I/O upgrade by June 30, 2005.

Budget

A cost estimate was developed for the Phase I activity based on a conceptual design. This estimate was used as the basis for allocating CSSTC program funding to support the Phase I activity. The cost estimate is provided in the following worksheets.

Cost Estimate for STAR Facility Modifications

Project Cost Estimate Worksheet – Vulnerability Assessment Center - Phase 1 STAR Facility								
	DESCRIPTION	MATERIALS/NONLABOR			DIRECT LABOR			MATERIALS & LABOR
ITEM		QTY	UNIT PRICE	SUBTOTAL	HOURS	RATE	SUBTOTAL	SUBTOTAL
1	**EQUIPTMENT PROCUREMENT**							
	- Labor				25	$100.00	$2,500.00	$2,500.00
	- Magnetic Starters	1	$800.00	$800.00			$0.00	$800.00
	- Control Valves	1	$7,450.00	$7,450.00			$0.00	$7,450.00
	- Flow Meters	1	$6,000.00	$6,000.00			$0.00	$6,000.00
	- PLC Control Cards	1	$1,800.00	$1,800.00			$0.00	$1,800.00
	- PLC Control Cables	1	$1,250.00	$1,250.00			$0.00	$1,250.00
	- Test Cart Materials	1	$700.00	$700.00			$0.00	$700.00
	- Misc. Pipe/Flanges	1	$3,500.00	$3,500.00			$0.00	$3,500.00
	SUBTOTALS			**$21,500.00**	**25**		**$2,500.00**	**$24,000.00**
2	**SYSTEM PREPERATION**							
	- Mechanical Installation			$0.00	40	$100.00	$4,000.00	$4,000.00
	- Electrical and Control Installation			$0.00	60	$100.00	$6,000.00	$6,000.00
	SUBTOTALS			**$0.00**	**100**		**$10,000.00**	**$10,000.00**
3	**DOCUMENTATION PREPERATION**							
	- Develop HMI Requirements			$0.00	20	$100.00	$2,000.00	$2,000.00
	- Develop Logic Requirements			$0.00	10	$100.00	$1,000.00	$1,000.00
	- Drawings and I/O list			$0.00	10	$100.00	$1,000.00	$1,000.00
	- Identify Equipment Protection/Operational Limits			$0.00	20	$100.00	$2,000.00	$2,000.00
	- Develop SO test Requirements			$0.00	20	$100.00	$2,000.00	$2,000.00
	SUBTOTALS			**$0.00**	**80**		**$8,000.00**	**$8,000.00**

Project Cost Estimate Worksheet – Vulnerability Assessment Center Test Beds - Phase 1 STAR Facility								
	DESCRIPTION	MATERIALS/NONLABOR			DIRECT LABOR			MATERIALS & LABOR
ITEM		QTY	UNIT PRICE	SUBTOTAL	HOURS	RATE	SUBTOTAL	SUBTOTAL
4	**PROJECT MANAGEMENT/PROJECT CONTROLS**							
	- Labor			$0.00	20	$100.00	$2,000.00	$2,000.00
	SUBTOTALS			**$0.00**	**20**		**$2,000.00**	**$2,000.00**
5	**BEA SUBCONTRACT**							
	- Labor			$0.00	80	$120.00	$9,600.00	$9,600.00
	SUBTOTALS			**$0.00**	**80**		**$9,600.00**	**$9,600.00**
			MATERIAL SUBTOTAL	**$21,500.00**		**DIRECT LABOR SUBTOTAL**	**$32,100.00**	
					305			
		PROJECT SUBTOTAL					**$53,600.00**	
		CONTINGENCY			**5%**	**$53,600.00**	**$2,680.00**	
		ESTIMATED TOTAL PROJECT COST					**$56,280.00**	

Cost Estimate for IORC Vulnerability Assessment Center Modifications:

PROJECT COST ESTIMATE WORKSHEET -- VULNERABILITY ASSESSMENT CENTER TEST BEDS--PHASE I								
ITEM	DESCRIPTION	MATERIALS/NONLABOR			DIRECT LABOR			MATERIALS & LABOR
		QTY	UNIT PRICE	SUBTOTAL	HOURS	RATE	SUBTOTAL	SUBTOTAL
1	**INTEGRATE EXISTING RTUs (3 ea.)**							
	- Engineering/Design/Order materials			$0.00	54	$120.00	$6,480.00	$6,480.00
	- Materials	3	$900.00	$2,700.00			$0.00	$2,700.00
	- Fabrication			$0.00	210	$90.00	$18,900.00	$18,900.00
	- Programming/software integration			$0.00	81	$120.00	$9,720.00	$9,720.00
	SUBTOTALS			**$2,700.00**	**345**		**$35,100.00**	**$37,800.00**
2	**BUILD INTEGRATED EMULATION ENVIRONMENT**							
	- Detailed design and engineering oversight				280	$120.00	$33,600.00	$33,600.00
	- Build distribution substation	1	$5,200.00	$5,200.00	90	$90.00	$8,100.00	$13,300.00
	- Build transmission substation	1	$3,600.00	$3,600.00	70	$90.00	$6,300.00	$9,900.00
	- Build generation substation	1	$4,000.00	$4,000.00	70	$90.00	$6,300.00	$10,300.00
	- Build termination panel	1	$5,800.00	$5,800.00	180	$90.00	$16,200.00	$22,000.00
	- Interconnect and test equipment	1	$2,400.00	$2,400.00	120	$120.00	$14,400.00	$16,800.00
	- Integrate software simulator (assumes hardware and software provided by others)				160	$120.00	$19,200.00	$19,200.00
	SUBTOTALS			**$21,000.00**	**600**		**$104,100.00**	**$125,100.00**
3	**BUILD STANDALONE EMULATOR**							
	- Engineering/Design/Order materials			$0.00	18	$120.00	$2,160.00	$2,160.00
	- Materials	1	$1,000.00	$1,000.00			$0.00	$1,000.00
	- Fabrication			$0.00	80	$90.00	$7,200.00	$7,200.00
	SUBTOTALS			**$1,000.00**	**98**		**$9,360.00**	**$10,360.00**
4	**ADD CABINETS AND PATCHING CAPABILITY**							
	- Cabinets and miscellaneous hardware	2	$4,000.00	$8,000.00			$0.00	$8,000.00
	- Patching hardware and cables	1	$4,800.00	$4,800.00			$0.00	$4,800.00
	- Fabrication			$0.00	160	$90.00	$14,400.00	$14,400.00
	- Design/configuration			$0.00	60	$120.00	$7,200.00	$7,200.00
	SUBTOTALS			**$12,800.00**	**220**		**$21,600.00**	**$34,400.00**

PROJECT COST ESTIMATE WORKSHEET -- VULNERABILITY ASSESSMENT CENTER TEST BEDS--PHASE I								
ITEM	DESCRIPTION	MATERIALS/NONLABOR			DIRECT LABOR			MATERIALS & LABOR
		QTY	UNIT PRICE	SUBTOTAL	HOURS	RATE	SUBTOTAL	SUBTOTAL
5	**PROVIDE PLATFORM FOR PROGRAMMING/CONFIG. MGMT**							
	- Workstations	2	$2,000.00	$4,000.00			$0.00	$4,000.00
	- Develop configuration management plan			$0.00	60	$120.00	$7,200.00	$7,200.00
	- Implement config. Mgmt. Plan			$0.00	60	$120.00	$7,200.00	$7,200.00
	SUBTOTALS			**$4,000.00**	**120**		**$14,400.00**	**$18,400.00**
7	**ADD PLUG AND PLAY CAPABILITY FOR IEDs**							
	- Design			$0.00	40	$120.00	$4,800.00	$4,800.00
	- Parts	2	$1,100.00	$2,200.00	18	$120.00	$2,160.00	$4,360.00
	- Fabrication				180	$90.00	$16,200.00	$16,200.00
	- Integration and testing				32	$75.00	$2,400.00	$2,400.00
	SUBTOTALS			**$2,200.00**	**270**		**$25,560.00**	**$27,760.00**
8	**PURCHASE AND INTEGRATE COMMUNICATIONS EQUIPMENT**							
	- Dialup modems	2	$800.00	$1,600.00	20	$120.00	$2,400.00	$4,000.00
	- Leased Line modems	2	$800.00	$1,600.00	20	$120.00	$2,400.00	$4,000.00
	- GPS/IRIG-B Time sources	1	$1,800.00	$1,800.00	160	$75.00	$12,000.00	$13,800.00
	SUBTOTALS			**$5,000.00**	**200**		**$16,800.00**	**$21,800.00**

MATERIAL SUBTOTAL	**$48,700.00**		**DIRECT LABOR SUBTOTAL**	**$226,920.00**
		1,583		
PROJECT SUBTOTAL				**$275,620.00**
CONTINGENCY		**5%**	**$275,620.00**	**$13,781.00**
ESTIMATED TOTAL PROJECT COST				**$289,401.00**

Phase I Project Tasks

A brief listing of the specific design tasks associated with the Phase I activity of the I/O upgrade is included here:

- **Test Bay Cubicles:**

  - Electrical
  - Signal Patch Panel

  Verify electrical power to the existing test cubicles. Design, procure, and fabricate test cubicle patch panel assemblies for four selected cubicles.

- **Equipment Rack Area:**

  - Layout Arrangements
    - Floor Plan
    - Rack Locations
    - Wall Plans
  - Electrical Service
  - Communications Cable Inter-Rack Routing

  Design, procure, and install electrical modifications, cable runs to the four test cubicles associated with this activity, and other modifications needed to locate the equipment in the test rack area.

- **Front End Communications:**

  - Rack Layout
    - 2 Leased-Line Modems
    - 2 Dial-Up Modems
    - Network Switches/Equipment
    - Serial Interface Patch Panel Assembly
    - Electrical Details

  Design, procure, build, and install a new panel with patch panel interface units to test cubicle and computer system communication cabling, patch panels to connect to the communications patch panel serial interface PP assembly, and a patch panel for network connectivity. The panel will house two (2) dial-up and two (2) leased-line modems. Cabling will be provided for connection from the modems to patch panels and from modems to phone jacks. Power will be integrated into the panel for easy connection. Network interface connections will be provided, configured, and managed by network support personnel.

- **Communications Patch Panel:**

  - Rack Layout
    - 2 Leased-Line Modems
    - 2 Dial-Up Modems
    - Serial Interface Patch Panel Assembly
    - Electrical Details
    - Communications Cable Inter-Rack Routing

  Design, procure, and install modems, serial interface and Ethernet interface PPs, and required cable assemblies to connect to the Front End Communications panel, and serial and Ethernet modular connector patch panels to interface with the EID and RTU bays.

- **RTU/Controller Bay:**

  - 2 racks with adjustable slide assemblies for mounting modular equipment housings
  - I/O interface design for connection with: TX, GEN, DIST and Standalone emulators

  Design, build, and integrate three new RTU/controller housing units. Design, procure, and install RTU racks, unit housing with RTU, I/O interface, power interface, connectors, devices, and wiring necessary to provide functioning RTU installations for three RTUs with modular interface to standard and new emulation units.

- **IED Bay:**

  - 1 rack with adjustable slide assemblies for mounting modular equipment housings
  - I/O interface design for connection with: TX, GEN, DIST and Standalone emulators

  Design and build new IED housing units. Configure for three new IED units. Design, procure, and install IED unit housing with I/O interface, power interface, and connectors, devices, and wiring necessary to provide functioning IED installations for three emulator units with modular interface to standard and new emulation units.

- **Miscellaneous:**

  - **Arbiter Clock**
    Rack Details
    Antenna Mounting Details
    Antenna Cabling Routing Details
    Configuration of Clock and Integration with System

  Design, install, configure, and integrate satellite sourced GPS clock unit with communications interfaces, power interface, and connectors, antenna, and wiring necessary to provide functioning time services to IED, RTU, and computer resources at the Test Bed.

- **Emulators:**

  1 rack with adjustable slide assemblies for mounting modular equipment housings

  - **1 Standalone modular emulator unit**
    Pattern design and assembly after previous designed units

  - **1 TX Unit**
    Digital and Analog signals
    Interface to IED device(s)
    Interface to RTU/Controller unit
    Manual Indicator/Control Switches

  - **1 DIST Unit**
    Digital and Analog signals
    Interface to IED device(s)
    Interface to RTU/Controller unit
    Manual Indicator/Control Switches

  - **1 GEN Unit**
    Digital and Analog signals
    Interface to IED device(s)
    Interface to RTU/Controller unit
    Manual Indicator/Control Switches

  Design, procure, fabricate, and install new emulation units providing transmission, distribution, and generation emulation functionality. Provide analog interface to each of the emulators to show power flow through the emulation when the units are connected. Provide control switches for all devices on the emulation panels along with status indication of each of the monitored and controlled devices. Install standardized interface connectors for cabling the emulators to any IED or RTU device.

- **System Management:**

  - Install new engineering management station
  - Establish Configuration Management Process for the Test Beds
  - Integrate communications with Test Equipment
  - Procure, configure, install, and integrate a new computer engineering management station for configuration, troubleshooting, modification, and documentation of the Test Bed RTU, IED, and other configurable assets.

- **Citect HMI/SCADA System**

  - Integrate existing system into Test Bed Communications

  Configure, install, and integrate a computer system for configuration, troubleshooting, modification, operation, and documentation of a Test Bed SCADA and process control system HMI platform for use in supporting testing applications for components and systems at the Test Bed and associated interfaces.

APPENDIX A

Phase II Description (funded by other Programs):

The Test Bed configuration will continue to be enhanced to support expanding test requirements as additional projects are developed at the Test Bed. Funding for these modifications will be negotiated through these projects and other avenues available to the INL programs. Currently, projected upgrades to the Test Bed configuration include the following (refer to Figure 5):

- Connectivity to additional test cubicles
- Addition of Oasis central station configuration to expand system-level testing
- Addition of fiber optic communications
- Communications with INL wireless test facilities
- Addition of second set of new integrated emulator units
- Additional control system computing resources
- Connectivity to the Test Range Facilities at SPERT and Scoville substations
- Expansion of the IED and RTU test bays
- Addition of computer soft controller technology
- Expansion of hardware and software-based I/O to meet system-level testing needs.

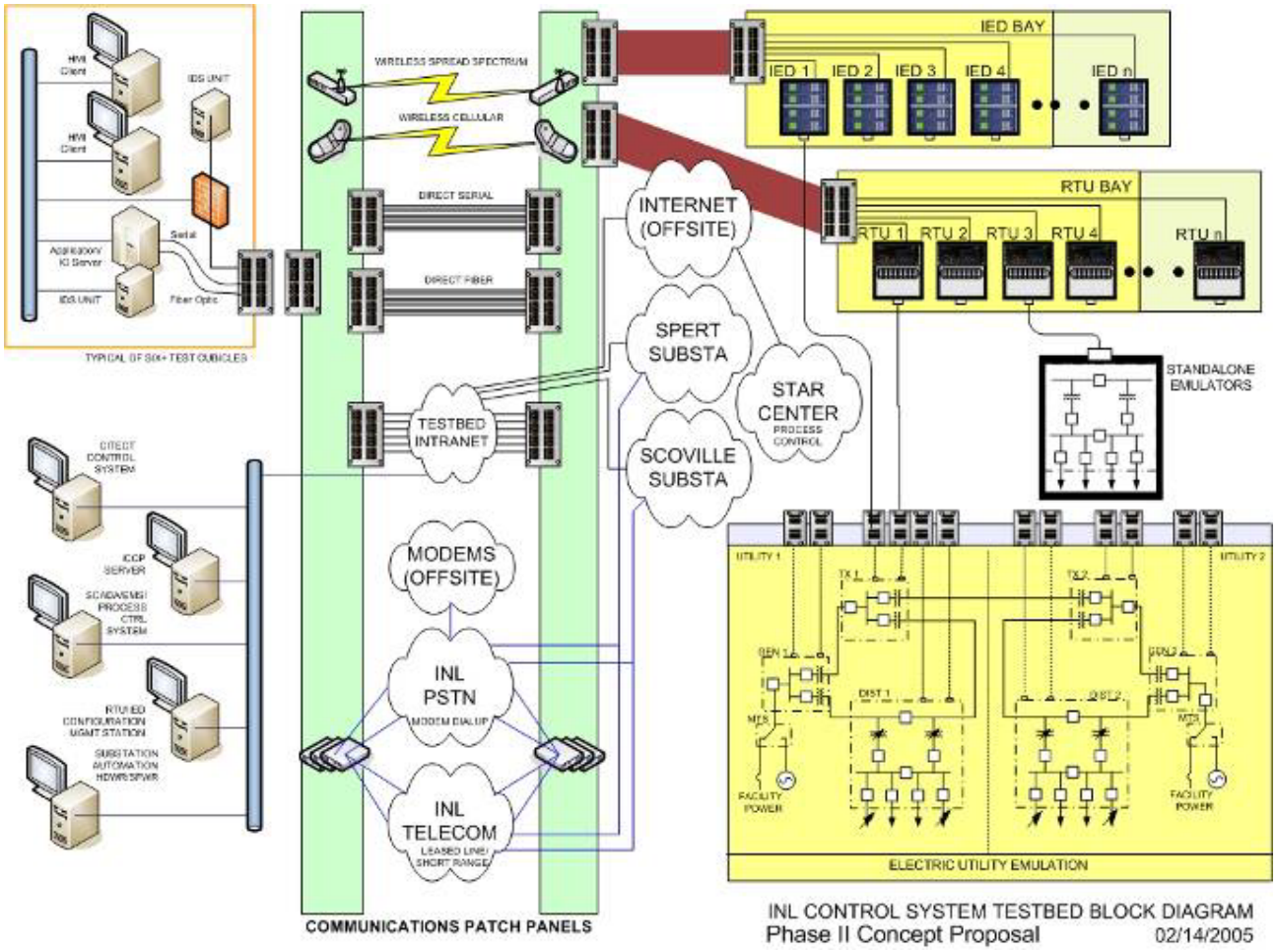

Figure 5. Phase II IORC and External Interfaces Configuration.