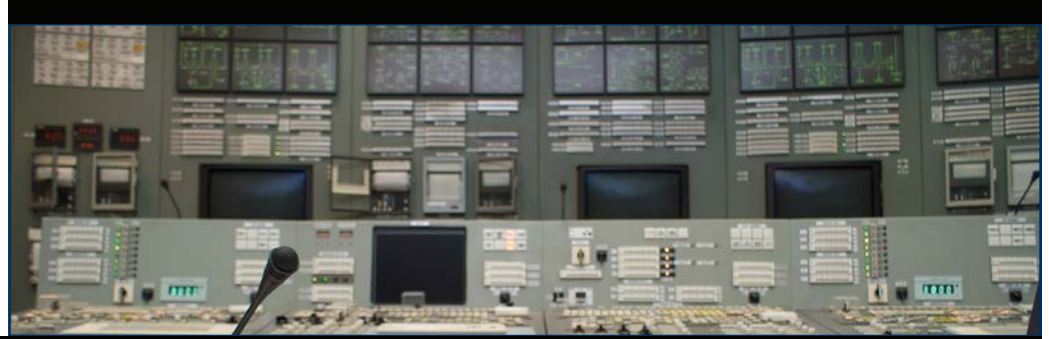Nuclear Plant Products and Services

Plant Process Computer Systems

The first Plant Process Computer (PPC) design was driven by the need to monitor, record and present a few key operating parameters to plant personnel.

Over many years PPC has evolved to become a critical monitoring and display component that aids the operators in maintaining safe, reliable and efficient operation of the plant. Conceptually simple, as illustrated in Exhibit 1, system complexity has grown exponentially since its inception in the late 1970s. The challenge facing system providers is to deconstruct that complexity, eliminate inter-component dependencies and create fully transportable modular solutions that are supported by current and future technology advancements.
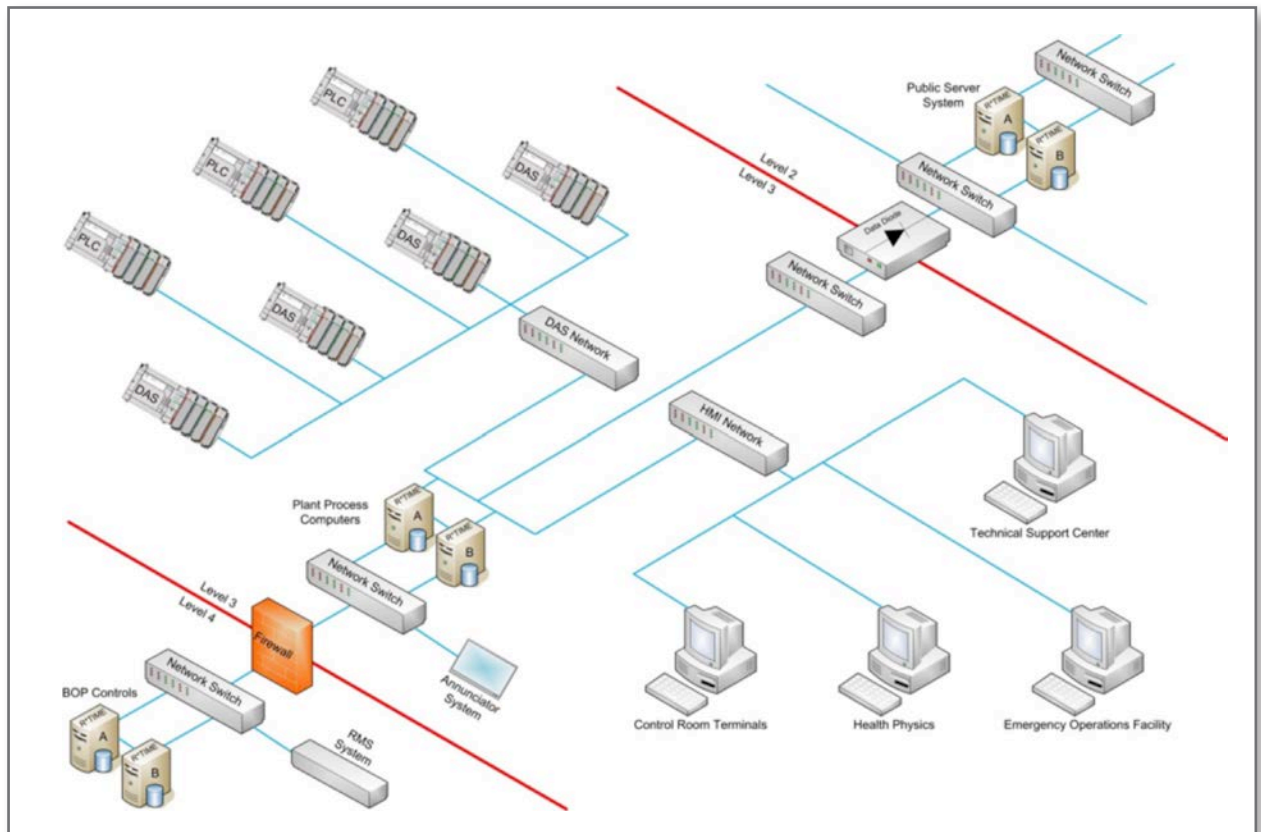

Exhibit 1

Plant Process Computer Systems

The key to achieving the modernization goals lies in a system resource management platform that resides over the operating system and manages the services that it provides to the nuclear applications and the supporting devices in the generating environment. Modularization of all software functions and standardization of communication among all system components enables the system's use of completely standard, off the shelf devices. **All of these elements combined form a system structure that supports the use of current technology and maintains PPC performance to plant decommissioning. The platform is also the basis of an obsolescence elimination strategy that dramatically reduces ongoing maintenance and support costs.**

The single incontrovertible truth about PPCs is that no two are the same; even sister plants on the same site built at the same time. Exhibit 1 is a good representation of a typical system with the detail omitted. The four common elements in

all PPCs are an I/O system collecting from a few hundred to more than ten thousand analog and digital points, a redundant communication network and server environment including cyber security components, a complex set of large format displays, work stations and associated peripheral devices and the nuclear software applications executing on the platform. Depending on the original plant design the components may be centrally located or widely distributed throughout the site. There are also a host of supporting systems such as the Simulator, Annunciator, Radiation Monitoring System, Meteorological Tower, Emergency Offsite Facility and Technical Support Center that also must mesh seamlessly to enable all members of the engineering, maintenance and operations teams full access to the information they need to maintain plant operation.

The Scientech plant information system platform is based on a set of products which are used extensively in nuclear and fossil power generation worldwide. At its core, the R*TIME Server and R*TIME Viewer software have been designed from the ground up to support the needs of the power generation client base. Both products have a 20+ year history of successful application in nuclear and fossil generation.

The single incontrovertible truth about PPCs is that no two are the same; even sister plants on the same site built at the same time.

Scientech emphasizes maintaining technologically current products and counts a number of industry firsts among its accomplishments, including:

- *All system software developed in C/C++/C#. In today's software environment "C" offers clients a platform more resistant to technological obsolescence that is much more easily maintained by the evolving workforce.*

- *First to deploy a plant computer platform operating completely in a UNIX environment (Palo Verde).*

- *First to deploy a plant computer platform operating completely in a Windows environment (TMI).*

- *First to deploy systems in a Microsoft Windows 2008 environment (Hope Creek and Millstone) and embrace Windows domain control as one facet of an environment that addresses evolving cyber security requirements and patch management needs in the domain environment.*

- *First to deploy RTP 2300 and RTP 3000 based systems. Scientech maintains a close working relationship with RTP and is always an early adapter of new technology from RTP.*

Flexible and Powerful System Platform

The Scientech R*TIME Server software has industry unique features such as the ability to simultaneously support up to 16 databases active in a single server environment. Each of the 16 databases is capable of supporting over 60,000 analog and 60,000 digital data points. The R*TIME Server database management tools facilitates on-line modification of virtually every database field to include the ability to add and delete database points while the system is in operation.

The multiple database environments provide users the benefits of being able to accomplish functional segmentation of system activities where appropriate, as well as, permitting nearly unlimited system expansion. The multiple database capability has also proven very valuable for parallel system validation and testing.

The Server and database environment support 12 database-configurable alarm limits for each point in the system. Alarm limits may be constant or may be variable based on the value of other points in the system. Alarm limits are plant mode dependent with support for up to 8 plant modes.

Plant Process Computer Systems

In addition to the 12 database configurable limits, the system provides support for Operator based limits. Operator based limits may be applied to any point in the system using on line tools without altering the pre-configured database limits. This feature gives operators control of cautionary alarms or alarms desired for certain plant evolutions without altering System Alarms.

Integrated with the server is an archive environment designed to provide reliable data storage and reconstructions. The archive system is able to record analog data as fast as 4 milliseconds and does not use exception based processing or compression which assures reliable, accurate data reconstruction.

In a redundant server environment, the archive system provides redundancy features that assure accurate recording and reconstruction even in failover conditions. The R*TIME archives fully support local disk archive, NAS based archive and SAN based archive systems.

Virtually all data in the on-line system is accessible by off-line products such as Microsoft Access, Word, and Excel through an ODBC compliant interface to R*TIME. In addition to having support for in excess of 75 proprietary or legacy interfaces, the Scientech R*TIME product natively supports OPC and Modbus interfaces and has gateway interfaces for DNP-3 to name but a few.

Scientech has field proven standard interfaces available for 3rd party commercial historian products such the OSI PI and the InStep eDNA products.

Data accessibility is a key issue in today's computing environment. While many systems have the ability to collect and store information, making that information easily available to the end user in a convenient and useable format can be a challenge. In addition to making data ODBC-accessible, the Scientech R*TIME environment provides an easy to use Excel interface that brings real-time and historical data to the users' desktop with ease.

In a typical Scientech R*TIME deployment, the Public Server System extends data access to the corporate desktop. Data provided to the corporate user is time synchronized with the plant computer environment assuring what the corporate user is viewing is consistent with what the operators on the protected network see.

Extensive Diagnostic Capability

The base Scientech R*TIME offering fully integrates the RTP I/O system to include RTP diagnostic capability. The basic R*TIME system health and monitoring processes collect chassis, card and point health information which is used to determine overall system health as well as point status. Information such as power supply status, redundant communication status, processor health information card status and where available, point health are all reported though the DAS communication process and rolled up to present an overall picture of DAS and System health.

Scientech has also taken the traditional concept of system health information and extended it into the "peripheral" arteries of the process system. As the traditional Plant Computer environment has evolved, designs have taken greater advantage of potential redundancy options offered by modern computing and network environments. While the redundancy options can result in increased system availability they can also result in a false sense of security. If the health of redundant components is not actively monitored, they cannot be trusted to be available when needed.

In a Scientech design nearly every component is monitored for health and availability. The capability includes monitoring redundant power supplies in server computers and internal server parameters such as temperatures and fan

condition. The monitoring capability extends into network switches where internal switch health and individual port conditions can be monitored. Monitoring extends further into the display workstations used to drive the control room display environment. In some instances monitoring capability has been extended to printers located in the environment.

In addition to its benefits for monitoring system health and possibly preventing system or component failures, monitoring now incorporates part of the cyber security threat mitigation strategy. Not only can active network ports be monitored for health and activity, ports intended to be inactive can be monitored and alarmed if they become active, allowing administrative staff to quickly take appropriate action. Note that the multiple database capability offered by the R*TIME server allows the extensive system health and monitoring database to be separated from the data typically available to plant operators. This capability allows the IT staff to have full access to data and health alarms without distracting or impacting operators with computer health information.

The Scientech R*TIME Data Viewer

Scientech has invested heavily in its data viewing technology. R*TIME Data Viewer is designed to seamlessly integrate data from the R*TIME server environment. The Data Viewer design stems from the needs of the nuclear industry and is highly tuned to the nuclear operations environment. The product is a full-featured graphical user environment with a drag and drop display building environment. Scientech maintains complete control of the product and does not rely on third party software or technology which maintains our unparalleled ability to continue to tailor the product to the needs of the Scientech client base.

Viewer has unique features such as the ability to integrate data from up to 64 data sources (R*TIME databases) into a single viewer environment and indeed to a single R*TIME screen. The ability to handle multiple data sources has significant implications when considering fleet monitoring options.

On the performance side, the viewer supports archive playback, high speed screen updates as fast as 250 milliseconds and supports local archive

caching for data points that are critical in providing almost instantaneous trend fills.

Screen navigation can be accomplished through virtually any pointing device, touch screen and standard keyboard. Screen navigation can also be computer controlled with computer directed screens based on plant conditions.

Software Development Process

Scientech uses a proven software design control methodology for software development that meets applicable ASME NQA and IEEE requirements. These controls include a design process with procedures for the preliminary and final design phases as well as the implementation and testing phase. Major review processes are performed in-house on the specifications, detailed designs, acceptance test procedures, manuals and documentation as required by the project Quality Assurance Plan. Software development activities are performed using Scientech Standard Operating Procedure SOP 20.1, Software Development and Control.

Scientech procedures require, as part of standard system development methodology, a thorough software configuration management system. This system provides comprehensive controls for software development during all phases of the project. Scientech uses a Serena product, PVCS

Version Manager, for maintaining configuration control on all its software products. The Scientech engineering standards and procedures govern the practices and procedures used in the preparation and document control of all Scientech designs, drawings, specifications and procedures. These standards are used to ensure that all products are designed and operate properly and are configured in accordance with current revisions of the documentation.

Scientech maintains a thorough, fully integrated Quality Assurance (QA) program as part of its normal software and hardware design process. This program is referred to as an "in process" QA program. The in process QA activities are those normally performed by the Scientech QA organizations as required and controlled by the design control procedures.

Each Plant Process Computer replacement project generates a Project Quality Assurance Plan (PQAP). The PQAP defines the project specific implementation of the quality requirements identified in the Scientech QA Manual including, where required, any Independent Validation and Verification (IV&V) for certain PPC applications.

Scientech uses Seapine's TestTrack Pro to document reported problems and the corrections for the problems. When a problem is reported or a change to the software is requested, an entry into TestTrack Pro is initiated, a number is assigned and logged and the problem/change request is assigned to a responsible individual. After the correction/change is completed, the resolution is recorded in TestTrack Pro and its status is updated in the log. The process is monitored to assure that problems and requested changes are being addressed in a timely manner.

Formal system testing is performed using test procedures that have been reviewed and approved. This testing follows successful completion of a dry run test of the integrated system using those procedures. The objective of the system testing is to demonstrate and document the compliance of the integrated system with the plant requirements.

The project team and cognizant engineering personnel prepare the procedures. The documents address testing requirements, philosophy, environment, specification, procedures and detailed test descriptions. The collection of test cases is selected to provide a fully-integrated functional test of the system. The appropriate functional organizations, in conjunction with the Project Manager, are responsible for the preparation, independent review, approval, release, control and revision of these test documents.

Plant Process Computer Systems

Project Time Line/Execution

While there are a great many variables in the completion of a Plant Process Computer replacement project, our typical completion time is approximately 18 to 24 months from contract award. A few major variables that come into play are generally:

- *Plant Outage Schedules* – Even if an installation is not intended to be outage based, the availability of plant personnel to support outage requirements impacts document review schedules, and in some cases, impacts staff availability for activities such as factory testing.

- *Phased Installation Schedules* – Phased projects have the advantage of breaking execution and installation into smaller and presumably more manageable tasks. Phased projects also tend to take longer and cost more to execute to completion.

- *Plant Urgency* – On occasion, plants delay replacement to a point where existing systems have become critically fragile and have begun to negatively impact generation. In these cases, efforts are made to accelerate normal process schedules.

- *Engineering Change Package Lead Times* – Each utility has their own requirements for lead times for review and acceptance of the Engineering Change Package for a Plant Process Computer replacement project. Scientech has encountered lead times for the approved ECP from 6 to 15 months prior to the PPC installation.

The normal development process begins with detailed system design. On the hardware side of the design, a hardware design document is produced. The goal of the document is to translate specification requirements into a hardware list and design that communicates to the client exactly what they should expect to receive and how it will be configured. The document enables the client to determine if the hardware design has been properly interpreted and will be implemented in a manner consistent with the plant needs. The document also has a primary purpose of conveying, to the architect engineer on the project, the details needed to complete the plant design package.

On the software side of the design, a Project Standards Document is developed early in the project. This document defines systemic standards to be used in the configuration of the R*TIME server, development of system displays, development of plant-specific software as well as any special user interface consideration.

The normal development process begins with detailed system design.

Some system aspects defined in the Project Standards Document include:

- Definition of alarm colors and behavior

- Definition of quality propagation rules

- Definition of display header information

- General rules for display navigation

- Use of color, font, line size, etc. on displays

- Any special rules related to shape behavior such as pumps, valves and motors

The document communicates to the development team the core set of rules to be followed in application development.

Coincident with establishing the core rules the Software Requirements Specifications are developed. These may be developed by Scientech and reviewed by the Client or provided to Scientech by the Client. Once agreed upon requirements are established, those requirements are translated into more detailed software design documents. Scientech then develops software and test procedures from the design information.

Obsolescence Management and Mitigation

The Scientech EverGreen process offers the promise of eliminating the major modification replacement paradigm of the plant information system with the achievable goal of extending the system's viability to end-of-plant-life.

Process computer hardware and software have dramatically different economic and operational life cycles than the I/O systems to which they are interfaced. I/O systems have exhibited much longer term stability and viability than computer systems. However, their end-of-life migration paths have also proved less predictable and potentially more disruptive than the end-of-life migration path for computer hardware.

Scientech has developed and fielded the **Refresh Strategy** as one element of the Evergreen process. Refresh recognizes aging and obsolescence issues in system components and software and provides specific mitigation activities that prevent system age from compromising safe, reliable and efficient operation of the plant to end-of-life and through decommissioning. The Refresh strategy also has the advantage of significantly reducing cost for ongoing system maintenance and support.

Plant Process Computer Systems

Cyber Security Aware

While most in the industry understand that complying with the evolving cyber security guidance is a difficult to manage situation, Scientech continues to develop its products to be compliant with the continually advancing requirements. As mentioned earlier, in a Windows environment domain controllers assist in enforcing security policies. The use of protocols that require a minimum of open ports in firewalls helps maintain firewall effectiveness. Scientech provides technology to help secure interfaces from higher security layers to the PPC and from the PPC to lower security layers including managing the use of vulnerable technologies such as OPC. We offer multiple solutions for integrating control system data into the PPC in a secure manner. Scientech continuously monitors industry guidance and offers new communications options that address the desire for unidirectional data flow as required.

On the hardware side of the technology, the use of managed devices to the maximum extent possible, allows increased physical security on the network. When used in conjunction with the Scientech infrastructure diagnostic tools, capabilities for detection of physical intrusion onto the protected network are provided. Scientech has developed interfaces and communication methods to support all major data diode providers and works with the plant to define and configure firewalls that fulfill all cyber security requirements.

The Overall Scientech Advantage

Scientech is the leader in the Plant Information Technology business both in nuclear and non-nuclear segments. As mentioned previously, Scientech has a number of technology firsts. Scientech is also leading the way with advanced service and maintenance options. One key to our ability to maintain a leadership position is a workforce that is balanced with a blend of seasoned, experienced nuclear industry veterans and augmented by a growing influx of young, fresh talent. The Scientech Plant Process Systems workforce has nearly doubled in the past 10 years. Technology that is current and familiar to today's college engineering graduate has enabled significant growth from the bottom up and has served to continue to keep the technology we provide fresh and forward looking. Previous experience in addressing fleet initiatives has provided Scientech with unique experience and perspectives that result in significant economies of scale, not just in product but in process, which yield true long-term savings to the fleet.

Delivering Solutions to the Worldwide Power Industry

Scientech, a business unit of Curtiss-Wright, is a global engineering, manufacturing and service company. Scientech provides plant process computer, digital control, and annunciator systems; thermal performance software; regulatory information databases and services; nozzle dams and installation services; reactor and steam generator specialized tooling; under-vessel BWR services and equipment; inventory database services (RAPID, OIRD) and supply chain analytics; probabilistic risk assessment (PRA) services; repair, refurbish and reverse engineered I&C services; power supplies; security and access authorization software; mobile technology applications; and equipment reliability solutions. We are committed to the safe operation and improved performance and reliability of power plants worldwide.

CURTISS-WRIGHT