Bridging Paradigm Gaps

Steve Cafrelli – Exelon Corporation
Joseph Clupp – Exelon Corporation

Abstract

The electric utility industry has undergone radical changes since the mid-1990s. These changes have produced a shift in several key paradigms around the industry, technology, and expectations for work products, especially work products related to plant process computers. Utilities and suppliers (the market) have, in some cases, responded and adapted to the paradigm shifts at different rates. Gaps have appeared where the response to the paradigm shifts has diverged. Gaps can create tension between utilities and suppliers due to misunderstandings and differences in expectations. In order to create an environment where both organizations can succeed, it is necessary to identify the gaps and understand the differences in order to build a more efficient, profitable business relationship.

This paper examines three key paradigm shifts in competition, technology, and work management, the utility and supplier (market) responses to the paradigm shifts, and identifies means to bridge the gaps that have developed. This paper also discusses Exelon's approach to address the paradigm gaps that have arisen in relation to plant process computers focusing on the financial considerations, strategies and tactics employed, and work management processes.

Introduction

Since the mid-1990s three key paradigms have shifted radically in the electric utility industry that has impacted the way Plant Process Computers (PPC) are viewed in the nuclear industry. Along with the changes mandated by a competitive market place, other changes in expectations regarding work management and technology stability have changed the way PPC's are managed and supported. Figure 1 represents the changes that have occurred in the last six to seven years.

The industry has transitioned from a highly regulated, non-competitive environment to a deregulated "market" competitive environment. This shift has led to a number of consolidations, acquisitions, and mergers. The consolidation, in turn, has led to changes in how organizations function. In particular, a shift has occurred in larger utilities away from the distributed single-unit operational philosophy to a centralized "fleet" approach for dealing with financial as well as tactical and strategic decisions.

Other paradigm shifts relate specifically to plant process computers. For example, the pace of technology changes has increased exponentially since the mid-1990s such that, in many cases, plant computer replacements are often obsolete by the time installation occurs. The pace of technology changes has affected how plant process computers have evolved. From the early 1980s to the mid-1990s, plant computers were seen as monolithic entities that were used as support to the bench indications. Most plant computers of this era had a limited viewing capability and limited resources for performing complex calculations.

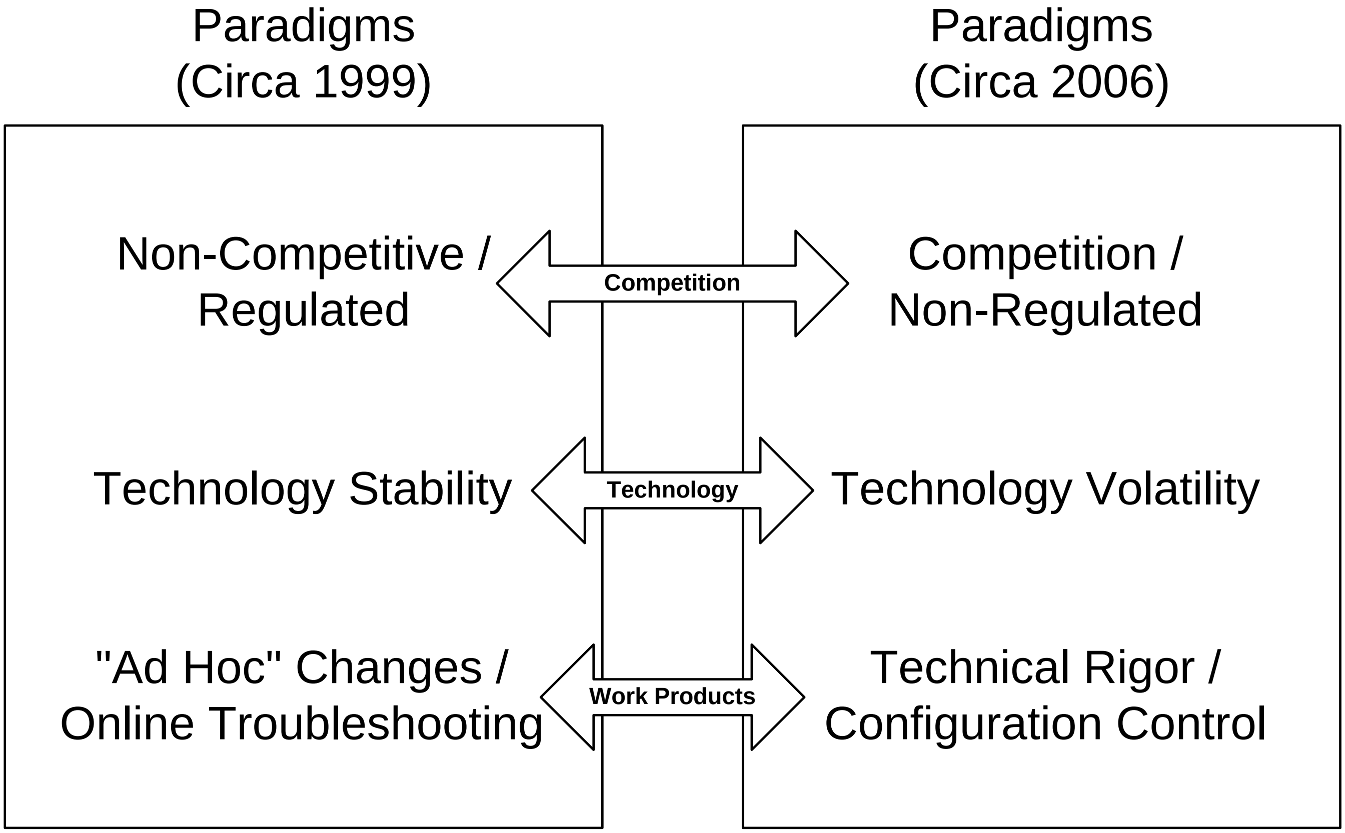
With the change in technology from the mid-1990s to today, plant computers have become more integral in the day-to-day activities being performed in the plant. In many cases, plant computer systems are subject to the Maintenance Rule and high reliability and availability have become critical requirements. A second change that has occurred is the manner by which the power plant itself is operated. Power plants now run with lower margins, that is to say, closer to the thermal limits, in order to maximize generation. Plant computer system reliability is crucial in allowing the power plant to be operated in this fashion.

In addition, with the advent of home personal computers, end user expectations at the power plant have risen significantly for easy access to integrated data using "standard" tools, such as Excel. Thus, plant computer systems have evolved from highly proprietary operating system and application software to more modular and open systems that can utilize industry standard platforms and operating systems such as Windows and UNIX.

The change in PPC usage has also caused a shift in work management and engineering expectations – how work products are developed, tested, and installed. Downtime for plant computer systems, which in the past may have been accepted as part of doing business, is now minimized due to demands by the user community. Thus, work is now more often included in system windows and must be scheduled like other plant work activities. Configuration changes to the plant computer systems must incorporate a high degree of technical rigor to ensure that changes are "done right the first time" in order to meet schedule requirements. Re-work and back out scenarios are tolerated less today than during the early days of plant computer systems.

This paper examines these three key paradigm shifts in competition, technology, and work management, the utility and supplier responses to the paradigm shifts, and identifies means to bridge the gaps that have developed as the utilities and suppliers (market) have responded at different rates.

Figure 1


Paradigms
(Circa 1999)
Paradigms
(Circa 2006)
Non-Competitive /
Regulated
Competition
Competition /
Non-Regulated
Technology Stability
Technology
Technology Volatility
"Ad Hoc" Changes /
Online Troubleshooting
Work Products
Technical Rigor /
Configuration Control

Competition –Regulation to Competition (Figure 2)

The wave of electric utility deregulation that swept the nation in the 1990's changed the face of electricity generation as well as the nuclear industry. This paradigm shift – the change from a non-competitive, regulated environment to a non-regulated, competitive "merchant" generation model drove plants to become more cost efficient and look for new ways to increase production while reducing costs. As a result of this shift, a total of 29 nuclear plants have been sold[1] since 1999. Table 1 shows some of the acquisitions, mergers, and consolidations of the larger fleet owner / operators.

In order to achieve economies of scale promised by mergers and acquisitions, a centralized approach has led to a shift from individual sites owned /operated by single utilities to creation of nuclear "fleets" whereby a single owner / operator controls multiple units. Corporate organizations were established and chartered with performing upgrades on a "design once, install many times" basis. Standardization became a key word for the new approach – not just for plant computer replacements, but for performance monitoring as well. The shift to management of nuclear sites on a fleet basis has given rise to corporate organizations whose purpose is to provide standardized support and to enforce consistency for the purpose of reducing maintenance and support costs.

As a result of the new focus on efficiency and cost control, funding for site projects and PPC replacements has become more challenging. In the regulated environment, cost management was important, however, costs were ultimately passed onto the ratepayer. With the shift to a competitive market place, cost management has become a more significant issue. PPC replacements do not offer the same return on investment as other projects and as a result must compete more rigorously for funding against other plant modifications such as digital turbine installations and steam generator replacements.

This has led to the need to perform long term planning for plant computer replacements across multiple sites in order to achieve economies of standardization and the development of long-term plans for computer replacements that extend anywhere from two to ten years. Suppliers need to recognize these changes in how the utility organization is managed and develop multi-unit fleet solutions that can be applicable to all plants in the fleet.

The change in the competition paradigm has also led to changes on how plants perform outages. Outage duration is now kept to a minimum in order to maximum plant generation. Shorter outages have had two significant affects on plant computer usage:

1. Shorter outages leave less time to perform maintenance on the plant computer systems
2. Shorter outages have placed a higher demand on plant computer system usage during outages in order to complete plant outage work items such as surveillance and calibrations

Shorter outages have necessitated increased oversight and management to ensure appropriate resources are available such that outage schedules remain on track. Utility expectations during outage periods is for suppliers to make senior management available in outage command / control centers during plant installations. This has resulted in increased support from suppliers, which ultimately affects the bottom line.

[1] NEI – U.S. Reactor Ownership / Management, http://www.nei.org/index.asp?catnum=2&catid=345

Figure 2

Paradigm Competition

Old Way	**New Way**
Individual Sites	Fleet / Centralized
“Ad Hoc” Replacements	Long Planning Process for Replacements
Funding Available When Needed	Internal Competition for Funding
Unique Design	Design Once / Install Many
Long Life Cycle	Short Life Cycle
Stable Business Models	Changing Business Models

Table 1
Selected Nuclear Power Plant Consolidations

Owner / Operator	*Number of Units*	*Original Owners*
Exelon	17 20 (pending)	Philadelphia Electric (PECO)
		Commonwealth Edison (UNICOM)
		Illinois Power
		General Public Utilities (GPU)
		PSEG (Pending)
Entergy	9	Entergy
		Boston Edison
		New York Power Authority
		Vermont Yankee
Nuclear Management Corporation	6	Point Beach
		Prairie Island
		Monticello
		Palisades
Dominion	6	Dominion
		Northeast Utilities
Constellation	5	Baltimore Gas & Electric
		Niagara Mohawk
		Rochester Gas & Electric
Progress Energy	5	Florida Power Corporation
		Carolina Power & Light
FirstEnergy	4	Ohio Edison
		Duquesne Light

Technology – Stability to Volatility (Figure 3)

From the early 1980s through the mid 1990s, technology changes around plant computers were slow and incremental. Many plant computer systems of this era were vendor-supplied hardware and proprietary operating systems. Site-specific applications were often written to the target hardware using the vendor-supplied software compilers and programming interfaces. Hardware and software changes often originated with the supplier and often involved a premium cost to stay "current". Plant process computer replacements were generally viewed by the utilities as a "brain transplant" which only needed to be performed every 20 years or so.

Starting in the mid 1990s, as computing platforms became faster and more cost effective, the paradigm began to shift. Each generation of technological advances has resulted in faster processors and more resources (memory and disks) for the same cost. Life-cycle support for older hardware, operating systems, and base applications continued to decline as suppliers explored new revenue sources through exploitation of the newer technologies and "built in obsolescence". The pace of these changes continues to accelerate presenting challenges for alignment by utilities and suppliers around the pace of technological changes.

The technology paradigm shift has also caused a shift in how plant computer systems are viewed. Gone are the days of the proprietary, monolithic configuration where one supplier provided custom-designed hardware, operating systems, and support software. Today, plant computer systems are expected to utilize commercial off-the-shelf hardware and software as well as provide open access to data in order to allow engineers to use common tools, such as Excel, to reduce and analyze plant data.

The perception of the lifetime of the plant computer system has remained the same. Utility management expects that any replacement effort will result in a "remainder of plant life" solution. This viewpoint is incompatible with the expectation of utilizing standard hardware and software components. There is little hardware or software today that is designed to last more than five years.

While utilities have readily adapted to changes in their competitive market place, utilities recognition of the issues around the plant process computers market place has generally not changed. For example, plant computer replacements that employ newer technologies have been challenged for the costs associated with refresh of the technology. While the utility organizations are quick to accept newer technological platforms, there is a reluctance to provide the base level funding needed to provide for system refresh to ensure the systems remain viable. In many cases, management is still influenced by older thinking that plant process computer systems and replacements are meant to last the life of the plant. In many cases, suppliers already exist in a competitive market place. The utility industry needs to learn to adapt to technology volatility as other process industries (such as petrochemical and industrial manufacturing) have while maintaining necessary controls to comply with NRC requirements.

Suppliers are much better at and ready to respond to technology changes. This is out of necessity in that new customers prefer newer technology and that the old technology is not available. Thus, in order to meet market demands, suppliers must ensure their products can quickly and cost-effectively by migrated to newer technological platforms. As a result of the need to stay current with technology, suppliers often plan for shorter life cycles (on the order of five years or less) between major product versions.

In addition to responding to technology changes, suppliers and utilities must also now consider cyber-security issues in relation to data access when designing systems. The diametric opposition of cyber-security and data sharing present a challenge for suppliers in designing plant computer systems that interface with corporate local area networks and intranets while meeting emerging NERC and NEI guidelines.

Work Management, Technical Rigor & Configuration Control (Figure 4)

Work Management

Prior to the mid-1990s, plant computer changes were requested, worked, and installed on a "first-come, first-served" basis. The processes for installing computer changes were less complex in terms of engineering change packages as well as system availability. However, with the change in the work management paradigm, this is no longer the case. Engineering change packages have become more complex and rigorous while requiring longer lead-time to implement. Also, computer outages must now be scheduled as opposed to requesting system downtime "on the fly". Thus, due to the plant planning process, computer changes that once were simple to install have become more onerous. Regular enhancements now must be scheduled as far as 22 weeks in advance. As a result of the longer lead-time and fewer opportunities to modify the plant computer system, more intelligence has been required to consider which changes can and should be combined into a single change effort.

In order to reduce operator distractions and also allow operation closer to thermal limits, process computer work is now treated the same as other plant systems. These work management processes must be adaptable and responsive to user-driven enhancements as well as break/fix when problems occur. Without efficient work management processes, plant computer performance may decline over time due to the inability to respond to problems and needed enhancements.

The utilities must be able to implement software fixes provided by suppliers in a timely manner. When measured against other plant enhancements these modifications often receive a lower priority and thus need to have robust, tested solutions that are delivered with reasonable confidence that the solution will work the first time. The "try this and see what happens" method is less acceptable in today's environment.

Technical Rigor & Configuration Control

Technical rigor is the set of behaviors and activities that ensure that a deliverable (hardware, software, system) has been sufficiently tested and challenged such that implementation occurs with a minimum of (or no) errors. Technical rigor is applicable from the earliest development of requirements through design, build, test, and installation. Without good technical rigor, latent problems may propagate through the system and surface later, creating a significant effect on performance, and resulting in unanticipated down time.

Technical rigor is just as important for suppliers of plant process computer materials and services. Although this behavior has only recently been proceduralized at Exelon, Exelon has had mixed results with the technical rigor applied to internal and external deliverables. The lack of technical rigor has occurred most in situations where assumptions are made concerning the requested enhancement or break/fix requirements.

Figure 3

Paradigm
Technology

Old Way	**New Way**
20-Year (Life of Plant) Life Cycle	5-Year Life Cycle
Unique (Vendor-Specific) Tools	Standard Tools
Non-Networked Systems	Design Considerations - Viruses
Limited Access to Information	Open Access / Information Sharing
	Data Integrity / Security

The challenge for both the utilities and suppliers is to ensure that the detailed requirements of requested modifications are well communicated and understood between all parties. If there is ***any*** doubt about a particular request, suppliers need to stop and ensure that all pertinent information is available and understood before proceeding with work. In addition, suppliers must recognize and anticipate design constraints and be aware that the customer may ***not*** possess the design expertise to fully understand a proposed solution. Finally, suppliers need to challenge any assumptions made during development of modifications or system design elements. The utilities can often assist and provide insight to the supplier when challenging design assumptions.

Throughout the 1980s and early 1990s, plant computer systems were considered by end users more of a tool to assist in day-to-day operations in determining plant conditions. The plant computer was utilized mostly as a scan and alarm system to alert the operators to changing conditions. As such, end-users were often agreeable to allow online troubleshooting and downtime for installation of software. If the installations did not proceed well, the loss of system availability was an annoyance, but well tolerated.

Starting in the mid 1990s, this paradigm began to shift. Today, expectations are that software changes are engineered and completed with a high degree of technical rigor such that solutions are tested to ensure expected performance and installed correctly the first time. Downtime for the purposes of “backing out” a failed installation is often met with increased scrutiny and is often accompanied with remediation tracked in the Corrective Action Program. Software changes that fail as a result of a lack of technical rigor are seen as an indictment of IT understanding with respect to how business is done at a nuclear facility.

Plant operating groups expect the plant computer changes to be engineered changes and not “build to fit”. “Build to fit” refers to modifications that are the result of a response to a suggestion without regard to other system effects or whether the suggestion is valid. With the increased emphasis on excellence in engineering design, the expectations of technical rigor are applied equally to software as well as pumps and valves. Thus, “the bar has been raised” in regards to performing modifications and maintenance on plant computer systems. Peer reviews, back out plans, and independent reviews are becoming standard lexicon within utility organizations for addressing plant computer changes. Increased monitoring of plant computer performance has been instituted as key performance indicators that are tied to economic incentives. Thus ***any*** downtime can adversely affect the indicators resulting in increased monitoring and scrutiny.

Another challenge for both utilities and suppliers is to recognize and properly respond to how shifts in the work management paradigm has been in direct opposition to the paradigm shifts for the pace of technology change. Whereas the pace of technology change tends to drive to faster, more rapid changes required to address user concerns and maintain system viability, the increased work management practices around configuration control and technical rigor have driven modifications to be less frequent and more stringent. This dichotomy alone leads to tension between the desires to be responsive to user needs while adhering to procedural requirements.

Figure 4

Paradigm
Work Management

Old Way	**New Way**
Error Tolerance	Technical Rigor
Ad Hoc Changes	Engineered Configuration Control
Non-Scheduled Work	Schedule Adherence

Building the Bridge

In order for both utilities and suppliers to be successful, a bridge must be built to span the gaps that have been created due to the varied perspectives and responses to the paradigm shifts. The purpose of the bridge is to facilitate understanding of issues that are important to both utilities and suppliers. In this example, the bridge consists of the following:

- Pillars – the financial aspect for both utilities and suppliers
- Cables – the strategies implemented that provide flexibility and strength
- Road (Deck) – the work management processes that produce quality and timely products

Pillars (Financial) (Figure 5)

Financial considerations serve as the pillars for the bridge – the reason for both the utilities and suppliers to exist. Financial influences, both internal to the utilities and external with the suppliers, set the foundation upon which the remainder of the bridge is built. Without positive financial incentives for both parties, the foundation of the bridge collapses. Suppliers need to recognize that any customer is looking to obtain products and services for the lowest possible cost. Similarly, utilities must recognize that the suppliers must be able to generate a fair profit; otherwise the supplier may eventually cease operations that leaves future product support in question and actually incurs additional cost to the utilities.

Utilities and suppliers need to be sensitive to several key components in the financial area. Utilities have not always done a good job of presenting a consistent message to the suppliers. If the fleet model is truly the model of the future, then utilities must do better in enforcing standardization across the fleet. For example, Exelon has four installations of the Scientech R*TIME system, however, no two R*TIME installations are running the same R*TIME base system or Data Viewer versions. Some of this is the result of mergers and acquisitions -- some is the result of the long planning process and the pace of technology change.

By the same token, suppliers such as Scientech must be willing to accept dealing with corporate fleet organizations. For example, maintenance agreements that in the past were tailored for individual sites or units should be modified to address a fleet approach. In addition, suppliers need to provide stable (within the context of the changing technology) technical solutions such that installed products and services can be refreshed without incurring repeated costs for performing “brain transplants”. This is not to say that suppliers cannot and should not improve their products, however, products and services should be designed for ease of incorporation into existing installations.

Contractual expectations and understandings are necessary such that changes to the underlying work processes are well defined and understood. In other words, the further one is removed from the day-to-day activities and work processes, the more likely that the individual (or organization) is no longer current with the expectations of work processes and work products. Thus it is paramount to clearly state and understand the rules and expectations surrounding work products and work practices.

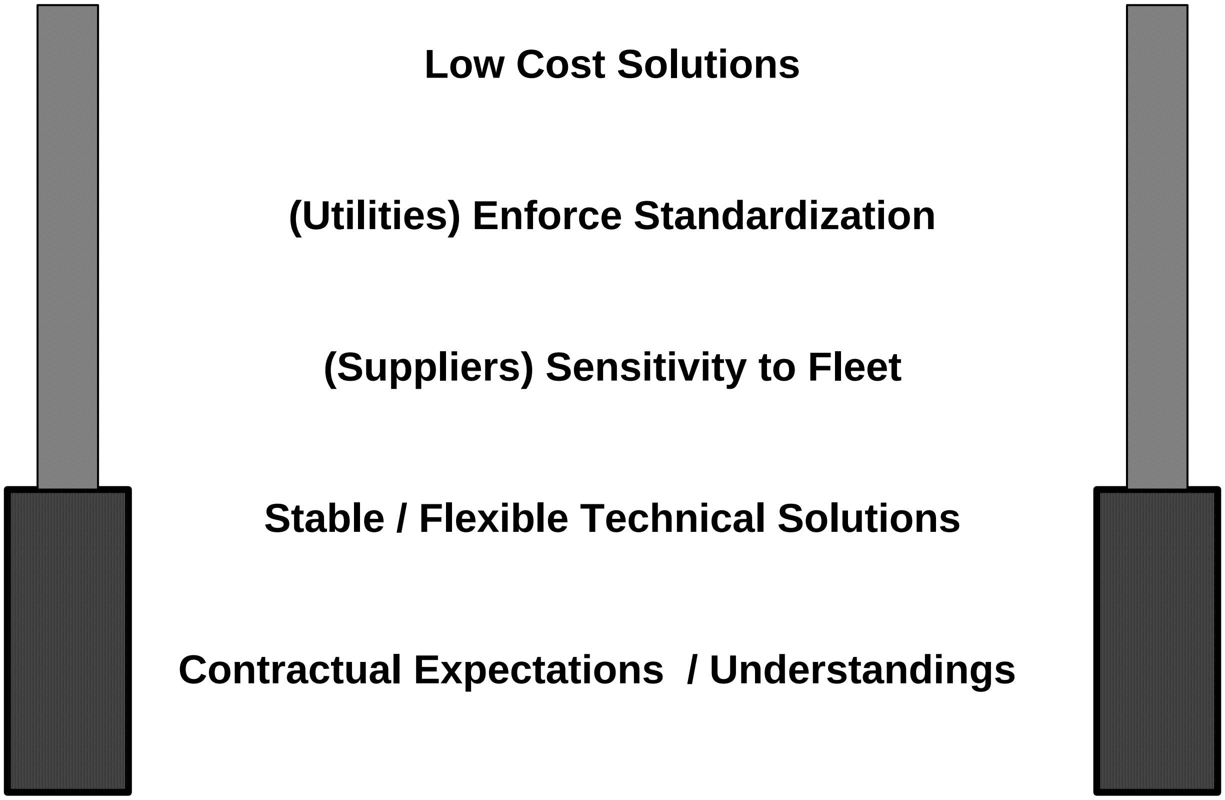
In order for utilities and suppliers to succeed, contractual expectations and understandings must be clear, concise, and well understood. Ambiguous and / or unrealistic expectations reduce the overall effectiveness of products developed as well as creating undue stress between utilities and suppliers. For example, utilities must clearly state positions, such as the fleet concept, and expectations from suppliers in responding to the concept. Another example is clear expectations around technical and management support of plant computer installations, especially when installation occurs during outages. Suppliers must clearly state their response to the utilities expectations as well as express their expectations.

Without open, two-way communication, misunderstandings and ineffectiveness will intrude on the processes for maintaining and upgrading plant computer systems. This ineffectiveness ultimately affects the end-user and can also have a financial impact on both the utilities and suppliers.

Two examples of building financial pillars at Exelon include the plant process computer purchase agreement with Scientech and the development of a master schedule for replacement at the various sites. The agreement with Scientech ensures that a standard product will be installed for each site. The master schedule allows for decision-makers to understand when financial resources are required to accomplish the organizational goals.

Figure 5

Financial (Pillars)



Low Cost Solutions

(Utilities) Enforce Standardization

(Suppliers) Sensitivity to Fleet

Stable / Flexible Technical Solutions

Contractual Expectations / Understandings

<u>Cables (Strategies and Tactics) (Figure 6)</u>

The cables of the bridge represent the strategies employed to address plant computer system issues. Sound strategies by both utilities and suppliers are designed to provide organizational flexibility and strength. Without flexibility and strength, the bridge will collapse. Suppliers and utilities must jointly engineer solutions in order to provide easy access to data in a secure computing environment. Non-secure computing environments that compromise data integrity or tolerate regular virus intrusions directly negatively affect the financial well being of the affected entity (utilities and/or suppliers).

Another key strategy is around the concept of using standard tools, such as Excel, for data reduction and analysis. In this case, utilities need to identify what standard tools are in place for end-users to view and manipulate data such that suppliers can ensure system designs account for the expected end uses.

There is one overriding certainty in the computer business – technology changes will continue to occur at a more frequent rate than most businesses can respond. This is especially true in the nuclear industry. Due to the time frame involved with most replacement systems, the hardware purchased at the beginning of the project is nearly (or already) obsolete by the time installation takes place in the plant. Strategies need to be developed around how to manage the installed platforms in regards to technology changes.

In many cases, the strategy for dealing with technology changes may affect the hardware refresh strategy. For example, a regular refresh strategy of three to four years will, in most cases, keep the hardware from becoming obsolete. In addition, since most hardware suppliers offer three or four year warranties, the hardware can be kept under warranty at all times.

Strategies that consider the longer-term issues that can affect plant process computers and performance need to be defined. Strategic items need to include items such as:

- *Hardware Refresh Philosophy*
- *Software Upgrade Philosophy*
- *Dealing With Technology Changes*

Hardware Refresh Philosophy

Hardware refresh strategies must be built recognizing plant computer systems have evolved from monolithic to modular entities. In the monolithic paradigm, the plant computer system was considered as a single entity – “the plant computer”. With the evolution to open architecture of systems, the plant computer hardware and software have been “de-coupled” from each other. Thus, it is possible to refresh the hardware platform on which the software executes independent of the software.

Hardware refresh strategies must recognize the funding competition with other nuclear plant needs and develop standards that define the triggers when hardware refresh should occur. In many cases, technological advances cause suppliers to move away from support for older technologies and operating systems. The business case for replacing obsolete equipment is often insufficient to successfully compete for available funding if the change cannot be done inexpensively.

Defining which components are within scope of the power plant configuration control processes and which components are not is a key strategy that can help reduce costs. This analysis should take place at the beginning of any replacement effort. Typically, the effort required to refresh components that are within plant engineering design space is more complex than those considered commercial equipment. Thus, the documentation of design boundaries is a key strategy for ensuring that refresh can occur at the lowest possible cost.

While most of the strategy surrounds justification on the utilities part, suppliers also have a role in this process. Software must be written by suppliers to be platform independent. If the software is platform dependent, the business case justification for performing regular hardware refresh becomes even more challenging as the cost increases.

The Hardware Upgrade Strategy area at Exelon is still under construction. Current efforts in this area include development of a hardware refresh roadmap similar to the replacement roadmap that clearly defines a cycle for refresh across the fleet. In addition, the real-time organization is working with the various design organizations to define design boundaries rather than specific components to allow for commercial changes. For example, rather than document a design that specifies a particular model of server, the design should indicate the characteristics of the server such that ***any*** commercial available server that meets the minimum boundaries can be used for refresh without reanalysis of the hardware design itself.

Software Upgrade Philosophy

Software upgrade strategies present more difficult challenges than do hardware refresh strategies. This too is a result of the evolution from large, homogeneous (one supplier of hardware and software) to modular, open systems (multiple suppliers of hardware and software). While hardware refresh efforts can be justified on obsolete or non-supported equipment, software upgrades must often stand solely on the business case, i.e., the benefits that are derived for the cost of the upgrade.

Consider the issues around a software upgrade for a Scientech R*TIME system. For example, the typical plant computer system supplied by Scientech consists of the following three components:

- Base System (R*TIME Server)
- Viewer (R*TIME Data Viewer)
- Site-Specific Applications

A relationship exists between each area such that if one area is “upgraded” other areas may be affected. The software products and development philosophy of suppliers have a direct affect the utilities ability to make the case for software upgrades. In the Scientech example, base system software development needs to be backward compatible with site-specific applications as much as possible to minimize the amount of re-work and testing involved with a base system upgrade. If a base system or viewer upgrade also triggers significant site-specific application work, the business case becomes increasingly difficult to make.

Communication between the suppliers and utilities for recognizing step changes in the product line also can affect the business case. This includes ***clearly*** communicating (as opposed to hinting at) when support will stop for legacy products. In some cases, suppliers may decide upon a "phase-out" support strategy where support for different components of a product are stopped, eventually leading to dropping support for the entire product line. In any case, suppliers published plans for product support can affect the business case for the utilities. This information is critical in transitioning the business case from a "nice to do" basis to a "must do" basis.

From the utilities perspective, software upgrades not only involve refresh costs associated with the supplier's efforts, but also include internal engineering costs. Thus, in order to strengthen the business case, suppliers should understand and design software components that can be "changed out" with a minimum of re-work and re-test. In addition, suppliers need to institute standards such that future upgrades are fairly consistent. There needs to be certain predictability as to the costs and efforts associated with upgrade of the base system and viewer components. As is the case with hardware strategies, definitions of which software and data are or are not under configuration control can have a significant impact on the cost of software refresh.

Exelon continues to make strides in developing software upgrade strategies. These include such elements as:

- Development of a database change procedure that defines which database points are within and which database points are outside engineering controls

- Development of a document that defines which software elements are user configurable and which are under configuration control processes

- Procurement, use, and continued maturity of development systems to provide offline test platforms (this activity is currently on-going)

- Development of a standard product that describes the IT details suitable for use by Design Engineering

- Development and use of standard test cases (this activity is currently on-going)

Dealing With Technology Changes

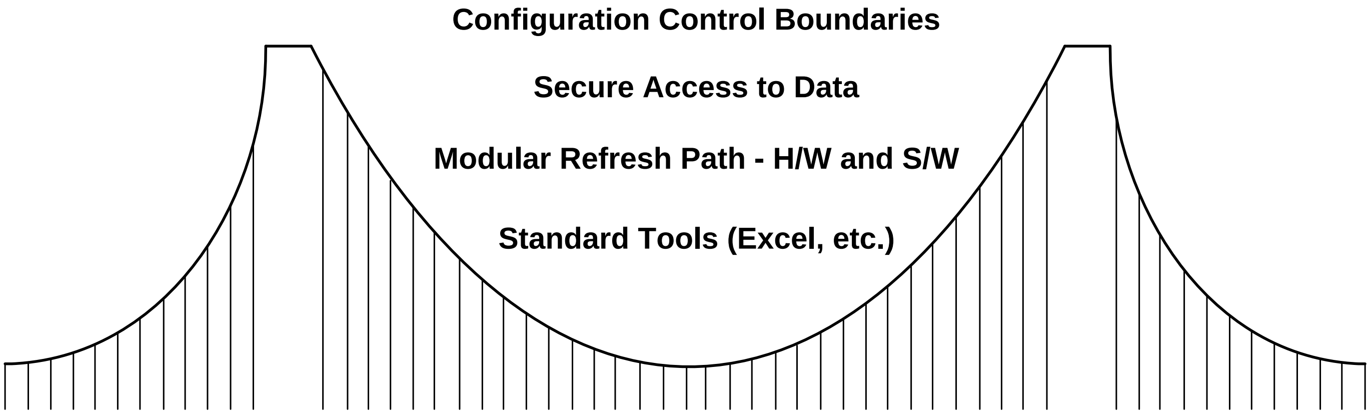
One key strategy to consider is the design elements required to allow communication between the dedicated plant computer networks and the overall general corporate networks. In particular, supplier's products that operate in a client/server environment must be able to exist in a corporate environment that must be secure and protected. Strategies around design elements that incorporate anti-virus strategies, patch management, and data access (use of firewalls) must be defined to be flexible in order to deal with the changing technology environment.

In general, utilities must improve communication to their internal customers to raise cognizance on the issues surrounding technology changes. This communication needs to demonstrate the need to embrace change and ensure the ***appropriate*** response to technology changes. This includes ensuring that the standard designs for the organization continue to be viable. Changes in technology may necessitate changes to current standards, which can affect the hardware refresh and software upgrade strategies. Again, when standards change, communication between the utilities and suppliers is essential to maintain an open dialog surrounding technology issues.

Exelon has responded to this challenge in several methods. First, firewalls have been implemented between the corporate network environment and dedicated plant computer networks for all sites in order to increase security and prevent unauthorized access to the plant computer network environment. In addition, data access to the end user community through the corporate network has been directed to plant server systems (PSS) or independent third-party historians such as Pi or eDNA. One advantage of this data access strategy is that the plant computer network components can be upgraded with minimal effect on the end-user community.

Figure 6

Strategies (Cables)


Configuration Control Boundaries
Secure Access to Data
Modular Refresh Path - H/W and S/W
Standard Tools (Excel, etc.)

Deck (Road) (Tactics / Work Management) (Figure 7)

Finally the work management processes represent the bridge deck, i.e., the roadway and way we get things done. The tactics employed are those that have the potential to most directly affect plant computer systems. Tactical influences include the following:

- *Clearly Defined Requirements / Problem Statements*
- *Robust Design*
- *Tested Products*
- *Use of Established Processes*
- *Value Added Maintenance Agreements*

Clearly Defined Requirements / Problem Statements

Clear, unambiguous requirements provided by the system owner are essential in order for both utilities and suppliers to be successful during plant computer system replacements. The requirements serve as the basis and target of what products and services are to be supplied with the system. Missing, incomplete, or poorly written (ambiguous) requirements often lead to miscommunications and a failure to produce the desired end result. Even in the case when the correct results are initially obtained, poor requirements can often lead to maintenance issues when trying to determine the real functionality.

For example, during the Oyster Creek replacement project, there was an ambiguous requirement around a specific SPDS alarm. This requirement, while on the surface appear valid, did not really reflect field transmitter response in relation to the presentation to the user. In particular, a requirement that involved selection criteria using two different scaled inputs was unclear and the desired result for the end-user could not be implemented as described. This ambiguity caused initiation of a configuration change shortly after the system was placed in service. The situation could have been avoided with a clearly stated, well-understood requirement statement.

A key component of defining requirements is defining “normal” and “abnormal” conditions and the expected response within the conditions. “Normal” conditions, in this case, is the expected (90-95% of the time) conditions or algorithms under which the hardware or software operate. “Abnormal” conditions refer to unexpected (less than 10%) chance of occurring. For example, if an algorithm uses three inputs to determine an average, how should the algorithm behave when suddenly there are only one or two (or no) inputs available to determine the average? The requirements not only need to answer the question for the immediate calculation, but also consider the effect downstream on other requirements.

At Exelon several activities have been taken or are currently underway to address clear requirements. These include:

- Development of standard project management methodologies

- Self assessments to identify weaknesses in requirements (on-going activity)

- Internal white paper for applicable staff dealing with writing and reviewing quality requirements

Robust Design

One component of our bridge deck is based on robust designs for plant computer systems. Plant computer systems that take into consideration the strategies previously discussed for future hardware and software refresh are critical to an organization's success. Poor or incomplete plant computer system designs that do not consider the strategic factors around refresh and future upgrade can have negative financial impacts.

Plant computer designs must translate requirements into reality. In particular, the design basis of normal and abnormal conditions should be defined. For example, nuclear plants are designed for normal operations and transient (shutdown conditions), but do not design against meteor strikes to the reactor building. The same holds true for plant computer designs – the normal and abnormal basis need to be clearly defined in the design and the boundaries understood for what is within and what is outside the design bounds.

In addition, robust designs must not only address the immediate requirements, but must also consider the effect of each requirement on the overall system. In particular, system designs must tackle system response when a key component or software module fails or begins to act erratically. Robust designs are key to minimizing downtime and the effect on end-users.

System designs must also take into consideration issues surrounding patch management, anti-virus implementation, general data access, and security of dedicated plant computer equipment as well as end-user clients. System designs must ensure the maximum stability such that end-users are not burdened with frequent service interruptions necessitated when new hardware and/or software is implemented. Configuration control processes are key to ensuring that system designs are well documented and understood in order to effectively make required modifications.

Tested Products

Products that are developed, either in-house or by suppliers must be well tested and "hardened". Testing needs to be comprehensive and robust. For example, testing the "normal" conditions needs to be done in order to demonstrate the desired functionality, however, testing outside the "normal" conditions also needs to be performed to some degree to show that the product behaves in a robust manner, even outside the normal bounds. If a delivered product is not properly "hardened", then failures when abnormal conditions occur can affect system performance, which can lead to financial penalties as well. In addition, the end-users also may develop a negative impression on the capabilities of the implementing organization and be less cooperative in supporting future product installations.

The need for well-tested products is a direct response to the paradigm shift around work management. Expectations for both utilities and suppliers are that supplied products function correctly the first time. The tolerance for ad hoc, on-line troubleshooting of software products on plant computer systems has decreased dramatically.

Exelon real-time systems have responded to the challenge of hardened products through the procurement and use of development systems to allow for additional testing. Also, peer checks have been introduced during product development and testing to help catch problems prior to production system installation.

Use of Established Processes

Nuclear plants rely on processes to accomplish work within the power block. For years, plant process computer work has often times worked outside (or on the periphery) of this process. In order to effectively manage and successfully process changes, then the established work management and scheduling processes must be followed. If the plant computer work is important to the plant, then the process will find a way to "make it happen". If not, then working outside the process will only serve to frustrate suppliers, support staff, and end users.

The real-time systems organization at Exelon has instituted a standard product that is useable by the Site Engineering (design authority) to develop change packages. Recent challenges at Exelon in work management have been met through meetings with Site Engineering to establish schedules for implementation and a prioritized work list with which all parties concur. This has led to pre-defined computer outage windows for implementing end-user defined scope of changes utilizing the existing plant scheduling processes.

Value Added Maintenance Agreements

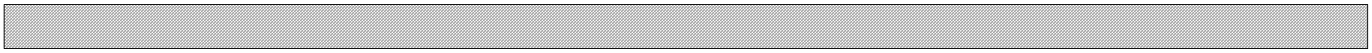
Maintenance agreements, particularly for software, can have a major influence on plant computer systems and performance. Non-existent or poorly structured maintenance agreements can lead to delays in addressing on-going emergent issues. Utilities that have adopted the fleet paradigm view this as an area where costs can be controlled and an opportunity to capitalize on the economies of scale.

As the fleet paradigm is adopted throughout the industry, there will be more desire for fleet-wide maintenance agreements. In response, suppliers need to be open to tailoring their maintenance agreements on a fleet-wide basis. Again, maintenance agreements involve two-way communication. Utilities that desire a fleet-wide agreement need to ensure that the interface with the supplier is managed such that the supplier is not overwhelmed by questions and requests from the individual sites.

A key component of any maintenance agreement, however, is identification of problems and solutions to the problems. This includes disclosure of problems discovered while developing new versions of the product. For example, if Scientech is developing R*TIME version 13 and discovers a problem that exists in version 11 or 12, then notification should be made immediately to users of versions 11 and 12. The timely notification allows the utilities to make a determination as to the extent of condition, remediation efforts, and schedule for remediation.

Figure 7

Work Management (Deck)



Clear Requirements / Problem Statements

Robust Designs

Tested Products

Use of Established Processes

Value Added Maintenance Agreements

Putting the Bridge Together (Figure 8)

Thus far, discussion has centered on the various parts of the bridge. The point, however, is that a bridge cannot be built with any one or two of the three components (pillars, cables, or deck). In fact, all three components, interconnected properly, are required to complete a functional bridge (see Figure 8). One of the key elements is that the bridge must be flexible. The bridge must be built to adapt to changing environments and taking advantage of opportunities for continual improvement. If flexibility is not built into the bridge, then failure of the bridge is inevitable.

Exelon has undertaken construction of several key bridge-building components that include:

- Creation of a corporate fleet approach to managing and maintaining real-time plant computer systems
- Definition of a standard for plant computer replacements
- Development of a long-range replacement schedule (roadmap) for all fleet units / plants
- Institutionalization of Technical Rigor and Configuration Control Processes
- Regular end-user meetings to understand expectations and prioritization for work
- Pre-defined windows to implement computer changes

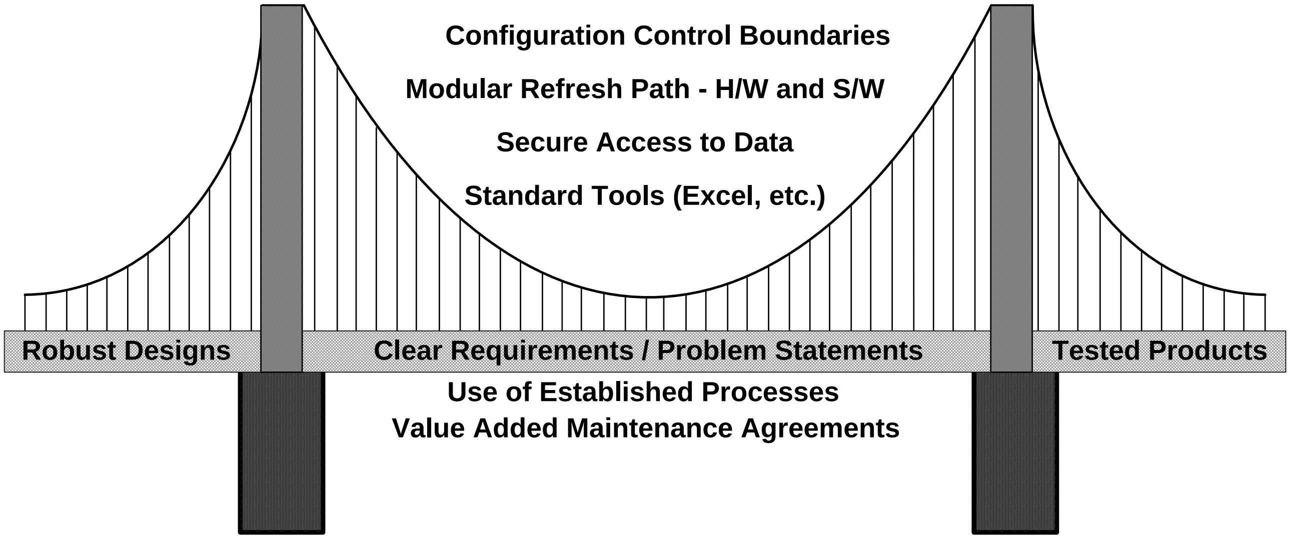
While some work has been accomplished, construction of other key bridge components at Exelon continues which includes:

- Refining and documenting hardware and software refresh strategies
- Successful resolution of a fleet maintenance agreement
- Improving work products through use of technical rigor
- Defining engineering documents with bounding conditions rather than specific design elements
- Development of engineering documents that define what is and is not within the boundary of configuration control
- Participation in user groups with suppliers to further communications

By understanding the paradigm shifts and the resultant gaps that have arisen, a strong, flexible bridge can be built that leads to greater understanding and profitability for both utilities and the suppliers. Failure to bridge the gaps may result in ineffectiveness and increased costs for both parties. Open communication between utilities and suppliers is needed to ensure understanding and sensitivity to the issues faced by both utilities and suppliers such that both can be successful, effective, and profitable. Without a properly built bridge that incorporates understanding and flexibility, working relationships between utilities and suppliers may become strained which further erodes trust and confidence between all interested parties. Thus, it is in the mutual interest of all to continue to engage in “bridge-building” behavior to build an open, strong, effective, value-added, and profitable working relationship.

Figure 8

Building the Bridge


Configuration Control Boundaries
Modular Refresh Path - H/W and S/W
Secure Access to Data
Standard Tools (Excel, etc.)
Robust Designs
Clear Requirements / Problem Statements
Tested Products
Use of Established Processes
Value Added Maintenance Agreements

Low Cost Solutions
(Utilities) Enforce Standardization
Contractual Expectations / Understandings
Stable / Flexible Technical Solutions
(Suppliers) Sensitivity to Fleet

Discussion Questions

1. What other paradigms and paradigm shifts in relation to plant computer systems may have occurred over the last 5-10 years?

2. What other factors have challenged your plant computer maintenance, upgrade, and replacement strategies?

    a. How have these challenges been managed?

    b. What strategies have been effective in addressing maintenance / refresh issues?

3. What approaches have been / could be taken to address the gaps discussed in this paper?