THE TOP 10 CONCERNS ABOUT OPEN SYSTEMS
UNDERSTAND AND RESOLVE THE MOST COMMON OBSTACLES TO CONTROL SYSTEM MIGRATION
In the past, a Distributed Control System (DCS) or Programmable Logic Controller (PLC) would have been the only means to apply control applications. Plants could network these older systems together, and then engineers would have to manually route each point, costing a user time and money. On top of all that, considerable time was required to install and set up special cables and hardware to connect the systems to work as one.

Now, users seek integrated systems. Industrial manufacturers need to remove the constraints of closed, proprietary control systems and free up their plant’s profit potential. There is a growing demand for open automation infrastructures integrating installed assets and co-existing with legacy systems—all while protecting valuable investments.

Instead of relying on costly high-end workstations and other proprietary control system hardware, end users want the freedom to purchase less expensive commercial PCs and use open software applications based on the familiar and user-friendly Windows operating environment.

They require solutions that integrate process control and information systems with both plant and corporate business systems. Instead of integrating disparate applications, users are recognizing the value of a unified information and application software system. A unified system reduces the problem of data exchange and synchronization and maintains information in a central repository shared by all business applications and reduces the total cost of ownership (TCO).

The new communication systems and architectures supporting the evolving process control environment are changing the methods and skill sets required to operate these systems. To replace the comprehensive support of proprietary DCS experts, process IT departments are being established to manage the day-to-day administration of open control systems and their associated network infrastructure.

Automation end users must now assume greater responsibility for engineering an open process control network (PCN) with the reliability, robustness, performance, and security traditionally associated with proprietary process control systems delivering real-time, mission-critical information. Whereas control engineers and operators once had a limited role in managing their DCS environment, they must now deal with many more parameters affecting control system operation. The number of user-changeable system files, registry settings, and other accessible administration files increases exponentially in an open system architecture.

As process control environments converge into the overall architecture of the enterprise network systems, IT organizations will likely have to take on the added responsibility of securing not only the traditional computing environments of the enterprise network, but also the converged mission-critical data of the process control system. Access control technologies have become even more crucial with the requirements of user and system communication in a process control setting. Proactive protection must include all converged systems, threat response technologies must be effective in recognizing and mitigating potential dangerous events occurring anywhere in the converged network, and remediation of vulnerable and untrusted systems must be safely administered on the network system without risk to neighboring devices and systems.

This migration from dedicated, proprietary, DCS- and PLC-based controls to open, Microsoft- and Web-based systems raises important concerns about new responsibilities, skill sets, and change management. Here are the major concerns and how they’re being handled by leading end users with support by Honeywell.

The Top 10 Concerns About Open Systems

1. Open systems require different skill sets
2. Transitions to open systems are challenging
3. You may need help
4. How to pay for it?
5. Who owns the support?
6. Lack of robustness of commercial systems
7. Operating system software churn
8. Outsiders “accessing” critical controls of live plants
9. Internal security: sabotage or theft by thumb drive
10. Managing a global, multi-plant environment

1. Open Systems Require Different Skill Sets

When plant automation was executed by centralized, proprietary control systems, a single automation supplier, employing a large team of systems experts, was responsible for maintaining the process control environment, updating equipment as needed, and restoring operation in the event of a failure or turnaround. Modern process control strategies are transitioning from closed, proprietary platforms to networks of flexible, distributed databases and open human-machine interfaces (HMIs) where users have PCs or workstations.
Early needs were limited to supervising and controlling process loops. More recently, functions such as advanced control, and interfacing with business systems have been added. In this environment, users need to optimize their assets, adhere to environmental regulations, and document production processes. All this put greater requirements on modern process control systems.

This trend raises an important question: Who manages increasingly complex, geographically dispersed open systems employing hardware and software from multiple suppliers?

2. TRANSITIONS TO OPEN SYSTEMS ARE CHALLENGING
Open technology also has impacted control system engineering and configuration. While proprietary systems were almost entirely engineered and configured in a design center and then packed in a box and shipped, open systems tend to have many more variations. Since each user site has unique characteristics, each open platform configuration has exponentially more unique choices. As such, many engineering practices that were once standardized must now be engineered in the field, adding to project complexity.

After the system is installed, site requirements continue to evolve. Overall, 80% of system outages are due to change, so industrial end users must strive for a culture embracing change management. Process plants need effective methodologies for managing: configuration databases, system capacity and availability, IT service levels, software releases, backups, and other key aspects of network operation and maintenance.

3. YOU MAY NEED HELP
The challenges presented by migration to open systems may be difficult to overcome using internal resources, especially in a difficult economy when budgets are cut and hiring is frozen. During these times, it may be both practical and economical to improve system and process management with remote services to:

- Increase return on assets
- Manage an aging workforce
- Improve safety and security
- Reduce the impact of incidents
- Make people more effective
- Enable better decisions, faster

At a Honeywell Users Group (HUG) meeting, Marathon Petroleum described how it decided to manage the challenges of open systems by partnering with Honeywell to deal with open system support (OSS) issues including migration planning and coordination, and management of change.

Honeywell uses its knowledge of Marathon’s systems, configuration standards, and site-specific requirements to help the company manage open-system patches and upgrades, expansions, and best practices.

By drawing on Honeywell support, Marathon was able to restore confidence in its multiple-facility open-systems initiative and meet its objectives for safety, reliability, and profitability.

Shanghai Petrochemical, one of the largest modern petrochemical enterprises in China, finds the best, most cost-effective ways to manage assets and maintain its technological innovations is using Honeywell’s Lifecycle Management (LCM) program. LCM is a comprehensive, cost-effective solution to manage and support the company’s existing assets as it undergoes technology migration and expansion over the next three years.

4. HOW TO PAY FOR IT?
Once plants start to understand what it takes to effectively support open systems, an immediate concern is rationalizing the cost of additional responsibilities. But while open system support is very different from maintaining proprietary systems, it is actually a lower total cost of ownership not necessarily more expensive, especially when you consider the lower initial hardware and software costs (including the new virtualization savings) return on investment.

In addition, many facilities find that the expenses associated with keeping a dated proprietary system working will more than cover the support of a new, open system. This is especially true when an older system is approaching obsolescence or must be interfaced with a modern business system. These are key factors in building a business case for migrating to open.

Still, the initial investment in skilled personnel and/or training at the same time as the purchase, installation and commissioning of the new system can be daunting. This large initial outlay can be mitigated by judicious outsourcing to experienced service providers.

Venezuelan ethylene glycol and ethylene oxide producer PRALCA took this approach for a migration to Honeywell’s Experion system. It partnered with Honeywell to upgrade its legacy TDC3000 system to Experion PKS, and its APM controllers to HPMs. Benefits included advanced operator effectiveness solutions designed for asset management and abnormal situation management, which would reduce unplanned outages and increase process uptime. Experion’s HMIWeb technology provides an operator interface using standard Internet technologies, and its HMI includes standard displays supporting navigation and operation of the entire system.

Entering into a Lifecycle Management (LCM) agreement with Honeywell ensured predictable costs for supporting PRALCA’s installed control system assets and ongoing modernization efforts. It saved money by locking in prices of software support, parts management and upgrade kits when signing the agreement, achieving savings by not having to negotiate multiple service agreements every year.

PRALCA management has the flexibility to make additions to the LCM, to extend the program, or to renew it when it is due, and its Santa Rita facility will be able to compete effectively in the marketplace as production technology advances.
5. WHO OWNS THE SUPPORT?
In many organizations, engineers support the proprietary control system and IT experts handle open systems. The transition from proprietary to open technology has highlighted the differences between the plant IT and process control departments, as well as the criticality of their respective systems. Indeed, many software-based solutions common to IT organizations are unsuitable for use with process control systems.

Unlike the typical business network, an industrial-strength PCN must deliver the same level of robust operation with open technology that end users have come to expect in the plant automation environment. In process control applications, components must work together seamlessly in the same system. The hardware must be more robust to endure vibration, heat and other harsh conditions not present in the typical office location. The embedded software must be fault-tolerant and able to execute where many home PCs would fail. The control hardware and application software must provide the control types required for plant-wide automation.

In the days of proprietary control systems, system administration requirements were limited and easily handled by the typical process control engineer. Modern open systems allow for greater flexibility in hardware and software, but with that flexibility, there is a greater need to manage software releases, hardware compatibility, and system integration. The task of managing new hardware and software releases has shifted from the main automation contractor to the plant engineering department. This transition of responsibility can consume a tremendous amount of time normally focused on implementing or optimizing and maintaining control equipment.

Each company will resolve the requirements for skills and man-hours among its process control, engineering and IT resources differently, according to its priorities for reliability, security, etc. Gaps and shortages can be addressed with services such as remote PCN administration, patch management and performance monitoring.

A secure connection allows remote system troubleshooting, diagnostics and system administration, as well as remote access for authorized plant and third-party engineers. Services are provided by engineers who are both Microsoft experts and understand the functions and criticality of systems within the process control environment. This frees up local process control experts to focus on optimization and control.

6. LACK OF ROBUSTNESS OF COMMERCIAL SYSTEMS.
The benefits of open systems technology are many, which have helped to drive its rapid adoption. Open system architectures, however, bring new risks often not fully recognized by users. The older, more structured proprietary systems, while less flexible, naturally applied a layer of protection that is no longer present unless specifically added or preserved in new systems. Increased complexity also brings greater vulnerability and reduced availability of individual components within a plant control system.

The robustness of commercial systems has improved dramatically over the past decade, and their reputations for fragility are largely no longer deserved. The problems that remain are mostly due to the rapid evolution of open-system hardware and software (“churn”), and the issue of security. These are addressed below as separate concerns.

7. OPERATING SYSTEM SOFTWARE CHURN
A key concern for both open systems users and solutions providers is how to best manage their installed base. At the Honeywell Users Group (HUG) conference in 2010, Harsh Chitale, vice president and general manager for Honeywell Process Solutions in the Americas identified efficient management of open systems as a key concern, particularly the “churn” associated with the Windows operating system environment and its associated costs.

As an open systems supplier, Harsh announced that Honeywell has a new contract with Microsoft to extend the life and support of Windows XP and Windows Server 2003. The company also has a new contract with Microsoft to extend the life of Windows 7 and Windows Server 2008. Under a new Recommended Maintenance program for Experion systems, users will be able to access expert resources such as smart and preventative maintenance tools, proactive performance analysis, rapid response to system events, and remote access to experts for troubleshooting.

ADDITIONAL REFERENCES

HYDROCARBON PROCESSING ARTICLE ON SERVICE MANAGEMENT
Automation service suppliers should be more than maintenance technicians.

PROCESS ENGINEERING ARTICLE ON REMOTE AUTOMATION
Advances in the field of IT are encouraging operators to extend their use of control systems to facilities hundreds of miles away from main operations.
8. OUTSIDERS “ACCESSING” CRITICAL CONTROLS OF LIVE PLANTS

Many plants remain leery of allowing third parties or contractors (or even their own corporate IT departments) to access their PCN. Open networking and distributed computing systems provide organizations with convenient access to information and resources, but also make it easier for hackers, competitors, and disgruntled employees to compromise the computing environment. A compromised process can lead to losses including productivity, capital assets and, possibly, human life.

However, remote services only require viewing, not control, for monitoring, data access, and diagnostics. Resolving the access issue can lead to rich rewards. To increase productivity and reduce support costs at its Spruance, Va., plant, DuPont uses Honeywell connected services for technical support. The program provides a secure, online connection to Honeywell’s global technical assistance center (TAC) support team, enabling faster and more accurate problem resolution. The online connection allows support engineers to log directly into DuPont’s system to see technical issues firsthand. DuPont estimates it has cut the time to identify and resolve issues in half when the online connection is used.

As part of its Solution Enhancement Support Program (SESP), OneSteel implemented a secure, online connection to Honeywell’s global technical assistance center (TAC) support team enabling faster and more accurate problem identification and resolution. The online connection allows Honeywell support engineers to log directly into the customer’s system to analyze the issue and determine what data or course of action is required to identify and resolve the problem efficiently. Since SESP online services have been implemented, OneSteel has experienced several benefits:

• Saving on expenses for Honeywell support staff to travel to the plant
• A 30-50 percent reduction in time to solve technical problems, rather than waiting for support staff to physically travel to the plant
• Ability to test solutions before implementing changes to the system
• Higher system availability and reduced risk through direct online technical collaboration with Honeywell engineers

HALLMARKS OF WORLD-CLASS CUSTOMER SERVICE

PROCESSSES: SEEK GLOBAL CONSISTENCY
• Process and tools in place for clear accountability for service delivery
• Service Quality Mgmt system fully deployed globally
• Consistent global Technical Assistance Center (TAC) capability
• Consistent global training capability
• Automated maintenance tracking tools deployed globally

PEOPLE: ENSURE SKILLED RESOURCES EVERYWHERE
• Right people, right skills & competencies, in right place
• Local capability and customer intimacy
• Global support infrastructure
• Organization supporting communication and change management
• Apply the proper skill anywhere in the world in a timely manner

PROGRAMS: MAINTAIN, SUPPORT, OPTIMIZE, CHANGE

Maintain:
• Predictive performance management
• Flexible contracting strategy

Support:
• Remote support and services
• Web-based self help services

Optimize:
• Plant operations improvement

Change:
• Non-disruptive migrations
• Efficient migration of applications and configurations
• Performance based contracts

EFFICIENCY: FIND A TOTAL SOLUTION PROVIDER

• Embedded system self-diagnostics to improve service problem resolution time
• Load-and-go migrations
• Technology tools to improve efficiency and effectiveness of support team
• Remote monitoring capability in all new products

9. INTERNAL SECURITY: SABOTAGE OR THEFT BY THUMB DRIVE

A secure interface with the business network allows involvement by offsite experts and vendors, but careful consideration must be given to balance the benefits of a highly efficient operational model against the potential risks that come with the expanded connectivity required to realize this model. In an open-network architecture, threats are most commonly posed by virus attacks, worms, network spoofing, impersonation, denial of service, eavesdropping, password cracking, data tampering, and packet modification.

Successful plants will use authentication, access control, proactive protection, and dynamic response technology to provide a holistic approach to network security. Successful plants will also put a secure firewall on the perimeter of the PCN infrastructure, as any connection into the PCN is considered part of the perimeter and should be strictly managed by a security policy. The most common entry points include: vendor access (potential way for an attacker to access the system without having to penetrate the firewall), corporate LAN connection (since the corporate LAN is connected to the Internet, this connection has the most potential for giv-
Designing effective security is detailed in the white paper, Security solutions to meet NERC-CIP requirements. Building a secure PCN requires close attention to certain aspects of network design. Technologies used, and the deployment of those technologies, must tightly secure the network environment from internal and external attacks or breaches. Both proactive and reactive protection methodologies must be implemented to ensure mission-critical communications run unaffected by security events. Plus, centralized command and control of security policies must be realized for operational effectiveness.

In one example, a refinery in Port Arthur, Texas worked with Honeywell security experts to be sure it had covered the bases:

- **Network Security**: Define who has access to the system
- **Process Security**: Protect devices and equipment
- **Behavioral Security**: Define the individuals
  - Users inside the company
  - Users outside the company
  - The Uninformed
  - Malicious Software

**10. MANAGING A GLOBAL, MULTI-PLANT ENVIRONMENT**

To help customers cope with the complex open technology environment, major automation suppliers such as Honeywell Process Solutions have developed service offerings focused on the assessment, design, and implementation of process control networks. Open system Manage services address important issues ranging from network administration and security, to data recovery, software management, and performance management. They are a cost-effective alternative to maintaining an in-house process and can significantly reduce your total cost of ownership (TCO).

Remote PCN monitoring and management services can provide qualified outside IT specialists who monitor the availability of network infrastructure devices and connected systems, and establish a secure remote access facility for mission-critical systems. Remote services can keep tabs on bandwidth reductions, data throughput issues, error rates, and other problems threatening to impact production. It also ensures proactive threshold alarming on network devices, systems, and applications. Remote connectivity provides a means to deliver both proactive and reactive services, and is an effective tool for managing firewalls, patches, and anti-virus updates.

Centralizing all critical events and trouble alerts through a common notification service can let users focus on their core business while the automation supplier keeps tabs on the network. If a device becomes unavailable, an alarm notification event is triggered. Once an alarm is determined to be abnormal, plant personnel or the responsible vendor is notified.

**SUMMARY**

The move away from proprietary control platforms to open systems has provided plants with significant performance improvements and cost savings. However, this transition has also posed major information technology challenges.

End users with open systems connected into their business environments can no longer rely on their automation supplier to provide an “out of the box” system with the same level of security as a proprietary DCS. In many cases, plant engineers and operators are now responsible for increasingly complex open automation architectures, and the specialized IT support functions that go along with them. These challenges can be readily overcome by a combination of assessing vulnerabilities; designing and implementing secure, effective networks; and ongoing management of these systems by teaming with automation supplier to provide best practices and knowledgeable resources.