

IT is FUEL for AUTOMATION

Bridging the IT Automation Gap

CONTROL SYSTEMS QUICKLY LEVERAGE EXPLOSIVE GROWTH IN NETWORKED COMPUTING TECHNOLOGIES

Over the past 20+ years, the evolution of controls from mainframe-based to total distributed control has been fast paced. Before the explosion of the networked computing, Control Vendors relied on custom proprietary hardware and software. A vice president in a world leading Control Company made a profound statement seven years ago when he said:

“Presently, we are a 80% hardware company and a 20% software company. We are working to reverse that to a 80% software company and a 20% hardware company.”

Control manufactures can no longer rely on selling proprietary hardware and software systems because the life cycle costs are astronomical. Further, DCS and PLC manufactures are under greater cost pressures to differentiate their control hardware! This is accelerating the race to transform their companies to an intellectual property business by incorporating their knowledge in software. Hardware is becoming more scalable due to the open interoperable technologies, the most significant of which are:

1. **ASi Buss** - a serial bus technology optimized for cost effective integration of discrete I/O-wide multi-vendor interchangeable modules. (See www.asi-interface.com)
2. **PROFIBUS DP** - addressing medium speed and PA lower speed loop-powered field bus communications. (See www.profibus.org)
3. **OPC** - a non-proprietary technical specification that defines a standard set of interfaces based on Microsoft COM technology. (See www.opcfoundation.org)

4. **Foundation Fieldbus** - a single, open, interoperable Fieldbus developed with input from more than 140 companies, including leading process and manufacturing automation companies and end-users worldwide. (See www.fieldbus.org)

THE IT AUTOMATION GAP

How can Information Technology (IT) integrate with automation in a way that does not compromise the requirements of the control system?

In the 90's, manufacturing companies spent billions of dollars believing that Enterprise Resource Planning (ERP) systems were the best way to reengineer their processes to more profitable businesses. When customers asked the question: . . .

How do we integrate our plant automation systems with our business systems? The standard answer was: “That’s no big deal, we can do that later on.”

Well *later on* is NOW, and it is no surprise that integrating manufacturing automation and control systems with ERP is a *bigger deal* than was anticipated by business leaders. The control engineers knew there were going to be problems, but it was difficult to get management to listen. Though the CIOs have a direct path to top company management, plant control engineering is not represented on the board of directors.

The task at hand is to decide who, what, when, why and how the manufacturing automation systems can feed the business “applications.” Also, IT is faced with how to incorporate paper reports and translate them to real world actions. Control engineers that have the ability to intelligently converse with IT groups can save businesses from repeating the same mistakes as they move to the e-business world.

ARCHITECTURE--BOTH HARDWARE AND INFORMATION SYSTEM--IS KEY

Architecture-satisfying business drivers are dependent on the level of hierarchal plant computing. In the real world, many of the best ideas are born before their time. This is true of the famous Perdue model for process control. Computer Integrated Manufacturing (CIM) enterprise architecture was formalized in the 70s and 80s and generated great interest in academia and the manufacturing industries. Implementations consisted of millions of lines of code on mainframes with custom interfaces between applications. Much is still used today! Most programs had to play software “tricks” because the problem had to fit the computer space available. Fortunately for us today, this is no longer a major issue. Remember: look before you leap into the Promised Land.

For a more recent treatment of the work of Purdue University (West Lafayette, Ind.) Professor Theodore Williams and the CIM Reference Model Committee’s work visit www.pera.net. This work is less abstract than the original CIM reference model and is called Perdue Enterprise Reference Architecture (PERA). At the site, you can find a body of work that is more manufacturing and process-unit focused. The modeling concepts presented on the website are worth reviewing. Sound engineering principles which we use every day are presented.

“A pile of bricks is not a building...A random set of software and hardware is not an enterprise.” Gary Rathwell

Let’s take a quick look at a model that represents a typical enterprise and relate it to an oil refinery. All manufacturing enterprises are made up of three core elements.

- 1. Facilities** - Typical equipment that makes up a refinery are processes such as crude distillation units, Catalytic Cracking Units, delayed coking units and many others.
- 2. People** - Traditional staff in an oil refinery consists of management teams directed by chemical engineers organized to support the day-to-day operations and interfaces with higher management at other locations. Research and Engineering departments typically reside in different locations as well. The IT organization is typically directed from centralized locations to minimize cost or outsourced to larger IT companies.
- 3. Controls and Information Systems** - In many refineries, process control is considered a core activity, so the staff is part of the site makeup as well as part of the technical organization. Information systems, in many cases, are globalized and centrally managed.

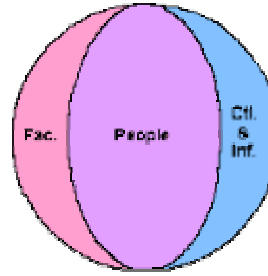
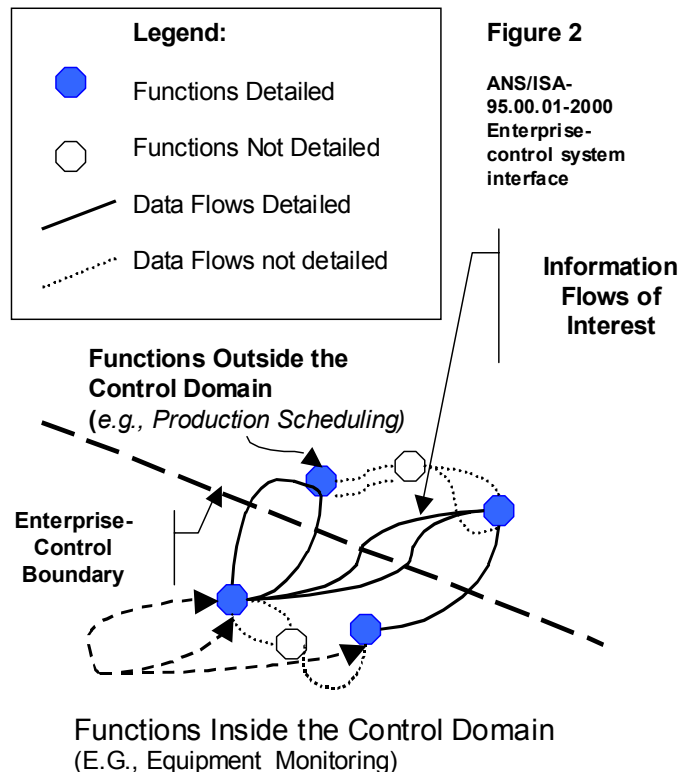


Figure 1. The PERA model

There are no quick fixes. Understanding the business needs between the process control and automation systems is what is sometimes called Information Engineering. It is a critical part of successful integration of automation systems and business systems. ISA and many other companies are working to define the interfaces between process control automation systems. There is no substitute for engineering. This requires a fundamental understanding of control engineering, chemical engineering, knowledge of the plant, computer network engineering, real-time databases, relational database systems, and engineered computer security to name a few. The place to start is by applying information engineering. Principles found in PERA, ANSI/ISA and the above-mentioned disciplines, including open interchangeable technologies, are critical to successful integration. Few companies have the breadth required to pull it all together.

ANSI/ISA-95.00.1-2000 Enterprise-Control System Integration Part 1: Defining the business process control interface boundary.



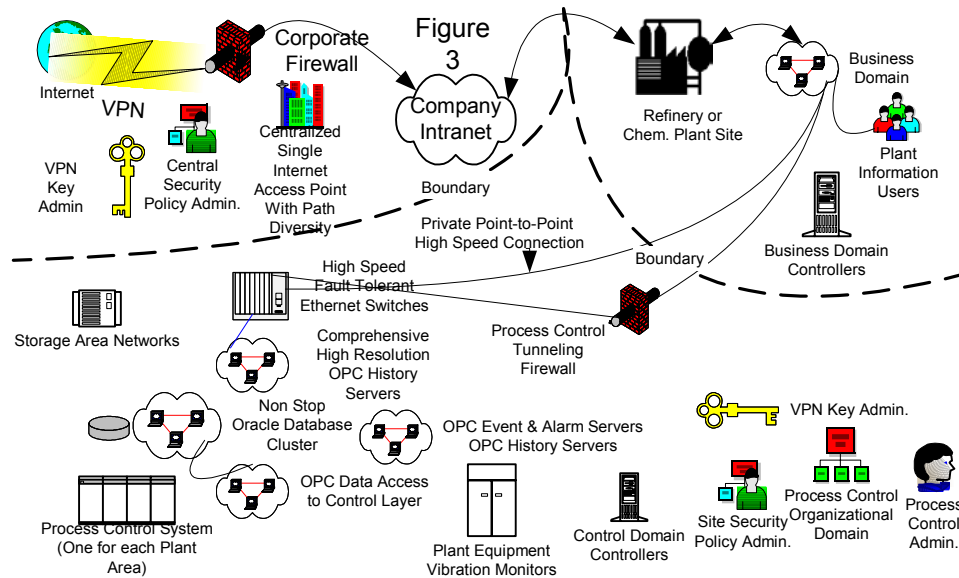
The ANSI/ISA model defines the terminology and functional hierarchy for integration automation to business systems (Figure1). Data flows are documented between the interface boundaries of controls. People have spent careers building expertise in process control, operations and Information Technology, and all need to effectively collaborate to define the interfaces needed to drive the process.

A hardware and software architecture, which has its genesis based on concepts formalized by CIM, is currently being applied at a major oil company. The five-year activity has invested over a billion dollars on a worldwide basis. It uses a distributed network of computers and LAN technology, but recognizes a true boundary is justified separating the control domain from the business domain.

DEFINING THE BUSINESS REQUIREMENTS TO BRIDGE THE IT AUTOMATION GAP

Careful planning is important when designing the hardware and software architecture to interface between the Control Domain and the Business Domain. Some of the more critical attributes to consider are:

- System availability for hardware and software components
- Control Domain information access must be predictable and scalable as load increases. It is best implemented by a dedicated private channel between the Business/Control Domain.
- Control Domain must be ultra secure to prevent unauthorized access and malicious manipulation of actuators
- Business functions should recover in the event of Level 4 systems failure once Level 4 systems are restored.
- Control Domain software upgrades and hardware additions do not affect service levels.
- Where practical, divide control functions by service and plant area so they can be serviced when a given area is shutdown for repairs.



The conceptual diagram in Figure 3 has three divisions: centrally administered functions, Business Domain administered functions and Control Domain administered functions. Many oil companies have global operations comprised of many sites. General company-wide security policies are typically administered from a central site. Largely to satisfy security concerns, most companies support private interconnecting networks through dedicated or leased lines—they comprise the company's Intranet system. The system interconnects all sites to form a connected enterprise.

VIRTUAL PRIVATE NETWORKS (VPN)

Competitive pressures to allow external companies to connect to the oil company enterprise are driving the need for secure encrypted access. Some companies are investigating leasing services for analytical measurements via Service Level Agreements (SLA). Analyzer vendors need direct access to their analyzers to evaluate the performance of the analytical measurements to ensure they meet the SLAs and to dispatch maintenance. This reduces the need for highly skilled and specialized analyzer technicians at each site. Deploying a VPN is a cost-effective solution to this problem.

OPC STANDARDS PROVIDE VENDORS NEUTRAL WAY TO IMPLEMENT CONTROL DOMAIN INTERCONNECTIONS

In the past, implementing an open information solution for a refinery or chemical plant computing system was not a choice. The evaluation of the vendor with the best proprietary solution was your best option. This is changing for the better.

OPC Foundation has open vendor interchangeable technologies to provide many of the needed data interfaces. This enables selection of best-of-breed components to build hierarchical information architectures. Important standards such as:

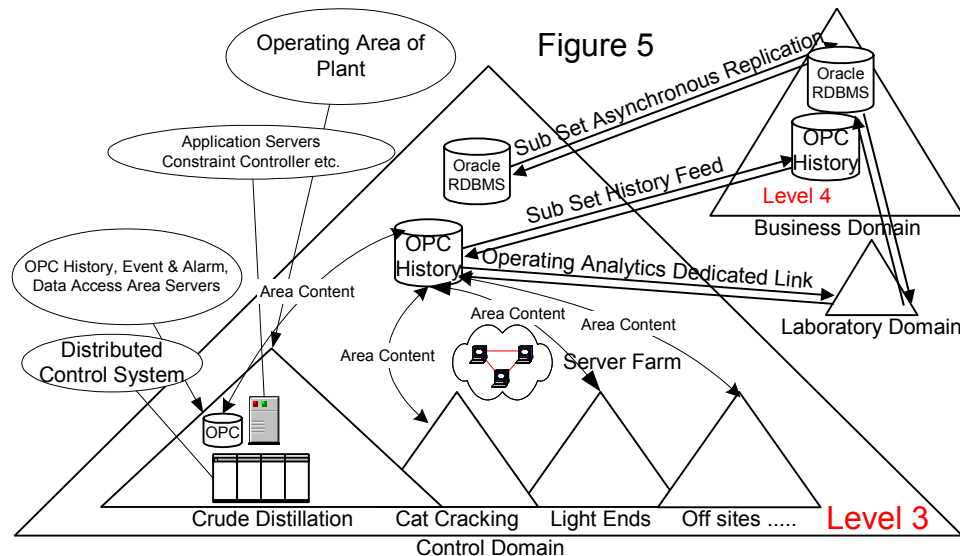
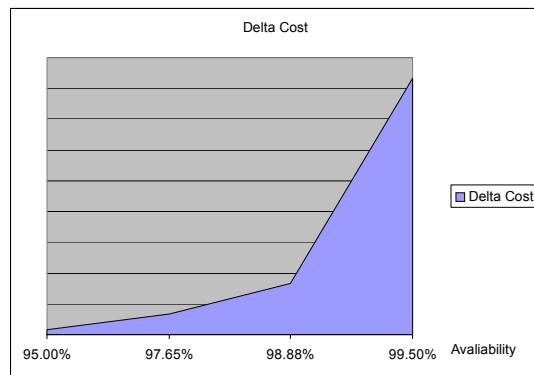
- **Data Access** for reading and writing data between an application and a process control device flexibly and efficiently.
- **Event and Alarm** mechanisms that allow OPC Clients to be notified of the occurrence of specified events and alarm conditions.
- **Historical Data Access** for reading, processing and editing data of an historian engine.

The dark side of open technologies is the user has the responsibility to design the system. In the past it was easy. You selected the vendor, and he told you how to configure the system. The vendor was the sole source of all technology. He had gateways for external interfaces and provided software drivers to integrate their system to your enterprise.

Designing today's Control Domain requires knowledge of computer operating systems, hardware such as Storage Area Networks (SAN), networking technology, control systems engineering, control technology such as multivariable constraint control, laboratory information systems, distributed control systems, to name a few. Cost trade-offs must be considered in the design. Control Domain's high availability and complexity is economically justified. This is true for non-stop operation in a continuous processing industry. This is also valid in some batch control situations where delays caused by poor control system availability negatively impact production. Relative cost increases for higher availability are presented in Figure 4.

Figure 4:

Source: Gartner Research, June 29, 2001



RESILIENT CONTROL DOMAIN ARCHITECTURE

Figure 5 is a model based on PERA concepts to deliver hierarchical levels of control. Also indicated are the Business Domain Level 4 interfaces. Each plant's operating area contains its own OPC history

servers. They are redundant and enable one server to be removed from service for general maintenance without the loss of history services. The servers have interfaces to the distributed control system and/or area PLC's. Upper-level control servers are redundant and provide a non-stop platform to support multivariable

constraint controls and unit optimizers. The unit optimizers could optionally run on a control domain server farm. Interfaces to the operating area machinery monitoring are connected to the redundant OPC servers to integrate unit-operating data with equipment reliability applications.

The Oracle relational database provides a high availability and robust relational database platform to support non-stop operations. Many of the process control applications such as blending, product shipping, alarm management; alarm summary and statistics are aggregated from the event and alarm OPC servers.

The time horizon for the Control Domain consolidated OPC history server is the longest area unit run length plus one year (a typical number is five years). This enables evaluation and analysis to be conducted throughout the entire run length of the unit. The content of this history server is comprehensive and contains history on all control attributes critical to understanding the control actions taken by the system. In a large refinery, the number of parameters in history is typically greater than 600,000 parameters. Contents include present value, output, range information, limits such as output, setpoint and controller mode. Having a comprehensive system allows detailed analysis of control system performance. As new ideas to analyze the quality of controls and needs for new controls are developed, there is no need to wait for history to accumulate. A comprehensive Level 3 history system has the history ready for analysis. The content of the Control Domain servers also includes information generated from calculations, and they are also information stores for process simulation output. This output is generated from process simulators and can be reconciled against the actual unit performance for new control strategy development.

The comprehensive Control Domain is the data feed for the Business Domain Server. Typically, this Business Domain server contains a subset of the data maintained at the control server. The duration of the Business Domain servers is 20 years of data. The Business Servers can recover from the Control Domain servers so the system design does not require the same degree of availability as the Control Domain. Note that the volume of information flow is methodical. Good systems design supports a dedicated point-to-point high-speed connection to support access to the Control Domain. All user information flow goes through the process Control Domain firewall. A limited and tightly controlled user population from the Level 4 Business Domain is gated through the firewall to satisfy business needs. The VPN connection is used to enable keyed encrypted access from the Internet to specific points in the Control Domain.

Laboratory Domain integration is critical and requires a dedicated link from the laboratory system since updates to models that are used in closed-loop control need reliable and consistent data flow.

CONCLUSIONS

1. As US and European standards are coordinated, the playing field for vendor independent, interchangeable systems and services will change for the good of all.
2. Bridging the IT automation gap requires application of standards such as the ANSI/ISA 95.00.1-2000 to clearly define interfaces between the Control and Business Domains.
3. Open standards are changing the way EPR systems are delivered and interfaced by applying Information Engineering methodologies such as PERA.
4. Virtual Privet Networks (VPN)'s are displacing leased lines to interconnect the enterprise.
5. Increased cost for high availability applications is justified for the Control Domain.
6. Specialized vendors will be able to better compete with the "All – In-One" vendors and provide better-integrated solutions.
7. Compliance with recognized industrial standards are fundamentally improving the way systems are designed and procured.



Craig Schiro, President, InfoTech Engineering Co., Baton Rouge, LA, has 22 years experience in the petrochemical industry including principal architect for a plant computing network linking control and business systems for a major oil company. He may be reached at craig.schiro@infotech-eng.com.