The Connected Factory

How Technology Trends are Reshaping the Way Things Get Made

JIM PINTO,
Managing Partner
JimPinto.com
Automation Industry Analyst
Technology Futurist

"The connected factory of the future will be distinguished by seamless connectivity between all networking and compute layers, and distributed, intelligent, autonomous I/O. It will deliver greater process efficiency, wider agility in operations and a more robust level of performance."

Executive Summary

The quick-paced and global nature of our economy today is effecting a sea change in the industrial automation industry—a level of change not seen since the automation revolution nearly 40 years ago. Manufacturing has become more competitive as extremely agile and low-cost producers come online and undercut long-established vendors. Customers meanwhile require ever-faster innovation and shorter product cycles, something traditional manufacturers cannot easily deliver. Along with increasing automation complexity, these trends suggest that vendors need new and more agile processes—now.

Because veteran manufacturers built their businesses and factories on proprietary systems and processes that in themselves were meant to deter competition, they cannot quickly and easily adapt to these new threats. What makes factories so unresponsive to changing marketplace conditions is their proprietary nature. Although highly automated, most factories use purpose-built technology to control and operate their production processes. There are multiple problems with this approach including the fact that any changes to the processes require new systems and devices—a lengthy and costly process in itself. In addition, the device and control layers on the factory floor cannot exchange information with the business and data networks that runs the company. People must be intermediaries, interpreting information and translating it into actionable data between the networks.

Manufacturers are beginning to recognize how traditional automation systems are hindering their ability to respond quickly to changing demands and effectively compete in today's global economy. In this regard, they are rethinking the components that add time and cost to their manufacturing processes. Several technology trends are emerging as a result, including: the move to open, standards-based compute architectures; platform consolidation; and, the convergence of automation processes.

What will eventually follow is the connected factory, a place that is distinguished by seamless connectivity between all networking and compute layers in the factory and distributed, intelligent, autonomous I/O. The connected factory will deliver a more robust level of performance, greater process efficiency, wider agility in operations to adapt to changing global conditions, and more seamless operations.

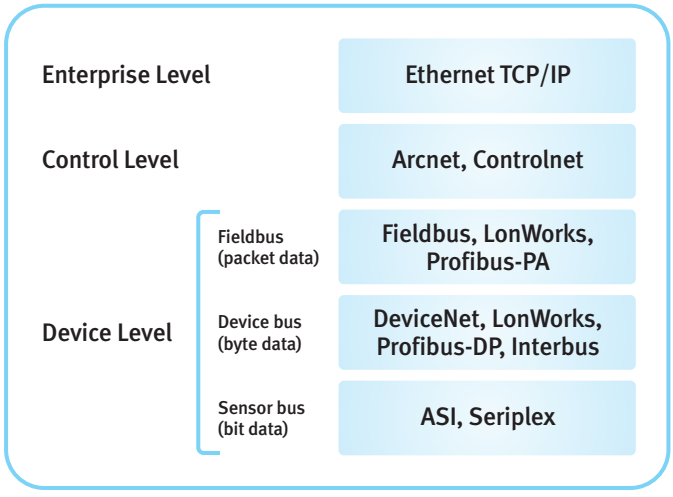
A Historical Perspective

Factories have been mostly automated for the past four decades and little has changed during that period. The same technology deployed in the 1970's is mostly in use today, although incremental advances have been implemented to increase output and introduce new complexities to the process. Meanwhile, technology itself, and especially computing technology, has undergone massive change. (More on that point later.)

Within the automated factory there are three levels of network, as illustrated in Figure 1—device level networks at the lowest level, control networks in the middle level, and enterprise networks at the top. By design, each of these is "closed" to the others and was developed at a time when open, general-purpose computing architecture wasn't suitable—or reliable—within the rugged environment that surrounds most manufacturing processes. Manufacturers purposely built proprietary systems that could give them a competitive advantage by making it difficult for competitors to copy their processes and/or products. Lengthy factory design cycles gave manufacturers time to recoup investment and build profits.

But products have shorter life cycles today and customers demand immediate reaction to changing marketplace trends. So factories built on proprietary systems and closed networks are being built at a time when the world expects more agility.

Figure 1. Three levels of networking in the automated factory



Opening Up the Factory

In an effort to become more responsive to customer demands and facilitate interchangeability between vendors, manufacturers began moving on a limited scale to adopting standards for networking technology within and between the three automation layers. Many such standards proliferate in industrial networks and are not necessarily compatible with standard IP networking protocol.

As a result, these systems remain isolated from the business side of the industrial enterprise and must be maintained separately. Some vendors support one networking standard and not others, so the challenge for manufacturers is still that of keeping current with closed technologies.

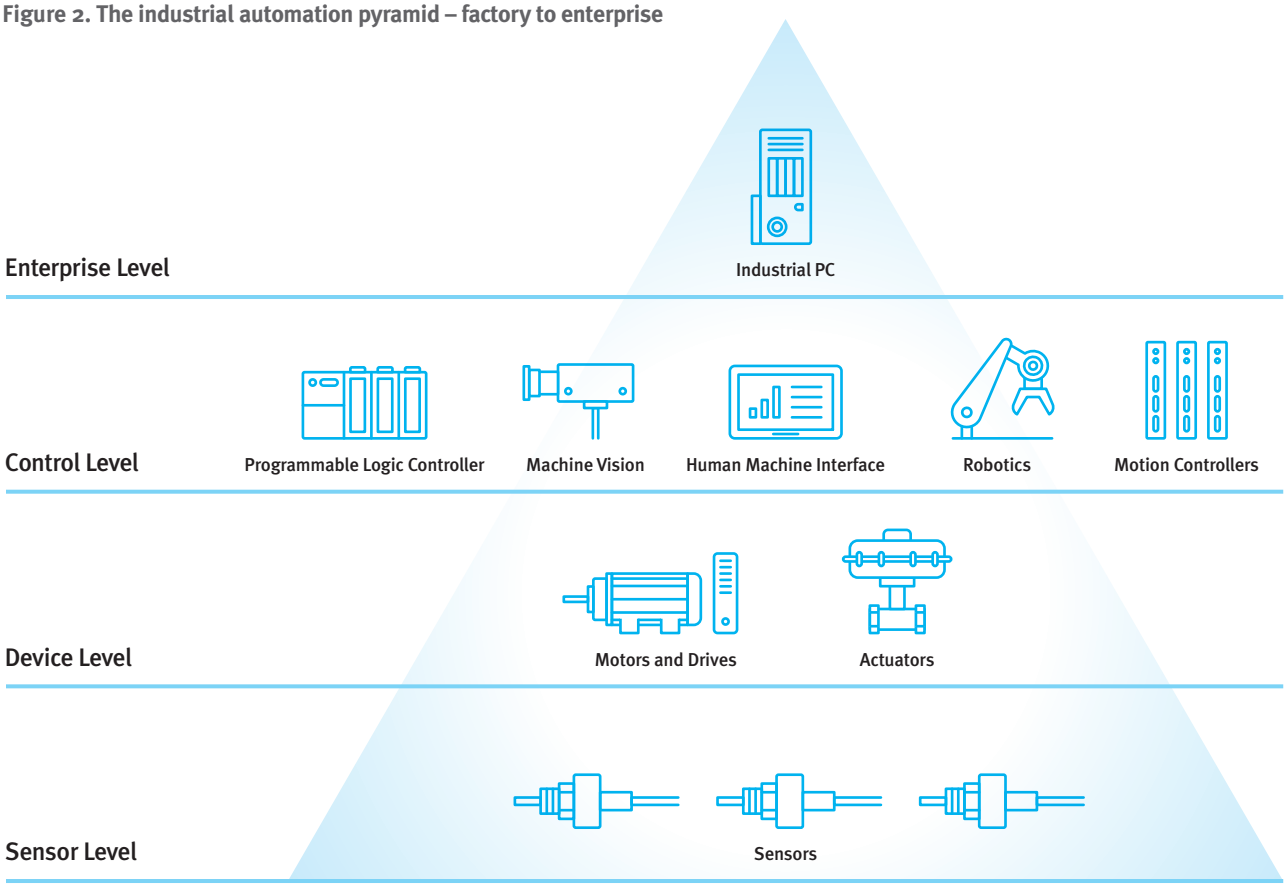
When considering the use of more general purpose and mainstream computing platforms and IP networking protocols, the logical question that arises is how open technology can possibly be applied to the very complex and highly specialized processes employed in automation. After all, the broad category of automation products encompasses all manner of specialized gadgets and instruments—controllers, sensors, displays, recorders and actuators—and a wide variety of systems with a mixture of those products, plus software and services. These devices bear no resemblance to a "computer" per se. And there are very few requirements for high quantities of any particular product—hardly any millions of anything. Millions of products are used, but many are specialized variations related to particular industries and requirements.

That said, these complexities might be summarized in basic terms as simply an assortment of various I/O: the measurement, processing and control of a variety of inputs and outputs. In automation and manufacturing processes, such inputs can include temperature, pressure, flow, level, speed, weight, position. Outputs are switches, solenoids, valves, heaters and other actuators, which are manipulated based on control algorithms related to desired values. And measurements may be displayed, recorded and controlled, with trending, alarming and a variety of other features and functions required for a wide range of processes and factory requirements.

The factory is often compared to a pyramid, with a large number of sensors and actuators spread out at the lowest levels, connected to consolidating I/O blocks at the machinery and systems levels, and those in turn connected to computers and controllers at the factory level, all networked into the enterprise system, as illustrated in Figure 2 (next page).

Once it is realized that factory processes boil down to I/O, it's easy to understand how general and open computing architecture might be applied to the connected factory. Beckhoff*, the fast-growing German-

Figure 2. The industrial automation pyramid – factory to enterprise



based manufacturer of industrial computers and I/O automation devices, embraces the use of open computing architectures. According to Beckhoff's* Gerd Hoppe: "One factor of Beckhoff* success is the focus on automation functionality delivered on the mainstream platform in general computing, which continuously delivers improvements in price/performance. Customers benefit significantly from adopting an open, mainstream architecture because the entire chain of tools, applications, training, knowledge and personnel has a worldwide base."

On that note, mainstream computing architectures have changed drastically in the past few decades. Industrial computer architectures are built to withstand the rugged and harsh conditions found on the factory floor and can even set up virtualized platforms that support both real-time, deterministic operations and enterprise operating systems on the same chip. What's more, these devices already support the common networking protocols found in communications and general purpose networks today, making them highly suitable for the consolidated, converged, connected factory of the future.

Consolidating Platforms Using Open Technology

One of the first developmental efficiencies to be gained in using mainstream platforms, or general purpose computing architecture, is the ability to consolidate task-specific devices onto a single platform. Andy Thome, Embedded PC Product Manager at Beckhoff*, suggests that the complexity of next-generation automation solutions requires such consolidation:

"Automation will have a growing demand to integrate ever more algorithms and perform a multitude of automation tasks in the same CPU environment (e.g. as central controller) to even better resolve complex automation tasks related to a vast variety of inter-dependencies." This means, "automation will grow to implement a mix of logic, motion, safety, XFC (extreme fast control) math algorithms such as simulation, vision, Ethernet, and other communication and more tasks such as validation, scientific methodologies, instrumentation, data acquisition, etc., to handle process requirements with complex dependencies on materials, resources, environment, process and tools in the most intelligent way imaginable."

Figure 3. Migration path for automation products towards unified systems architecture

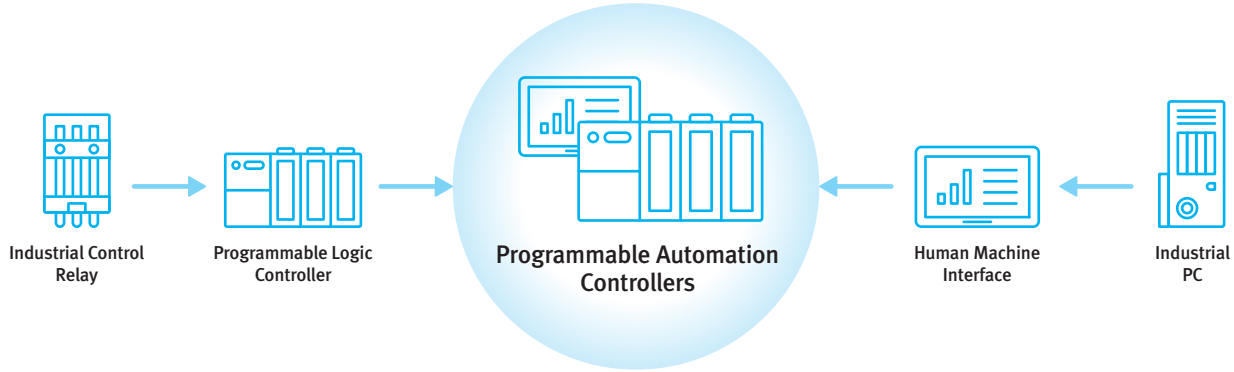


Figure 3 shows the migration path as relays, embedded controls, programmable controllers and industrial computers merged and consolidated into standardized industrial computing architectures.

Consolidation can take two routes: vertical integration of functions through the different automation layers, and horizontal integration to collapse multiple control functions onto a single device. A lot of the consolidation taking place today is of the vertical sort, combining the industrial computer or HMI with the real-time control layer. This enables greater use of open, modular architectures, flexible and configurable enough so users can customize and optimize it to meet particular needs using components for controlling and automating both machines and plants. All parts of the system are designed to maximize software and hardware integration. There can be one programming and engineering tool for the complete system. This capability includes transparent access for all parameters and functions within the entire system, combining PLC, SoftPLC, remote I/O, motion control, drives, PID control, user guidance, visualization and data handling, along with a maximum integration level to the enterprise though the use of Ethernet TCP/IP, Internet, and IT standards. Horizontal device integration includes more related functionality into the same, more versatile industrial computer product—including HMI with control algorithms and a variety of operating functions in the same box.

"The technology of the chip must contain within it the concerns of robust behavior, hard real-time, virus protection, and real user interfaces. Taking a page from all of the application contenders and combining them into one technical package is difficult but doable."

DICK MORLEY,
"Father of the PLC"

Dick Morley, acknowledged "father of the PLC", discusses the growth of computers in industrial automation: "Industrial monitoring and controls represent a growth opportunity. Analysis of systems indicates that large complex systems fail often and have little ability to respond. The future system will consist of small boxes that are intelligent, do data manipulation with local control.

"The system of the future will have a proliferation of multitasking computers both in the local area and in the system arena. Fast, secure communication between processors is important. What most industrial users care about is robust performance–that the equipment never freezes, always supplies reliable service and is virus free."

Connecting to the Internet

It should be noted here that industrial networks today are adopting IP protocols and general purpose computing architectures as new systems are introduced. This is because of the many benefits available simply by being connected to the Internet and the enterprise. In the factory and process control environment, the islands of automation of the past are steadily melting way with the connection of virtually everything to everything else, to central networks and the Internet. Although there is a long way to go before such transformation is complete, the revolutionary result will be a proliferation of "the connected factory."

The Connected Factory Gains Momentum

The trend toward adopting the computing and communications standards born out of the IT domain—what has been described earlier as general purpose or mainstream computing and IP networking protocols—is quickly gaining speed. While manufacturers have used Ethernet for some time in proprietary ways, the use of the standard, routable TCP/IP networking protocols really distinguishes the current convergence.

The term "Industrial Ethernet" is typically used to describe any of the Ethernet based protocol solutions for industrial use. The more fundamental protocol of importance is TCP\IP as the network and transport protocols that enable the so called "Industrial Ethernet" protocols to take advantage of enterprise equipment (Ethernet based and others) as well as be routed into the enterprise.

It is important to note that this process is not simply a matter of taking enterprise equipment and plunking it down in the factory. Industrial Ethernet cannot match IT systems identically because they must support industrial-focused application protocols. Plus, these industrial nets are almost exclusively flat, switched networks. The switch-based network has been key to overcoming concerns about determinism in a collision-based network such as Ethernet. Enterprise networks are typically organized in subnets separated by routers; industrial networks cannot typically accept the non-deterministic delays introduced with routers, and they are only used at the edges of the network.

EtherNet/IP extends commercial off-the-shelf Ethernet to the Common Industrial Protocol (CIP)—the same upper-layer protocol and object model found in DeviceNet, ControlNet and other industrial networks. CIP allows EtherNet/IP system integrators and users to apply the same objects and profiles for plug-and-play interoperability among devices from multiple vendors and in multiple sub-nets. EtherCAT and MODBUS TCP/IP are examples of enhanced, industrial Ethernet protocols which promotes transparency from sensors to enterprise systems.

The evolution of integrated architecture on EtherNet/IP simplifies networks and helps drive plant-wide optimization. Touting EtherNet/IP as the world's leading industrial network makes clear the mission to help enable plant-wide control, visualization and decision support, with the ability to manage all applications–manufacturing, process-control, safety systems, motion controls and drive applications—all on a single network. Because Ethernet is highly cost-effective, the benefits of employing this technology within factories makes great sense.

The convergence of the plant-floor networks to the business enterprise via EtherNet/IP solves another problem: that of getting manufacturing data to the decision makers on the business side to enable more accurate and informed decision-making. Of course the move also optimizes internal assets and support resources through adoption of a standard protocol. The interface between traditional control engineering roles and IT department roles is changing as Ethernet blurs the distinction between IT and manufacturing.

A Word About Security: Stuxnet

The closed and proprietary nature of traditional automation networks has rendered them relatively immune from security threats. As the factory floor has started opening up to IP network access and general computing systems, it has also been opened to the nasty bugs that travel there.

The July 2010 discovery of Stuxnet, a Windows*-specific computer worm, brought with it the realization that critical computer infrastructure can be vulnerable to malicious code.

Stuxnet, which has still not been traced to the source, spies on and reprograms industrial controls and hides its changes. Automation suppliers are all developing security technology solutions at all levels of hardware and software. And this is a major concern for everyone in the industrial automation field.

Stuxnet changes the playing field in more ways than just increasing awareness. It has also changed the way future malware will be written and will impact industrial controls systems," noted Eric Byres, Chief Technology Officer of Byres Security Inc., an acknowledged expert in industrial automation security. Stuxnet "has shown that it is relatively easy to create malware that can break the chain of trust between a controller's logic and its I/O and then use this to cause serious safety issues in any process."

He goes on to note that the downside is that "unlike in the IT world, we cannot simply load firewalls or VPN software into these devices to address these security issues. Nor can we update their firmware is any significant way. So the only hope to is to install some sort of security mitigation at the point that the controllers connect to the control network. In other words we need a controls-aware security chip, board or module, either in every switch port or as a module right in front of the CPU."

Conclusion

The large, centralized production plant is a thing of the past. The factory of the future will be small, movable (to where the resources are, and where the customers are). In the old days, this was not done because of localized know-how and investments in equipment, technology and personnel. Today, those things are available globally. Services migrate worldwide to the best low-cost providers. Knowledge moves easily and can be transferred anywhere. Naturally, these processes move more easily if automation systems are based on open systems that all use the same computing and communications language.

Initiatives in security and low-cost/low-power processors will generate significant new growth at all levels of the automation pyramid during the next 3-5 years. Standard computer/network architectures will spread into all corners of the factory and plant floor.

In the 5-10 years timeframe, industrial automation systems will shift from deterministic, hierarchical type controls towards smaller, more distributed processing and intelligent, autonomous I/O. This will bring major advantages such as robust system performance, predictive diagnostics, and the ability to operate seamlessly with multiple device networks.

0811/MB/PDF 325867-001