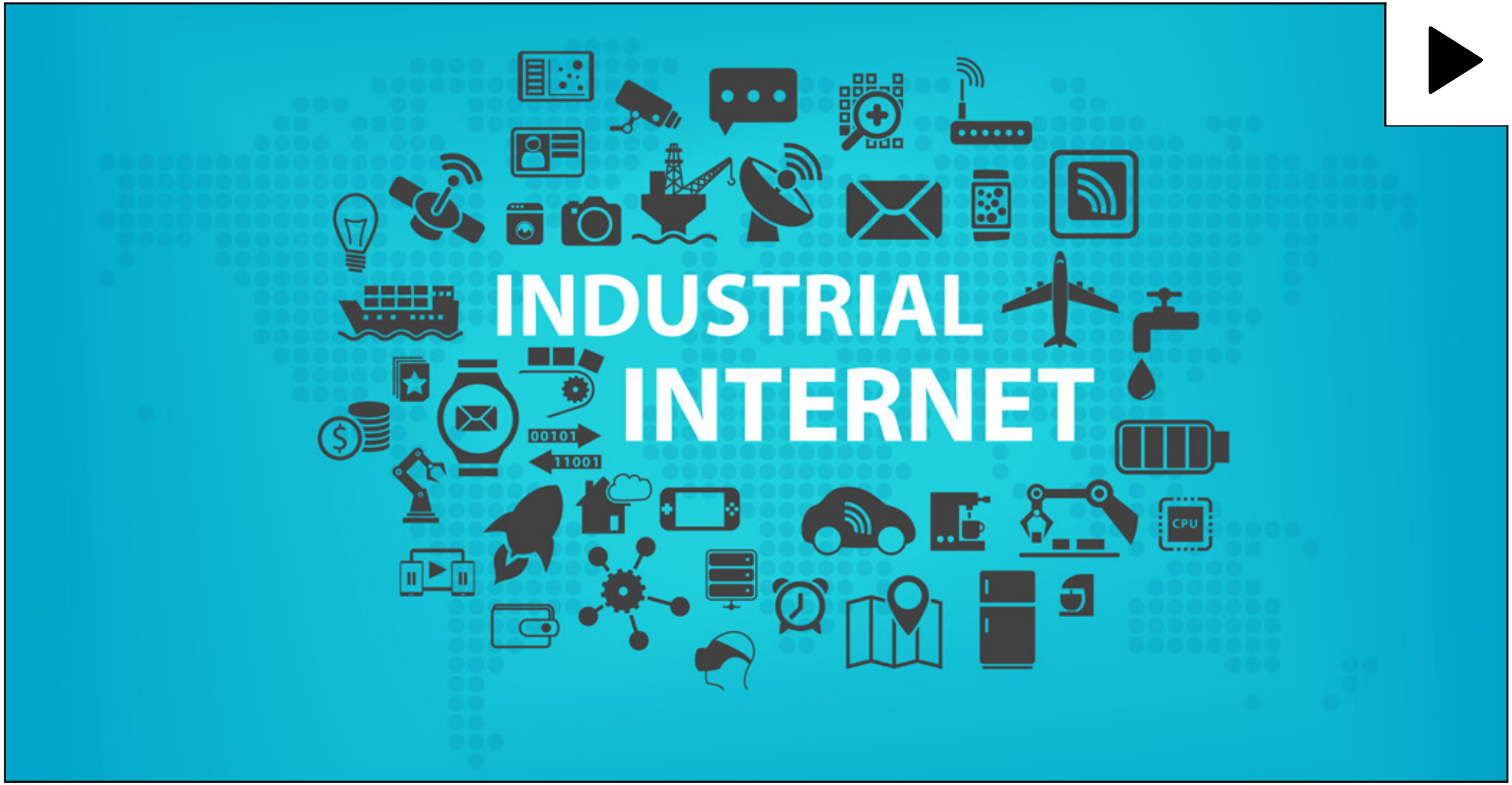

AutomationWorld® TACTICAL BRIEF

Next Level Network Integration:

Reliable networks hinge on the integration of IT and OT, safety controls and time-sensitivity

CONTENTS

The Challenge of IT/OT Convergence in Manufacturing

Many manufacturers still see strong resistance to bringing information and operational technologies together, with mistrust coming from both sides. That needs to change.

By Luigi De Bernardini, CEO, Autoware

The convergence of information technology (IT) and operational technology (OT) is one of the key mantras in smart manufacturing. This convergence has many different faces with several organizational and technical implications.

OT typically refers to the control and automation technologies supporting operations, which historically have been intentionally separated from IT. This separation originally generated from the different technologies involved and the different skills needed. Early IT systems were proprietary, required internal programmers and were used to calculate finance-related figures, including payrolls or commercial transactions. At the opposite end, OT consisted of turnkey, proprietary systems designed to operate only on vendor-specific equipment.

With the more pervasive use of IT technologies at the operational level, things are changing from a technical point of view. Some simple examples include the usage of Microsoft technology with continued adoption of SQL databases to collect and analyze production and process data; the rapid adoption of Ethernet-based communication protocols at the machine level; the rapid diffusion of web-based user interfaces; and the increased popularity of mobile solutions to access data and perform tasks requiring Wi-Fi networks at the shop-floor level.

Nevertheless, there's still strong resistance to change at the organizational level. Most of the clients I talk with still have two strongly separated departments for operations and IT. They have different people, goals, policies and projects. They not only operate in a very separate way, but sometimes they even have conflicting approaches, like they're fighting to expand supremacy and take control of Middle-earth (or avoid doing that). And, worst of all, they do not seem to trust each other.

This is a situation that needs to be solved urgently. Continuing to operate separately not only slows the adoption of solutions based on technologies that fall outside of operations' comfort zone, but also exposes companies to fault or security risks that could significantly impact production.

To rectify this situation, some strategic and organizational challenges need to be addressed. First, the strategies of the IT and OT departments need to be aligned. Responsibilities need to be unified, or at least the IT and operations managers (CIO and COO) need to have partly common and overlapping goals and targets, which would force them to work cooperatively. A joint task force—if not a specific department—with joint governance and responsibility must execute projects, harmonize duplicated or overlapping systems and processes, and promote the development of the interdisciplinary skills that are now missing in most companies.

This is not a process that will happen overnight, nor can it happen

Continued
The Challenge of IT/OT Convergence in Manufacturing

solely based on a change in the organizational chart (although that does need to be done). It's a cultural shift that requires time, effort and a progressive plan.

One of the first things to do (after having put the organization in place) is to identify simple pilot projects that can offer tangible value and a low-risk benchmark for the company. These projects should not only provide a good opportunity to train resources and progressively develop the specific mix of IT/OT skills in the team members, but also help managers learn to share goals and develop a new shared governance model to effectively and continuously support the initiatives.

The difficulty in developing an effective governance for IT/OT projects should not be underestimated. IT typically has stronger models than operations for managing projects; they cannot just be taken as they are and applied to OT. The cooperation between IT and OT needs to extend to adapting those models for use in operations, considering the different impact of projects and the different culture of the involved stakeholders.

Being smart in manufacturing is the only option. That's not new, but you must adapt quickly to stay smart in such a rapidly changing environment. Effectively solving the IT/OT convergence challenge is a must. It's not a short journey, so get the journey started as soon as possible.

Is Integrated Safety Acceptable Now?

Many in industry agree that it is. Fewer automation professionals seem to be holding onto the idea that processes will be safe only if the safety controls are kept separate from process controls.

By James R. Koelsch, Automation World Contributing Writer

No one wants safety to be an afterthought, a function imposed upon a well-designed process. For a growing number of manufacturers, that means they are replacing separate safety and process controls with control schemes that instead integrate the two functions. Once considered by many as a dangerous practice because of concerns about common-cause failures, integrated safety is coming into favor for the benefits it offers.

Integration not only eliminates hardware redundancies and reduces wiring to drive costs down, it also simplifies programming, assists alarm monitoring, and promotes better diagnostics.

Paper Converting Machine Co. (PCMC), a machine builder based in Green Bay, Wis., prides itself on its machine safety stance. “We differentiate ourselves from competitors by guiding our customers through the safety process and educating them on the opportunities safety presents,” explains Jason Stover, senior electrical project engineer. PCMC has climbed aboard the integrated safety bandwagon.

PCMC uses Rockwell Automation’s GuardLogix integrated platform to help its engineers design safety from the outset into upgrades of the company’s tissue converting, packaging, flexographic printing and non-woven technologies. With the integrated controls, the engineers can perform a risk assessment and define functional-safety requirements early in the design process. Then they can use it to verify and validate the safety system once the design is complete.

Because the process and safety controls are on the same platform, the engineers work in one programming environment. The common platform also permits sharing information between the controls to contextualize machinery operation and information, according to Steve Ludwig, safety programs manager at Rockwell Automation. This allows designing both safety and productivity into a machine from the beginning for maximal efficiency.

Complexity is the reason why PCMC chose the GuardLogix platform over other forms of integration, such as simply sharing a backplane or power source or linking a process controller to a safety controller over a network. “If there are only a few safety functions, a few safety relays may be fine,” Ludwig offers. “Separating the standard and safety logic devices makes sense if you have a small number of safety functions and no need for diagnostics and safety information.”

As complexity increases, however, so does the need for a configurable safety relay or an integrated controller platform. “For moderate to complex machines, the balance tends to weigh heavily in favor of integrated control systems, especially in applications that require data sharing between control and safety tasks,” Ludwig says.

Continued
Is Integrated Safety Acceptable Now?

Paths to integration

Other automation vendors echo Ludwig's point in various ways. John D'Silva, safety technology manager for factory automation at Siemens Industry, says that industry is balancing cost with its need for reliable automation. "The failure or error rate of standard automation technology under normal circumstances is acceptable for many operations, but not for high-risk applications," he says. Examples of high-risk applications include presses, robots, chemical processes, high-pressure operations, burners, and fire and gas sensing.

D'Silva compares the situation to deciding how to send a letter. "Normal delivery is expected to be as affordable as possible at a certain reliability level," he says. "Everybody, however, will use special mail for important messages."

Today, integrated safety is increasingly being perceived as delivering the expected reliability. "The traditional concept of separate conductors for safety signals and non-safety signals goes away when all this data can be consolidated onto one fieldbus that can carry both types of signals," explains Dan Klein, fieldbus technology manager at Turck. "As long as the safety function is maintained, there is no need for a separate network infrastructure."

To establish the necessary communications, many automation vendors have adapted the fieldbus technologies they were already using in general-purpose I/O to consolidate wiring, reduce complexity and cost, and enhance diagnostics. The key development driving this adaptation has been safety network protocols that establish fail-safe operations over existing general-purpose fieldbuses.

One example of this, highlighted by Klein, is of a shared communications bus operating as a "safety monitor" on an AS-Interface communication network. Here, safety control occurs at the monitor, and process control is at the

AS-Interface master. Another example he offered is an Ethernet system where multiple masters can share the same communication network to provide safety and non-safety control independently.

AS-Interface is an early example of I/O combination in a device-level fieldbus protocol. "The concept has since been extended to other widely adopted protocols, including CIP Safety over DeviceNet and EtherNet/IP, and Profisafe over Profibus and Profinet," Klein says. OpenSafety, an open protocol for safety communications over "black channel" Ethernet (more on "black channel" later in the article), has also been a critical development for manufacturer-specific safety solutions over industrial Ethernet, he says.

Consolidate to one network

The one-network concept has become a popular method for establishing integration. "Most users have become more comfortable with it and are even demanding it," notes Deana Fu, product manager at Mitsubishi Electric Automation. "While some users still prefer separation at the controller level, they see the benefit in better data sharing over one network, which simplifies maintenance and troubleshooting."

An example is Mitsubishi's iQ-R Series platform, which has independent controllers for process and safety control. Not only do the controllers sit on the same platform and share the same core components, such as power supply and peripheral devices, but they also sit on the same CC-Link IE Field network and are programmed using the same software package.

"The two independent controllers communicate with each other through a shared high-speed data bus that is tightly synchronized and is not affected by I/O and network traffic," Fu says. "There is no wiring or gateways between the two controllers, eliminating unnecessary points of failures."

The one-network concept is finding use not only in machinery and discrete parts manufacturing, but also in the chemical and oil and gas industries, where incidents can result in extremely expensive failures, environmental damage, or even human fatalities. "These users are generally more comfortable with a hybrid approach where the main process and safety functions are physically separated at the controller level, but integrated at the network level for information sharing, diagnostics and monitoring," Fu explains. The greater visibility helps operators resolve problems quickly as they arise.

Built-in redundancy and protection layers on today's networks mitigate the risk of having common points of failure when both controllers are on the same network, according to Fu. "We've built a loop-back feature into a ring network topology that allows communication to continue without interruption, even when a station or cable is disconnected," she says about CC-Link IE Field, an integrated network over industrial Ethernet. Consequently, a faulty station can be disconnected from the network without affecting communications among the other stations, and substations can take over the

Continued
Is Integrated Safety Acceptable Now?

network if the master station experiences an error.

Don't overload the bus

One of the challenges for implementing integrated controls is not overloading the bus. Response times can become unacceptably high if you put too many devices on the network. "So you need to make sure that the throughput is right for all the data on the network so that you can maintain the safety integrity levels (SILs) for the application," advises John Sullivan, project director at DMC, a Chicago-based system integrator. "Vendors have certainly made that easier by setting up high-priority channels on their networks for safety information."

An example of a high-priority channel is the "black channel" that Profisafe establishes on Profibus and Profinet, the networks that DMC prefers to use on its projects. Safety PLCs also give priority to safety functions.

Profisafe adds the black channel to an existing network as software. Safety information flows through the black channel, but it uses the same basic communication protocols used by the rest of the network. "The Profisafe protocol has no impact on the standard bus protocols," Siemens' D'Silva says. "On the other hand, it should be as independent as possible from the base transmission channels, be it copper wires, fiber optics, wireless or backplanes. Neither the transmission rates nor the error detection mechanism plays a role. For Profisafe, they are just black channels."

Despite such remedies, reaction times can slow down as the amount of communications traffic increases. Although response times are usually sufficient for the SILs in most discrete-parts manufacturing, there are instances where they are not, Sullivan says. "It, for example, may be difficult to justify integrated safety for an

overhead-crane application that needs millisecond response times," he says. "Also, bigger lines and large process applications often have so much data that separation tends to be better."

Even so, Sullivan does not think that hardwiring is inherently safer than integrated controls, mainly because hardwiring restricts options. He points to how integration made it easier to group equipment in a project that he and his colleagues completed recently for three floors of equipment at a food manufacturer. In this application, they were able to create overlapping safety zones. One e-stop, for example, could control five pieces of equipment, and the next one could also control five, yet both could share two pieces of equipment between them.

"It's technically possible to do that with hardwired safety, but it's usually too complex and costly to be practical," Sullivan says. "With a safety-rated PLC, it's relatively easy." Hence, he believes that integration can enhance safety in ways that had been impractical in the past.

Profisafe allows integrating a variety of safety devices on networks. Drives are an example. "Nowadays, they can provide safe states without de-energizing the motor," D'Silva says. "For example, the new SOS [safe operating stop] feature holds the motor under closed-loop control in a certain position." Consequently, users need not always cut power completely to put a device into a safe state.

A case against integration

Although integrated systems can often save money and enhance functionality, not everyone is convinced they provide enough safety. "We think that it's wrong to integrate control and safety because it runs the risk of common-cause failures," says Buddy Creef, director of North American sales at HIMA Americas, which provides stand-alone safety automation.

The risk comes from the similar, identical or even shared components that usually come with integration. "If you're running control and safety on similar pieces of hardware, operating systems or I/O networks, then you run the risk of the same problem causing a failure in both," Creef argues. "Control and safety need different operating systems, configuration programs and networks. By differentiating the two, there is never one problem that would make them both ineffective."

And integrating control and safety is not the only way to control costs and enhance functionality, Creef adds. Developments in safety instrumented systems (SISs) can help, too. Manufacturers like HIMA have exploited the faster processors, multitasking architectures and high-speed communications available today to develop increased diagnostics and what HIMA calls sequence of events. "We can report on up to 20,000 different actions in the system within 1 ms," Creef says.

These reports can flow directly into the alarm-and-events applica-

tion of a basic process control system (BPCS) through a one-way connection. Because establishing such links can be a hassle for users, HIMA has done much of the work for them. Engineers at its DCS Labratory in Germany have developed the necessary methods for the major brands of DCSs and have published them in manuals.

Although the pendulum has certainly swung in favor of integrated control and safety systems in many quarters, Creef believes that it is beginning to swing back. “Several major users who have accepted integrated systems in the past are no longer accepting them,” he says.

In pursuit of IT security

One company that has reverted is Bayer CropScience, a German manufacturer of crop-protection products. Concerns over IT security have convinced the company’s Process Control Technology (PCT) group to change its mind about integrating safety and control. “Now, we use a separated solution when we build a new plant,” says Bernhard Holzenkamp, senior manager of global PCT.

This policy applies to both controls and networks. “You also have different engineering stations and different databases,” Holzenkamp notes. Wherever possible, he and his colleagues specify hardware from different vendors to avoid common failure modes and create more layers of separation.

Now, the only common point is the human-machine interface (HMI), which the company uses to view process information from both the SIS and the BPCS. “We usually do that with a redundant Modbus connection,” Holzenkamp says, “but there are no safety signals going through it.” The traffic goes only one way to make activity in the SIS visible on the BPCS’ HMI.

The new policy is already being implemented in a nearly completed expansion in the herbicide production at the company’s plant in Muskegon, Mich. The SIS is from HIMA and the BPCS is a DeltaV system from Emerson Process Management. These systems oversee a process consisting basically of a continuous reaction, a formulation operation, and a packaging operation.

“It’s a mid-size project,” Holzenkamp says, not-

Pre-Configured Industrial Distribution Frame (IDF)

The Pre-Configured IDF is specifically engineered to deploy and protect rack mount Ethernet switches in industrial applications. Extra-depth allows room for cable management, power management, and switch stack cables and accommodates up to 5 switches. The innovative design provides consistent equipment deployment with faster installation and can significantly lower the risk of downtime due to switch overheating.

ing that about 70 pieces of new equipment and 800 I/Os are being installed. Because the project is an expansion of an existing facility, the company elected to continue using the conventional 4-20 mA wiring in combination with remote I/O used in the rest of the plant, rather than introducing new fieldbus technology.

In the past, the company had installed integrated systems mainly to reap the benefits of dealing with only one vendor. Holzenkamp also points to other benefits, such as less training for personnel, fewer system interfaces, easier access for remote-service providers, and greater simplicity from having just one database and one engineering station.

When you do an IT security assessment, however, these advantages often disappear. "For example, one engineering station is no longer an advantage," Holzenkamp says. "It may be better to create a physical separation that prevents access to one system from the other." At Bayer, the preference is to go so far as to put the safety and process control cabinets in separate rooms whenever possible.

The Muskegon facility has both the safety and process control cabinets in the same room. But to add a measure of security, the engineering station for the SIS remains disconnected and locked away in the control cabinet until the engineering staff needs it to make modifications.

So far, Bayer has no plans to replace existing integrated systems with separate ones. The PCT Group, however, has begun reassessing IT security on each of the company's integrated systems so that it can be strengthened wherever necessary.

4 Reasons Why Time Sensitive Networking Matters

With a new IEEE standard in the works, Time Sensitive Networking is quickly moving past the concept stage for industrial automation use.

By David Greenfield , Director of Content/Editor-in-Chief Automation World

Chances are good that you've likely heard the term Time Sensitive Networking (TSN). Chances are also good that you're not completely clear on what it is and what it means for industrial automation. After all, TSN is a communication standard designed by IEEE for streaming of audio and video data. In fact, before adopting the TSN moniker, it was known as Audio Video Bridging (AVB). The name change came as IEEE sought to expand the scope of the standard.

TSN has been garnering a lot of attention in industrial automation circles due to the rise in interest around the Industrial Internet of Things (IIoT). Though much of the data collected by industrial sensors and control systems in an IIoT application are not time sensitive, there will also be a great deal of "mission-critical, time-sensitive data that must be transferred and shared within strict bounds of latency and reliability," says Todd Walter, chief marketing manager at National Instruments (NI).

Since existing IT and industrial Ethernet networks are "defined by IEEE 802 standards—which specify requirements for different Ethernet layers and functions and ensure interoperability between devices—industrial suppliers, IT vendors and silicon providers are collaborating within IEEE 802 and the recently formed AVnu Alliance to update standard Ethernet protocols…for time-critical data in IIoT applications," Walter says.

That's where TSN comes in—to ensure this mission-critical, time-sensitive data is not held up on the network, which will be increasingly congested with IIoT data.

Walter says the AVnu Alliance, working with member companies such as Broadcom, Cisco, Intel, and NI, will drive the creation of an interoperable ecosystem through certification, similar to the way the Wi-Fi Alliance certifies products and devices to be compatible with the IEEE 802.11 standard. Walter serves as the industrial segment chair for AVnu Alliance.

With TSN poised to play a larger role in industrial networking, Walter points to four key benefits of TSN for industry:

- **Bandwidth:** Large data sets from machine vision, 3D scanning, and power analysis can put a strain on network bandwidth. Proprietary Ethernet derivatives commonly used for industrial control today are limited to 100 Mb of bandwidth and half-duplex communication. TSN will support full-duplex standard Ethernet with higher bandwidth options such as 1 Gb, 10 Gb, and even the 400 Gb version in IEEE 802.3.
- **Security:** TSN incorporates top-tier IT security provisions. Segmentation, performance protection, and temporal composability can add multiple levels of defense to the security framework.
- **Interoperability:** By using standard Ethernet components, TSN

Continued
4 Reasons Why Time Sensitive Networking Matters

can integrate with existing brownfield applications and standard IT traffic. In addition, TSN inherits many features of existing Ethernet, such as HTTP interfaces and web services, which enable the remote diagnostics, visualization, and repair features common in IIoT systems.

• **Latency and Synchronization:** TSN prioritizes the low-latency communication required for fast system response and closed-loop control applications. It can achieve deterministic transfer times on the order of tens of microseconds and time synchronization between nodes down to tens of nanoseconds. To ensure reliable delivery of this time-critical traffic, TSN provides automated configurations for high-reliability data paths, where packets are duplicated and merged to provide lossless path redundancy.

Explaining how TSN is capable of providing these benefits, Walter says that network interference with mission critical data is avoided through the use of "time synchronization, scheduling, and time-aware traffic shaping. The traffic shaping will use the schedule to control logical gating on the [network] switches. The non-time-sensitive traffic is blocked during specific time-windows to ensure that the egress port is ready when the time-sensitive traffic is expected. The time synchronization to control the schedule and traffic shaping is accomplished using IEEE 802.1AS, essentially a profile of the IEEE 1588v2 standard."

The IEEE 802.1 Time-Sensitive Networking Task Group and the AVnu Alliance are currently working on the TSN standard for industry. Walter says portions of the standard and working references from vendors will begin to appear this year. In the meantime, you can learn more at: http://www.ieee802.org.

Secure and Stable Networks for Connected Automation

No matter how many things you can get connected, the benefits don't add up if the network they're on is flawed.

By Michael Belfiore, Automation World Contributing Writer

Six hours into an eight-hour process at a pharmaceutical plant, production hit a fatal snag and shut down, essentially flushing $100,000 down the drain. The problem: A software update came at just the wrong time. What would have been a routine update in the IT world proved a costly mistake in the world of operational technology (OT).

Welcome to the brave new world, where IT and OT intersect in ways that plant operators couldn't have imagined just a few years ago. That intersection is allowing companies to streamline processes and maintenance, and connect vendors and suppliers with data to save time and money. Except when it doesn't go as planned.

In the case of the pharmaceutical company, the problem was a window that popped up on an interface to ask the operator if he would like to update the software. Choosing to update resulted in a reboot of the batch server that was running a medicine-making process—and the loss of vital genealogy required by the U.S. Food and Drug Administration (FDA).

It was, as Gregory Wilcox, global technology and business development manager for Rockwell Automation, later put it, "a really bad day." The batch was ruined and the pharmaceutical company could only call in Wilcox and other experts to recommend policies, procedures, technology and training to help make sure that kind of mistake was never repeated.

Despite the potential pitfalls, the benefits of connected automation—machines and processes that share information with each other and the businesses that operate them as well as with customers and suppliers—are legion, and growing all the time.

"Connecting plant-floor assets with the enterprise, and connecting manufacturers and suppliers can offer tremendous value," says Scot Wlodarczak, a manager for industry marketing at Cisco and a spokesperson for Industrial IP Advantage, a trade group dedicated to education about industrial information architectures. "In fact, it's estimated that four out of 10 companies will be disrupted in their market position by companies fully embracing connected factory solutions."

Key to realizing those benefits is mitigating the potential risks—which, fortunately, can be done with proper planning and use of already-established best practices. It starts with getting off on the right foot.

Connecting the dots

Laying the groundwork for connected automation starts with an evaluation of what an automated process or factory already has to work with, and where managers want to go with it, says Tony Shakib, vice president of Cisco's IoE Vertical Solutions Engineering organization. The starting point is what Shakib calls level one—just getting the component pieces, including machines, connected and sharing data.

An important consideration here is how tightly to link IT and OT

systems, says Ryan Lepp, director of business development for industrial automation and the Internet of Things (IoT) for Panduit. “Is your end goal a completely converged network, where IT and OT coexist?” he asks his customers. His recommendation is for as unified a network as possible to reduce costs.

Once machines and processes are sharing data, Shakib says, companies deploying connected automation can proceed to level two—making use of all that data. Predictive maintenance is one benefit to be achieved at level two. “By having a constant connection monitoring the health of these devices, quite often you can predict when something’s going to go down months ahead of time,” he explains. Reducing or eliminating downtime is an obvious benefit, saving millions of dollars for manufacturers.

Also at level two, data can flow the other way, back to the machines. “Rather than having to spend hours changing a machine over manually to work with a different product, the machine has devices onboard that automatically can get changed almost just with a recipe,” says Robert Miller, senior manager of strategic collaborations and partnerships at Mitsubishi Electric Automation. The recipe (information about how to build a new product) instructs servos and other parts of each machine to reconfigure themselves to handle products of different sizes, shapes and weights.

Level three connects a factory with outside suppliers and customers, potentially extending the benefits of connectivity to the entire supply chain. But greater connectivity presents greater security risks. “End users need to adapt and embrace these new business models to remain competitive,” Wlodarczak says. “However, turning traditionally siloed industrial networks into borderless industrial Ethernet networks shared with suppliers can open up new attack vectors.”

Fortunately, careful planning and best practices can prevent a bad day.

Securing the network

Proper security practices operate on multiple levels, Wilcox says. “We always recommend to customers that they use a holistic defense-in-

IntraVUE

Automation networks are susceptible to interruptions which often result in downtime, and lost production. While conventional tools are frequently unable to detect many types of network interruptions, IntraVUE provides the capability to identify and report information critical to improving uptime of the Industrial Ethernet infrastructure.

depth approach," he says, which should address security at the physical, electronic and administrative levels.

Physical security not only restricts physical access to certain areas of the plant, but also prevents machines and controls from connecting to the wrong networks or devices. Source: Rockwell Automation

Security at the physical layer can be as simple as restricting physical access to certain areas of a plant to only those who need to be there. That's an approach all too often overlooked, Wilcox says. "Unfortunately, sometimes our customers have what's commonly referred to as an M&M approach to security," he says. "It's hard candy outside and it's soft and gooey inside. Once you get past the perimeter, whether at the receptionist or even a guard, at times there are no procedures to actually track visitors." Access control provided by locked doors opened by ID badges can go a long way toward mitigating this potential security risk.

Physical security can also extend to physically preventing machines and controls from connecting to the wrong networks or devices. This can be ensured with cables that will not connect to the wrong places. Panduit, for example, makes cables and connectors that foster this level of physical security. "We have an entire line that can be used to configure and construct the physical security of a network," Lepp says.

At the electronic level, says Miller, the right kind of network can ensure that only known devices are able to share data, Miller says, noting that CC-Link IE is an Ethernet-based network that provides this level of security. "CC-Link IE is inherently deterministic and inherently secure because of the technology and the communication that it uses," explains Miller, who serves as director for the Americas for the CC-Link Partner Association. "Unless the network controller knows about a certain device, that new device will not be able to communicate across that network." In other words, he explains, "You couldn't just walk up to a CC-Link IE network, plug into it with a laptop and hack into the system."

Finally, administrative access controls should restrict users to only parts of a network or to software that they have been authorized to use. Packages like FactoryTalk Security from Rockwell Automation can help system administrators establish the appropriate levels of access to software and hardware based on who is logging in to the system from which locations.

Stabilizing the network

As the example with the rebooting batch server at the pharmaceutical plant exemplifies, greater connectivity also can present challenges to maintaining uptime. Uptime is often less critical in the purely IT world than it is in the operational world, and bringing operational-level uptime to a converged network is the name of the game for many plant operators.

Step one in ensuring network uptime is simplifying wherever possible, Lepp says. That requires planning. "If there's no strategy or

plan," he explains, "you develop this nest of communications, where you may have critical points of failure."

Planning should include such factors as ensuring that switches have enough capacity to handle the volume of data passing through them. "That is something that's going to become more and more of an issue," Miller says. "As more devices become available to be put on a network and to monitor through the network, there's going to be more and more data." And more data increases the risk of network congestion, which can bring a process to a grinding halt.

Lepp cites the case of a food and beverage plant whose network teetered on the brink of collapse at any given moment because of too much network traffic. "If you added anything, it would crash the network," he recalls. "If you took that extra device out, the network could recover and you could start the machine again." Lepp and his team solved the problem by carefully assessing the network and then redesigning it to handle more data.

Such reconfigurations could include what's known as zone architecture, Lepp says. "What a zone architecture does, is it pulls the switches out of a control panel and puts them into a rafter or higher level, then you disburse the backbone network off into individual zones," he explains. That way, even if a control panel does go offline for any reason, the distributed switches keep the network and the systems that depend on them up and running.

In addition to reducing data loads, zone architecture promotes redundancy, another key to enhancing uptime. This can extend to cables as well as to switches. Lepp and his team make sure that there are backup data lines connecting switches, controls and machines. Equally important is that the lines don't all follow the same route. "If you have got redundant fiber lying in the same pathway, then the physical location isn't redundant," Lepp says. "As soon as you hit that with a forklift, your network is down."

The future of connected automation

Cisco and Rockwell Automation have collaborated on the Converged Plantwide Ethernet

Increase Your Network Security

Prevent unauthorized access or accidental breaches by establishing a robust physical network infrastructure that offers barriers to network-wide security risks through the use of an integrated physical and logical architecture that includes Panduit Micro Data Centers

(CPwE), an evolving set of reference architectures for connected automation. Each partner maintains its own labs where best practices are designed and tested before being added to a growing library of reference materials. For example, a white paper released in June outlines use cases for deploying industrial firewalls. Panduit also recently introduced physical infrastructure recommendations for the reference architectures.

All of which should help plant engineers and operators in the future avoid the kinds of problems faced by the pharma manufacturer and its errant software upgrade process. In that case, Wilcox says, plant managers were able to keep the problem from happening again through additional operator education (don't accept a system upgrade while a batch is running), improved communication between IT and OT departments (don't try to upgrade production servers while they're running), and preventive controls (critical systems are only upgradable on maintenance days). "To my knowledge, that customer has never had an incident like that again," he says. "A little pain upfront, but it was a happy ending."

Call it growing pains on the way to a new world of connected automation.

Industrial Ethernet Diagnostics

Proper diagnostics and support of your Industrial Ethernet network will save you money, conflicts with other departments, and plant or equipment downtime.

A simple act such as connecting a new device, or changing the configuration of a switch, have shut down production lines and created downtime losses in the thousands. Don't think because you are not responsible for the infrastructure, or are using an outside support organization, that this will prevent or help identify the problem. Frequently the problems are unique to Industrial applications.

Major companies have recognized the need to provide local support for these time critical real-time networks. They also realize that the local plant floor resources are the best way to reduce downtime. These resources however require an easy to use solution that will assist them to prevent or minimize the occurrences of these problems. IntraVUE has been selected by some of the largest Food & Beverage, Pharmaceutical, and Automotive companies to support their applications.

What companies within Food & Beverage, Manufacturing, Forest Products, and Municipal Markets are saying about IntraVUE:

"We had a process control network melt down the other day. I was able to use the IntraVUE as a troubleshooting tool to get the issue isolated and ended up swapping out a bad network switch that for all intents and purposes, appeared to be operating properly from the front lights but was dropping links worse and worse. It took us a little over an hour to get the mill back up and running."

"I just wanted to let you know that IntraVUE just saved me an 80-mile roundtrip to the plant on a Saturday night just to change-out an Ethernet PLC module. Since I was able to quickly identify the issue by simply looking at the live IntraVUE network status I just had one of our onsite employees swap out the module."

"We had a switch go down on Friday and I could immediately tell what was happening. The live view provided an accurate and real time view which allowed our support people that are not network experts to fix the problem quickly."

"IntraVUE allowed us to easily identify servers and their network connections which had to be replaced. The live view gave us the ability to be sure no other computers were disturbed in the process."