Control Systems

- Reliable EtherNet/IP control systems
- Case study: Control system retrofit
- Motion control system choices
- Evolution of data management
- Mitigating process control safety risks
- DCS and SCADA in digital transformation
Control Systems: Choices and Challenges

Whether you’re working on motion, process or safety control systems, you probably have questions. What do I use to upgrade the controls on turbine peaking plants? How do I build reliable EtherNet/IP subnetworks for this factory floor control system? How do I choose feedback methods when designing motion control systems for robots or mobile machinery? It’s one project, but controls engineers have to know everything from data management techniques to safety system standards—or at least know where to go to get up to speed quickly. That’s why you’ll find so many useful bits and diverse sources in this edition of AUTOMATION 2021. You can learn about the roles of DCS and SCADA in digital transformation or dig into a case study about retrofitting a distributed control system. Also discover how technology makes it possible to operate multiple virtual machines on a single hardware platform, essentially turning a motion control system into an edge server. Automation and control technology changes fast. The subject matter experts we’ve gathered here are key resources for the challenging puzzles you need to solve today, and in the future.

Renee Bassett
Chief Editor
The Roles of DCS and SCADA in Digital Transformation
By Kevin Finnan and Wataru Nakagawa, Yokogawa
Requirements for open architectures and enhanced cybersecurity, driven by digital transformation, will shape the future of these systems.

Case Study: RDI Controls Executes Control System Retrofit
By Josh Eastburn, Opto 22
An engineering services company designed distributed control systems to retrofit three turbine peaking plants.

How to Mitigate Process Control Safety Risks
By Scott Hayes, MAVERICK Technologies
Prevent potential catastrophes before they occur by applying proper safety procedures and standards.

Advancing Automation Requires an Evolution in Data Management
By Juan Carlos Bravo, Sergio Diaz, and Neil Wang, Emerson
Integrated, contextualized data improves flexibility and speed to market without impacting production.
Five Recommendations for Reliable EtherNet/IP Control Systems
By John S. Rinaldi, Real Time Automation
Build reliable EtherNet/IP subnetworks on Ethernet for factory floor manufacturing systems using these five tips.

How to Choose Between Standalone Encoders and Integrated Motor Feedback
By Christian Fell, POSITAL-FRABA Inc.
Designers of motion control systems for robots, manufacturing equipment and mobile machinery have options.

How a Motion Control System Turned Edge Server
By Michael Reichlin, Real-Time Systems
Operate multiple virtual machines on a single hardware platform without impacting the controllers' real-time core.
The road to industrial autonomy is open and variable, offering myriad choices for operational excellence. Whether your company is at the start of its journey or well on its way, Yokogawa enables smooth transition from industrial automation to industrial autonomy—IA2IA. Key to that transition is OpreX, our evolving suite of solutions and products comprising control, measurement, execution, and lifecycle that will help customers optimize everything from business management to operations. Yokogawa. Advancing your IA2IA.
The Roles of DCS and SCADA in Digital Transformation

Requirements for open architectures and enhanced cybersecurity, driven by digital transformation, will shape the future of these systems.

For decades, industrial control systems have played an important role in industrial automation by allowing process manufacturers to collect, process, and act on data from the production floor. Currently, these systems are in transition. Ongoing technological and industry developments have paved the way for DCS and SCADA systems to support digital transformation.

Process manufacturers typically employ DCS and SCADA technologies to monitor and control the operations in their facilities. The DCS was designed to replace individual analog and pneumatic loop controllers, which were cumbersome when applied to very large processes such as refineries. SCADA originated as a solution for operations that span broad geographical areas, for example, pipelines and utilities. Later, a variant that uses an HMI in conjunction with PLCs evolved for plant automation applications.
However, DCS and SCADA systems are now doing much more than simply monitoring and controlling. They are integrating with additional intelligence at every level of the industrial automation architecture to facilitate predictive asset lifecycle management and value chain optimisation while advancing the stakeholder experience and improving security and safety. Although this particular industrial control system transition is already underway, the larger transformation of industrial automation systems has only recently begun.

**Distributed control systems**

At its core, a DCS is a platform for the automated control and operation of an industrial process or plant. A DCS uses local area networks (LANs) to interconnect sensors, actuators, controllers, and operator terminals for process control. While it originally served the need to control large continuous processes such as refining and petrochemicals, it was subsequently extended to batch processes.

**SCADA systems**

Although SCADA systems originated by serving applications that require broad geographical area coverage, the concept evolved with the inception of PC-based HMI, which replaced more expensive minicomputers in the 1980s. Instead of a wide area network that interfaces with remote terminal units (RTUs) at locations such as pump stations, a typical in-plant SCADA system uses Ethernet for communication between the HMI and PLCs. In the in-plant category, the SCADA system architecture shares many similarities with DCS architecture. In the remote scenario, a SCADA system can connect corporate operations with multiple plants, each of which uses a DCS. Process manufacturers can use these enterprise-wide systems for data communications without facing geographical restrictions.

Essentially, DCSs and SCADA systems both play important roles in plant automation. Despite this similarity, however, key differences separate these two types of systems.
The differences between DCS and SCADA

The differences extend far beyond the fact that a traditional SCADA system can work with a wide area network whose bandwidth is much lower than in a DCS LAN.

A key distinction is that a DCS uses distributed workstations for operator HMI. Each workstation can communicate directly with controllers on the DCS LAN. In a SCADA system, all communications between HMI workstations and PLCs will funnel through a server. Thus, the server is a single point of failure, the failure of which could render the entire process essentially invisible to all users.

While the architecture of a DCS and a SCADA system might otherwise appear identical, the DCS includes numerous, often subtle features such as redundant electronic circuits, which increase the system availability and minimise downtime. Redundancy extends to remote I/O: all remote I/O electronics and the communication networks between them and the DCS controllers are, or at least, could optionally be redundant.

While SCADA HMIs and servers are typically commercial off-the-shelf (COTS) PCs, a DCS uses non-COTS components that are optimised to the task. In addition, in a DCS, the Windows operating system is kept isolated from the process, which enhances cybersecurity. A deterministic DCS LAN guarantees that a critical message such as a high priority alarm, will indeed arrive at its destination. The SCADA system typically relies instead on the high bandwidth of the LAN.

Since a single DCS vendor typically supplies the entire system, components such as controllers and workstations are more tightly integrated than they are in a SCADA system. Common benefits include simplicity or reduced engineering costs. Still, for a given process, a DCS will be more expensive than a SCADA system, but in processes for which unplanned shutdowns are very costly, the price difference is justified. While SCADA suppliers could deploy redundant servers or high availability computing platforms to make those systems more reliable, their availability will not be as high as a DCS.
One advantage of a PLC over a DCS is the processing speed. A PLC typically offers significantly shorter cycle times to scan I/O points and execute control and logic operations. Although DCS and PLC technologies have largely converged, their origins are completely different. While the DCS evolved from analog and pneumatic PID loop controllers, the PLC was originally a replacement for hard-wired relay logic panels. In discrete logic processing, speed is of the essence, and a PLC will perform such logic processing much faster than a DCS would.

The DCS was designed for continuous PID loop control in process industry applications, in which the PLC provides much less of an advantage in cycle processing time. An application with a combination of continuous control and discrete logic control will typically use a DCS for the former and a PLC for the latter. Often, the DCS will integrate with a PLC, which has been supplied on a skid-mounted process unit such as a turbine-driven centrifugal compressor. Some DCS vendors have developed very efficient interfaces for such situations.
DCS and SCADA systems both comply with the ISA95 Purdue reference model architecture. The first level – the field level – of the automation pyramid includes devices, actuators, and sensors on the production floor. The second level – the control level – uses PLCs and proportional integral derivative (PID) controllers that interface to field-level devices. SCADA systems traditionally act as data funnels, transporting a broad variety of information for process control, asset management, historical analysis, and IT applications. A DCS will often use multiple servers – which could be part of, or considered to be, a SCADA system – to communicate with corporate and IT systems.

A modern DCS or SCADA system will interact with several software and hardware components. Each resides in the first and second levels of a manufacturing control operation and pulls together all five levels of the automation pyramid. Because of this, it acts as the glue for digitalisation, quickly facilitating a flow of information through processes from the plant floor to the boardroom.
The evolving role of DCS and SCADA with digital transformation

Both DCS and SCADA systems are undergoing transformations in line with broader digital transformation trends, such as the Industrial Internet of Things (IIoT). This transformation comes with the promise of improved industrial automation capabilities and value for process manufacturers.

New challenges that end users have brought to light have prompted vendors to consider how it would be possible to reimagine operational technology (OT) automation systems using COTS and information technology (IT) components. End users require that vendors incorporate best-in-class COTS hardware and software to create automation systems that surpass the reliability, security, and end-user value of today’s DCSs.

They also desire a system that enables them to preserve their control strategies by porting them into upgraded or new systems. In addition, end-users have requested modularised hardware elements – computing, networking, storage, and I/O terminations, for example – to allow for incremental upgrades. Finally, they would like software that has been decoupled from the hardware and I/O to allow execution anywhere in the system.

How is digital transformation changing DCS and SCADA?

Forward-looking process manufacturers are investing in digital transformation, and DCS and SCADA are ultimately part of such efforts. As a result, they are evolving alongside all other process manufacturing technologies. Changes to DCS and SCADA systems fit within the ongoing transformation of the automation pyramid, which is also evolving. IT/OT convergence and virtualisation technologies, for example, are blurring the distinctions between the pyramid’s levels and enabling the migration of some engineering and software applications to the cloud.
With the integration of cloud technologies, process control systems can perform edge computing and serve as robust data sources for the IIoT. Cloud-based environments facilitate the convergence of data across multiple sources and improve data availability to support insightful decision-making and application interoperability.

What are the requirements for SCADA and DCS in digital transformation?

To take advantage of cloud technologies, the IIoT, and edge computing, process manufacturers need to modernise their aging automation systems. On the whole, the drive toward digital transformation has created a need for a more open and secure system architecture and design.

Increasingly open systems

The NAMUR Open Architecture (NOA) and Open Process Automation Forum (OPAF) are driving major open architecture initiatives in industrial automation and prompting a shift away from proprietary architectures. Both initiatives describe vendor-neutral systems that allow the use of
state-of-the-art equipment and functions at all times and the continued use of proprietary software applications in the future.

A key OPAF objective is to transition away from vendor lock-in, which has historically been an issue with large DCSs. The requirements for the architecture currently being considered by OPAF are interoperability, modularity, standards conformity, compliance with security standards, scalability, and portability.

In the case of NOA, an independent domain called M+O (monitoring and optimisation) is prepared separately from the existing system, and data is directly collected from robots, drones, and new sensors, for example, for corrosion, sound, and vibration. Furthermore, data in the existing system is imported by OPC UA, and advanced control, analysis, and diagnosis can be realised even in the field. From the viewpoint of security measures, compatibility with zone design recommended by IEC62443 is enhanced, and system design and maintenance can be easily performed.

More problematic is a lack of continuous upgrades from some DCS vendors. If their vendor ceases to provide upgrades, manufacturers are compelled to resort to a rip-and-replace approach, in which the old system is completely replaced by an entirely new one. In this scenario, the production loss and costs incurred while transitioning to the new system often far outweigh the system cost. By creating an open, interoperable specification, OPAF aims to foster the development of less expensive and improved process control systems.

**Increased security**

Digital transformation has created a need for secure network architecture and design in addition to increased openness. Security is especially important as IT/OT convergence and new technologies, such as cloud computing, introduce new security risks.

Since exposing data to the Internet presents security risks, it is vital that process manufacturers keep their SCADA systems up-to-date using contemporary cybersecurity resources. The International
Society of Automation’s (ISA) 62443 series of standards – which the International Electrotechnical Commission (IEC) has adopted – and the National Institute of Standards (NIST) 800-16 offer helpful resources and guidelines for network administrators and cybersecurity engineers.

Since their data exchanges typically rely on radio or public communication infrastructure, SCADA systems are more vulnerable to cyberattacks. As they oversee wide area networks, there are more points of entry. Meanwhile, a DCS is also not completely secure from cyberattacks and requires comprehensive measures, particularly on entry points into LANs.

A new standards-based approach to cybersecurity has been designed to encompass IT and OT systems. While OT typically uses the NIST cybersecurity framework, IT requirements and interactions with third parties could involve additional standards, such as ISA/IEC 62443 and ISO 27001.

While integrating IIoT technology, IT/OT convergence implementation teams will continue making decisions regarding the

<table>
<thead>
<tr>
<th>YOKOGAWA’S CYBERSECURITY PORTFOLIO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assessment and Analysis</strong></td>
</tr>
<tr>
<td>Security Assessment</td>
</tr>
<tr>
<td>OS Patch Management</td>
</tr>
<tr>
<td>Malware Inactivated Service</td>
</tr>
<tr>
<td>User/PC Setting Management</td>
</tr>
<tr>
<td>Backup Recovery System</td>
</tr>
</tbody>
</table>
segregation of OT networks from corporate networks, OT network isolation from the Internet, least privilege access controls at site and process levels, and cross-site communication restrictions. Meanwhile, cybersecurity domain expertise is evolving to encompass the formerly disparate OT and IT domains.

**What does the future look like for DCS and SCADA?**

Requirements for open architectures and enhanced cybersecurity, driven by digital transformation, are likely to continue shaping future DCS and SCADA developments. As a result, these systems are currently in transition, but the digital transformation journey for industrial automation systems has only just begun. This journey comes with challenges for process manufacturers — for example, upgrading a
legacy system can seem incredibly daunting at the outset. But the potential benefits of digital transformation make addressing such challenges more than worthwhile.

Digital transformation promises to bring a new era in industrial automation. In this era, machines will execute complex control functions with self-learning capabilities and minimal operator intervention. That will allow process manufacturers to reduce accidents and production downtime resulting from human error and achieve optimal plant operation.

Find more articles and resources like this one at https://www.yokogawa.com/us/library/

ABOUT THE AUTHORS

Kevin Finnan is a digital transformation and industry marketing consultant at Yokogawa Corporation of America. He was previously an independent consultant, vice president of marketing for CSE-Semaphore, and director of marketing at Bristol Babcock. Finnan has more than 30 years of experience in a variety of vertical markets and has launched more than 40 automation and measurement technology products.

Wataru Nakagawa is a system product content marketing manager for Yokogawa Electric Corp. He was system marketing for integrated control and safety systems for more than 10 years and is now responsible for integrated control and safety systems (ICSS) digital contents. Nakagawa graduated from Waseda University with a master's degree in engineering.
No more kicking the can.

Here's the cybersecurity guide you've been looking for.

Get the groov EPIC Cybersecurity Technical Guide to learn more about:

• Creating secure zones and conduits between IT and OT networks (ISA/IEC 62443)
• Protecting legacy automation with device-level firewalls
• Restricting and centralizing user access
• Securing remote access with embedded VPN
• Encrypting communications with SSL/TLS certificates, HTTPS, and MQTT

Download your copy at: op22.co/cybersecurity
Case Study:
RDI Controls Executes Control System Retrofit

Pennsylvania-based engineering services company RDI Controls designed distributed control systems to retrofit three turbine peaking plants with Opto 22’s groov EPIC and SNAP PAC controllers.

In regional power generation systems, combustion turbines have become a mainstay recently. They work by compressing and accelerating air to high speeds, then injecting fuel to create a mix that burns at thousands of degrees. The combustion reaction drives the vanes of the turbine, which in turn, drive an electric generator.

These powerful, complex machines are used in combined cycle configurations for baseload generation, whereby the waste heat output from the turbine drives other power-generating systems. They are also used in simple cycle arrangements for so-called peaking plants, which handle mid- to high-demand power fluctuations.

By Josh Eastburn, Opto 22
Pennsylvania-based engineering services company RDI Controls provides fully engineered retrofit packages for industrial and aeroderivative turbine control systems, including demolition, installation, control valve and field device integration, water injection, nitrous oxide (NOx) emission mitigation, generator protection, and auxiliary/balance of plant (BOP) controls.

One of RDI’s customers invited the firm to bid on a project to retrofit three turbine peaking plants, each equipped with Westinghouse W301 and GE Frame 5LA combustion turbines in a simple cycle configuration with each operating in the 20 to 30 MW range. The previous iteration of the control system was designed with a pair of Allen-Bradley ControlLogix PLCs for each of the six turbines, but due to repeated control and maintenance issues, the customer needed a better-engineered solution that was easier to troubleshoot and more reliable.

**Project objectives**

- Peaking plants trade off efficiency for responsiveness, generating significant waste heat and losing work to turbine operation rather than power generation. To minimize these losses and reduce stress on the system, it was critical for RDI to keep the turbines running within tight tolerances during startup and operation.

- High-speed, rotating machinery requires a great deal of safety consideration as well. RDI’s solution must include fail-safes to handle situations such as load rejections, which occur when there is a sudden decrease in demand and can cause a turbine to accelerate beyond capacity and break apart.

- Although each turbine would have its own control system, every plant housed a pair of turbines, which used common subsystems that would need to be integrated into the primary controls. These included ammonia control systems and electric starter motor controls.

- For speed, cost, and error-reduction, RDI aimed to leave as much of the existing field wiring in place as possible.
Solution

To satisfy these objectives, RDI designed a distributed control system (DCS) at each site using a combination of Opto 22’s groov EPIC and SNAP PAC controllers (Figure 1). Lou Bertha, principal engineer at RDI Controls, said it was this same kind of experience that first led him to try Opto 22.

“At the time, Allen-Bradley was the biggest contender in industrial turbine control, but it was expensive and kludgey. From a flexibility standpoint, for my money, Opto 22 gave me more bang for my buck. I was able to do just about anything you could do with A-B at a fraction of the cost.”

More than 20 years later, RDI Controls has carried out over 160 retrofit and design projects on a variety of turbines from brands like GE, Westinghouse, Pratt-Whitney, and Rolls Royce using control systems from Allen-Bradley, ABB/Bailey, and Westinghouse/Emerson (Figure 2). But Opto 22 continues to be Lou’s supplier of choice, and his ability to deliver affordable, high-performing systems continues to win him business.
In recent years, Opto 22 has expanded its range of edge-oriented control options, which embed high-level automation functions like data transformation and distribution, database transactions, and manufacturing execution systems (MES) at the controller level. This change helps to simplify control systems and bridge (operational technology (OT) and information technology (IT) networks. To support this level of integration, edge controllers also provide more processing power, storage, and connectivity than traditional PLCs or PACs.

Using Opto 22’s groov EPIC edge programmable industrial controller, as well as older SNAP PAC controllers, RDI easily outbid the competition. It designed a distributed system that incorporated high-speed PID control, secondary control and networking, and embedded third-party communication.

At the peaking plants, the controllers integrate all functions of the W301, F5LA, and shared subsystems (Figure 3). Subsystems are integrated using native peer-to-peer communication and through

Figure 3: Site overview screen showing Westinghouse W301 and GE Frame 5LA status.
embedded OPC UA communication. Additionally, each site reports to an external historian through a secure PAC gateway and integrates with a Citect SCADA HMI network, which RDI also designed.

**Distributed control architecture.** One EPIC provides primary governor control for each turbine, managing fuel mix, combustion, and shaft speed, with one PAC providing backup control and overspeed protection. An additional EPIC handles sequencer control, including the startup of auxiliary systems, process monitoring and coordination, and alarming, with a second PAC integrating high-density thermocouple sensing for temperature limiting and ramping. Finally, RDI uses the dual Ethernet interfaces on each controller to set up redundant network connections (Figure 4).

![Figure 4: An illustration of RDI's site-level control network incorporating primary, secondary, and subsystem control.](image-url)
This distributed control architecture provides RDI with inherent fail-safes. Since all four controllers are peers on the network, not remote input/output (I/O), each has the ability to interlock the system in the event of a partial loss of control or network connectivity.

“Network redundancy is critical,” said Lou Bertha. “We can’t let the system fail for the sake of a bad switch. But in the event of network issues, each controller has the ability to trip the system as needed while maintaining its own control functionality, for example, lube oil operation, fan control, monitoring, etc.

“I can say that [full controller redundancy] doesn’t matter since the control is at the I/O level. If we are isolated from the network, we can continue running, and if we lose the I/O, redundancy won’t matter anyway.”

As with remote I/O, distributing control and I/O across multiple controllers also allowed RDI to reduce costs and minimize rewiring. High-density and specialty I/O was placed on lower-cost PACs and then located close to the equipment, rather than requiring long runs back to the primary controllers.

In Lou’s assessment, “The existing hardware was susceptible to damage if moved and the drawings were out of date, so we avoided rewiring altogether by dropping controllers into existing panels” instead of building new panels or attempting to marshal field wiring to a smaller number of controllers.

Fortunately, with the EPICs as primary controllers, performance is not an issue. Powered by quad-core ARM processors, Lou said “the horsepower is amazing.” Proportional-integral-derivative (PID) control functionality is used for speed, load, startup, and temperature control with the speed control loop executing at 50 ms or less. With that speed, RDI was easily able to maintain the turbine/generator speed at 3,600 RPM to within ± 1 RPM.

**Subsystem integration.** To interface with the shared subsystems at each of the three power generation sites, RDI leveraged a mix of hardware and software communication options included in Opto 22’s
EPIC and PAC controllers. With these embedded tools, there’s no need for RDI to maintain a separate communication server. The EPIC sequence controllers independently coordinate data passing between the starting resistor controller (SRC), ammonia system, the other turbine controllers, and remote I/O for both native and non-native communication.

For example, the SRC, a kind of electric starting motor, is controlled by an Allen-Bradley PLC, which adjusts the output of the SRC in response to the turbine speed. It needs to get that information from the Opto 22 network, and normally would require an external protocol gateway or OPC server to make that happen. Instead, RDI uses Inductive Automation’s Ignition Edge communication platform, which is built into groov EPIC.

Ignition includes its own OPC UA server and a suite of native protocol drivers for common industrial devices, creating a bridge between the EPICs and the PLC. It consumes A-B tags and exposes them as OPC UA tags, which can be linked directly to the control engine and other applications running on the EPIC.

Figure 5: RDI integrated Allen-Bradley PLCs into its groov EPIC control strategy using Ignition Edge.
Compared to passing data via an HMI/PC interface, this approach provides a fully independent link between the systems to ensure it maintains operation in the event of an HMI/PC failure. Lou Bertha said, “If you haven’t used this on a project, it’s fantastic. I could shut down the HMI and it will keep running. If I were using the HMI to pass tags around, as is common, I would have been in trouble.”

RDI uses the native OptoMMP protocol to communicate with the other subsystems. Turbine flow rate and temperature are passed to the ammonia system, which RDI had previously retrofitted using Opto 22 SNAP PACs to control the amount that is injected into turbine exhaust gas. Another PAC interfaces with Modbus serial devices to communicate voltage and protective relay statuses. And a pair of PACs create a non-routable interface for the external OSI PI historian. One PAC is linked to the control network, gathers data, and passes it to another PAC on the historian’s network. The dual independent Ethernet ports on each PAC allow RDI to segment the networks so that data can only flow out, not in.

Results

“We definitely had a competitive advantage price-wise,” said Lou Bertha. “We redid everything, including demo and install, and still came in 30 to 40% cheaper than competing bids.” With Opto 22, RDI won the peaking plant contract and then completed the project in only two weeks.

Besides lower material costs, Lou attributes his advantage with Opto 22 to three factors:

- Control at the I/O level: Opto 22 automation systems leverage intelligent I/O networks to distribute functions that, in a traditional
Case Study

remote I/O system, would typically be handled by a central controller. This architecture ensures that systems can continue to run even with partial impairment.

▶ Flexibility: groov EPIC and SNAP PAC are designed with embedded hardware and software tools—multiple networking options, communication servers, data processing functions—that provide engineers with many options for designing and scaling systems.

▶ Openness: Opto 22 products are built on open standards and technologies, making it easy to integrate with 3rd-party devices and external systems.

By leveraging these capabilities, RDI was able to meet the project’s objectives for performance and reliability. With no external dependencies or expensive server licensing, the system was also straightforward to design and simple to maintain.

"With Opto 22," Lou said, "we can do more and my customers are happy. It’s easy. It’s clean. The system just runs. If people don’t have to think about it, they are happy."

For more information on RDI Controls, you can find them at rdicontrols.com.

ABOUT THE AUTHOR

Josh Eastburn is director of technical marketing at Opto 22. After 12 years as an automation engineer working in the semiconductor, petrochemical, food and beverage, and life sciences industries, Eastburn now works with the engineers at Opto 22 to understand the needs of tomorrow’s customers. He is a contributing writer at blog.opto22.com.
IS YOUR CONTROL SYSTEM 5 YEARS OLD?

No matter its age, your control system could be taking on excess risk and running inefficiently.

**Typical Control System**

<table>
<thead>
<tr>
<th>Age</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 years</td>
<td>Modify and Update</td>
</tr>
<tr>
<td>8 years</td>
<td>Patch and Re-Optimize</td>
</tr>
<tr>
<td>10 years</td>
<td>Perform Upgrade or Migration</td>
</tr>
<tr>
<td>15 years</td>
<td>High Risk, Execute Migration</td>
</tr>
</tbody>
</table>

Talk to a **MAVERICK** expert about optimizing your control system performance.

MAVERICK TECHNOLOGIES
A Rockwell Automation Company
mavtechglobal.com info@mavtechglobal.com 888.917.9109
For a process facility to operate effectively, efficiently, and safely depends on two factors: People and automation seamlessly working together. Many companies find ways to train and develop their people. On the other hand, automation systems are often considered relatively static. They function acceptably, so little attention is paid to them. Entropy takes its toll, and the process operates with a tolerable level of deterioration—maybe a few instruments don’t work properly, maybe the operators can’t see a reading or two in the control room, but production goes on with just enough maintenance to avoid catastrophic failure... at least for now.

Automation and safety systems protect us from serious incidents. Here’s how to prevent these potential catastrophes before they occur by applying proper safety procedures and standards.
In these situations, a simultaneous deterioration of the automation and safety systems can take place, along with an erosion of personnel skills. It’s subtle, but it can occur over time as a few instruments drift out of spec and key personnel retire, find better jobs, or get let go—resulting in a little less knowledge and experience on every shift. Considering these issues, how can we mitigate risk and ensure our process control system is operating effectively?

**The first safety layer**

The basic process control system (BPCS) is the first line of defense for safety. It should keep the process on an even keel to prevent upsets and react appropriately to abnormal situations. But if the BPCS isn’t as good as it should be due to a lack of attention and maintenance, and if resource tribal knowledge and skills are lacking, the safety instrumented system (SIS) takes on greater importance (Figure 1).

When the BPCS begins to weaken, incidents escalate more frequently, and the SIS is much more likely to see action. If the SIS is robust, it should protect the facility and its people, but routine reliance on this last line of defense is never a sound strategy.

These situations make it especially critical to keep the BPCS and the SIS functioning as intended. In many respects, this attention can compensate for inexperienced operators as they come up to speed on the facility and its processes. When the BPCS is sound and well maintained, the operators and safety systems will be called on less frequently as the process becomes more stable. And effective human-machine interfaces (HMIs) will make an operator’s job much easier.

Ultimately, to ensure effective process control, we need to ask, “Is the facility safe enough?” which prompts more specific questions:

- Have we identified enough of the ways hazards could develop with our process?
- Have we drawn the line between tolerable and intolerable risks?
- Is the facility safely controlled by the BPCS and operations?
Does the BPCS keep the facility safe and stable when running in automatic?

Are the safety instrumented functions (SIFs), as designed, able to protect from the intolerable hazards when used in combination with the other layers of protection?

Are there standards relevant to our industry and processes that can help inform our decisions and guide our SIS design (see Sidebar 1: “Understanding Safety Standards”)?

Do all the elements of the facility’s automation, safety systems and people work together to ensure safe operation?

The basic process control system (BPCS) is the first line of defense for safety. It should keep the process on an even keel to prevent upsets and react appropriately to abnormal situations.

Many people tend to compartmentalize process facilities as they think about the different elements. The SIS is especially isolated in this regard, often viewed as totally independent both conceptually and mechanically. The reality is usually more complex (see Sidebar 2: “Independent and Separate”). While the ability of an SIF to do its job independently must be preserved, the safety hardware is probably more integrated with the BPCS than most people realize and the pressures to integrate the BPCS and SIS continue to increase.

As mentioned earlier, for a facility to run well, the people and the automation systems must work together seamlessly. The process should behave predictably in a steady state with the operators having a clear situational awareness of what’s happening within the facility and its processes. Think for a moment of what is required for reactor operation (Figure 2):

- The mechanisms controlling feedstock flow into a reactor must be well controlled and stable to keep feed proportions and residence time correct for full and efficient reaction.
Temperature control must be stable.

The reactor must have sufficient capacity to meet process requirements, with some margin for safety.

Burners and heaters need to start and stop reliably.

Valves, manual and automatic, need to move positively and shut off completely when necessary.

The list could go on. For all these basic functions to operate as designed when required makes the difference between an efficient and productive operation and a potential accident site.

An effective BPCS is the most important element for safety. A facility or unit unable to maintain steady-state control automatically during normal operation is an accident waiting to happen. Upsets can be triggered by an unexpected change in feedstock or some other equipment malfunction, but an effective BPCS should be able to automatically compensate for many of these abnormal situations. The intervention of an operator may be necessary but knowing when this should happen and the correct steps to take should be clear. Operators should not be left staring at the screens asking, “What just happened?” and “What should I do?”

When a production unit must depend on its SIS to handle routine upsets and frequently occurring abnormal situations, it’s time to examine the BPCS. This will likely be obvious to everyone involved as frequent SIS trips will cause havoc due to corresponding production interruptions.
Because the BPCS is the first line of defense in a properly designed and maintained facility, most SIFs are specifically designed to be low demand, with frequent use to be avoided. In the process industries, low demand is defined as no more than once per year. There is a significant difference between calling on an SIF once a year as it was designed to handle versus every day.

Even if the BPCS is working as designed, there are still times when the safety systems will be called upon, and their proper operation is critical in these circumstances.

**A comprehensive, coordinated approach**

Looking at a facility or production unit with the purpose of improving the SIS must take all the operational elements into consideration. Once the process, feedstocks, reactions, and other steps are understood, it’s time to work on the daily operation in greater depth.

1. **How well is the process running now, and what has been happening over the last year?**
   - Number of times it started up and shut down intentionally
     - Is operation continuous for long periods or subject to regular stops?
   - Number of times it shut down unintentionally
     - What happened to cause it to stop due to an upset, equipment malfunction, or SIS trip?
   - Maintenance history
     - Is all the instrumentation working and in calibration?
     - Are routine repairs handled quickly, or do they end up deferred for cost reasons?
     - Is diagnostic information used to guide maintenance planning?
SIS trip history

- How often did a SIF activate to shut down some or all the unit?

**Independent and separate**

The underlying concept of an individual SIF and the larger SIS calls for layers of protection able to function independently—a given SIF must be able to do its job without dependence on any other system such as the BPCS. The layers in a layers of protection analysis (LOPA) assume the BPCS is one layer, the SIS is another layer if the BPCS fails, and the dike holding the spill is another layer standing by if both the BPCS and the SIS fail. This maintains independence, but the result can be a collection of small, uncoordinated operations scattered throughout the process.

Some companies try to make each SIF totally self-contained and disconnected from any other system. This “air gap” is intended as a means of protection and necessary to ensure independence. The same concept is often applied as a strategy for cybersecurity protection. If a system can’t be reached, it can’t be hacked.

This practice becomes problematic for two reasons. First, air-gapped systems are not usually as isolated as their proponents believe. If there is no other means of protection, the system may be far more vulnerable than realized. Second, it loses the practical benefits of integration. An air-gapped system has no means to connect to larger networks, including historians, remote support, and for management visibility. Useful things are lost to provide protection, which is ineffective and thus a poor practice.

Some SIFs should be coordinated with the BPCS. The SIF needs to do its primary function independently, but operations may benefit if the action can have a response that mitigates the production disruption.

When they dig into the situation, many people are surprised at the extent of SIS integration with the BPCS when they look closely and realize how far it’s gone in their facility. They often convince themselves that their systems are fully separated when the reality is much different. Others embrace the advantages of integration and push it as far as possible without totally giving up required safety system independence. Each company needs to determine where it wants to be on the spectrum, and this question should be part of any major system analysis project.
2. How effective is the BPCS?

- Ability to run in automatic
  - Does the BPCS operate effectively by itself, or do significant parts of the facility run in manual?

- Instrumentation
  - Are there enough transmitters?
  - Are they measuring the right variables in the right places?
  - Are they sized and ranged appropriately for the specific application?

- Startups and shutdowns
  - Are these procedures automated or handled manually?

- Alarm management
  - Are operators flooded with alarms, more than they can respond to?
  - Are there “stale” alarms?
  - Are some regarded as nuisances and disabled or ignored?

How well do the operators understand and do their jobs?

- Situational awareness
  - Do the operators have a good idea of what’s happening, or is the process a black box in some instances?
  - Can they respond to abnormal situations?

- Life in the control room
  - Do the operators see what they need to see on the HMIs?
  - Are the graphics well laid out to deliver critical information?
  - Do they keep to a few familiar screens when problems occur,
or do they have to jump between rarely used views to see what they need?

Once these basic operational questions are answered, it’s time to start digging into the SIS itself and its history:

▶ How old is the HAZOP analysis on which the SIS was built?
▶ Is the facility still configured as it was then, or has it been updated? Have the HAZOP analysis and SIS been updated to stay current? Is there a good sense of how management of change is supposed to work?
▶ Was the SIS built in accordance with any specific safety standards?
▶ Have the experiences of the facility over the years reflected the expectations of the original HAZOP, or have different kinds of incidents happened that were not anticipated?
▶ Do the individual SIFs get tested as frequently as they should?

These are not trivial questions with simple answers. Launching an analysis of a working facility or unit is a major undertaking. Some companies try to limit this analysis to the safety system alone, working with specialists to delve into layers of protection analysis (LOPA) and HAZOP analysis, and how the individual SIFs work together. This is fine as far as it goes, but the SIS does not exist in isolation. A more thorough evaluation looks at the larger automation picture, and how people work within the context of its operation.

**Cyber threats emphasize** the need for the BPCS and SIS to work together in a coordinated effort to protect the facility. On the positive side, there is updated information in the IEC standards to help you protect these critical systems.
One thing missing from the list is cybersecurity. While related to the issues discussed so far, it needs to be examined on its own. Suffice it to say, the BPCS can come under attack either directly from the outside or via the corporate networks. If control is disrupted, the facility may have to depend on the SIS to protect it. At the same time, as SIS functions are also now being integrated, they can also be attacked. If anything, cyber threats emphasize the need for the BPCS and SIS to work together in a coordinated effort to protect the facility. On the positive side, there is updated information in the IEC standards to help you protect these critical systems.

**Dig into historic roots**

To perform an effective safety audit and analysis, look at the operational history for at least a year, and dig into the causes that could have created incidents, not just ones that did. This is similar to near miss reporting for personal safety. The incident occurred when a worker slipped on a spill and broke his arm, but the blame rests with the 10 people who stepped over the spill and didn’t report it.

An obvious area of concentration is examining all the circumstances surrounding unscheduled shutdowns. But the digging must go deeper to look at what could have caused incidents or prompted near misses. Safety incidents are disruptive to production and therefore expensive, but they also tell a lot about a facility’s condition, its automation systems, and people.

How often does the SIS trip and cause a shutdown? Each of those incidents should be examined in detail to identify the cause. If it’s related to poorly configured process equipment, a quirk of the automation system, or an improper procedure or work instruction, it needs to be fixed.

**Understanding a complex picture**

The safe and effective operation of facilities and processes has many facets. No single element can ensure success, but it only takes one to
cause failure. Facilities should be evaluating their operations constantly looking for ways to improve production or solve problems (Figure 3).

To start, companies often look first at the SIS and realize they need help from a third-party expert—someone who can bring a fresh set of eyes to the situation. Often, different individuals bring new insights and a broad experience base to bear on potential problems. Getting third-party expert help for SIS analysis and improvements is important since it requires specialized knowledge. However, given the linkage between the SIS and BPCS, studying either in isolation is short-sighted. Both systems should be examined together, even if they are not fully interconnected.

An experienced consultant can bring deep domain experience on all fronts, tying together all the factors involved in your operation. By combining and applying process knowledge, automation depth, and SIS expertise, facility operation can be improved and incidents avoided. But it’s not just about the mechanics, it’s also about people.

Safety doesn’t happen by chance. All the elements must work together to make it happen correctly. Just remember, with intentionality from management, the right help from external experts, and automation and people working together seamlessly, you can mitigate safety risks and ensure an effective process control system.
Understanding Safety Standards

Standards relevant to process plants

When discussing safety systems, the topic of standards will invariably come up in the conversation. Some people resist the idea, considering standards to be in the same realm as regulations designed to make life more difficult. With the one exception explained below, this is usually the wrong way to look at things because standards are written by users to make implementations easier and more consistent. One of their primary intents is to help users sort through situations and solve problems without having to re-learn costly lessons.

As you begin your own discussions, here are several standards you should follow:

**IEC 61508:** This is the broadest over-arching standard related to industrial safety in a wide variety of forms. It discusses both discrete and process manufacturing, so it covers a lot of ground. For process manufacturers, it defines devices used in SIFs, so it provides the qualifications to determine if, for example, a given pressure instrument is suitable in a safety application.

**IEC and ISA 61511:** This standard is very important for process industries and covers the most critical elements of SISs for process manufacturing facilities. It provides the most comprehensive picture of what an SIS needs to look like and how it should work. For example, when working through your LOPA, an SIF must prevent an incident (e.g., safety shutoff) and not mitigate the effects of an incident (e.g., re-suppression system). This standard is undergoing changes, so it is important to work from the most recent revision. Many of the changes relate to definitions of specific terms, but some take a deeper dive into some personnel issues related to the individuals involved in designing, building, and evaluating safety systems. The standard stresses the importance of having a variety of people involved in the process to ensure the same set of eyes is not evaluating every element.

**IEC 62443 and ISA-99:** These cybersecurity standards are for industrial control systems. A lot of recent work has gone into the technical reports that define cybersecurity lifecycle and safety zones.

**API:** There are many standards under the American Petroleum Institute umbrella, and they frequently serve as commentary on how to implement some of the specifics of IEC 61511 within the oil and gas industries—particularly for offshore installations, pipelines, and product storage. For companies not working with bulk volumes of flammable products, these standards are effectively irrelevant.

**OSHA Process Safety Management Standard, 29 CFR 1910.119:** Here’s the exception: This is a government regulation and carries the force of law. It defines what safety systems are supposed to do, so there are many “Thou shalt...” kinds of statements. However, it does not discuss how to implement the rules. Those decisions are left to the other standards and the company’s judgment.

Obviously, these comments are intended simply as pointers toward areas where you should be doing much deeper research. For any safety system design, consideration must be given to the appropriate standards, so any outside consultants working with you need to bring a high degree of familiarity to the discussion.
ABOUT THE AUTHOR

Scott Hayes (scott.hayes@mavtechglobal.com) is DCSNext® Portfolio Manager at MAVERICK Technologies. He has more than 20 years of experience in process control. He is a licensed control system engineer and a TÜV certified function safety engineer.
The CX7000 Embedded PC delivers the efficiency and performance of TwinCAT 3 software in an ultra-compact controller format. This further enhances the scalability of PC-based control technology from Beckhoff ranging from DIN rail mounted mini-PLCs to many-core Industrial PCs. Equipped with a 480 MHz processor and 12 configurable multi-functional I/Os, the CX7000 offers an attractive price-performance ratio and exceptional flexibility. The CX7000 supports simple system expansions using the Beckhoff I/O terminal system.

- ARM Cortex™-M7 processor (32-bit, 480 MHz)
- Compact dimensions: just 49 x 100 x 72 mm
- Multi-functional I/Os allow variable use:
  - 8 digital inputs, 24 V DC, type 3
  - 4 digital outputs, 24 V DC, 0.5 A, 1-wire technology
  - fast counter input
  - encoder input
  - 2 analog 0…10 V inputs
  - 2 PWM outputs

Support the most versatile applications:
- safety technology
- compatible with EJ system
- motion control
- explosion protection
- EtherCAT
Advancing Automation Requires an Evolution in Data Management

Breaking down data silos for integrated, contextualized data improves flexibility and speed to market without impacting production

The last five years have seen a massive shift in the way industry designs and secures automation systems, with much more emphasis on the value of data. And with each passing year, more new software and technology continues to shift how we generate, store, and access critical plant information. This evolution in data management starts where input/output (I/O) enters the system, enabling new control and analytics, and resonates all the way up the automation stack, touching every level of the enterprise.

Industry needs data at all levels of the enterprise to stay competitive with increased speed to market and the ability to rapidly

By Juan Carlos Bravo, Sergio Diaz, and Neil Wang, Emerson
shift production to meet new customer needs. But just having data isn’t enough. If data is trapped in silos or hard to interpret and analyze, personnel across the enterprise will struggle to implement the process, software, and hardware changes necessary to stay flexible enough to compete in the global marketplace.

The technology shifts poised to shape process control over the next five years are focused on this challenge—designed to harness the latent power of the control system to end data silos and leverage data-in-context, unlocking nimbler, more efficient, and more profitable operations.

**Advanced Physical Layer (APL),** a new, Ethernet-based physical layer, enables plants to dramatically increase the data connectivity and capacity of the control system.

**Expediate information from field devices**

Traditionally, the capacity of communications from field devices into the I/O subsystem was limited by the electrical properties of necessary interfaces. As a result, many existing automation systems contain myriad I/O types with a large variety of I/O signals, from traditional I/O to communication protocols such as HART, Modbus, Profibus, etc., each using different physical media and wiring strategies. This variety complicates design and installation. Over time, communication protocols have evolved to fully digital, Ethernet-based protocols with mostly similar names: HART-IP, Modbus-TCP, and PROFINET. However, use of Ethernet devices has been limited by wire length, additional power wiring, and non-hazardous area installation.

Today, Advanced Physical Layer (APL), a new, Ethernet-based physical layer, enables plants to dramatically increase the data connectivity and capacity of the control system. Ethernet-APL provides a physical media enabling digital protocol devices to communicate across long distances via a pair of wires that also provide power. Multiple digital protocols can coexist on the same network.
Since many Ethernet-based protocols are extensions of previously used protocols, there is no need for end users to re-train their personnel. For example, HART-IP is the enhanced version of the long-used HART over 4-20mA—now fully digitized and secure. All the tools for device configuration, calibration, and troubleshooting can transition from the non-Ethernet protocol to the Ethernet-base type. The user experience for Ethernet devices will be quite similar to fieldbus-type devices, just much faster—no more waiting for the device configuration display to populate with information.

**APL is on the horizon**

As with any new technology, it will take some time before APL is widely available in all device types. Complex and/or critical devices such as Coriolis meters or digital valve controllers will be the first to realize the benefits of APL, followed by simpler instrumentation such as pressure or temperature transmitters. Time will tell if any existing discrete devices will transition to become “smart” Ethernet-APL devices.

As APL gains popularity, end users will have to seek out solutions that do not require two dissimilar I/O subsystems: one supporting traditional signals and another completely separate APL subsystem. Otherwise, APL adoption will suffer similar deterrents as when the fieldbus solutions were introduced. Emerging solutions that enable users to easily swap out a legacy device for an APL device will be ideal (Figure 1).

![Figure 1: Smart Junction Box supporting both Ethernet-APL and traditional field devices.](image-url)
**APL is more secure**

The industry is moving to more open architectures. The NAMUR Open Architecture (NOA) intends to make information available for different use cases including process control, monitoring, and optimization. Smart field devices will need to transmit data to multiple places—not only to the control system or the asset management system. Ethernet-APL may allow for control and monitoring solutions to share the same infrastructure without forcing all the signals through the control system first.

Ethernet-based protocols will facilitate the routing of information to all the required end points. However, with the increased exposure of field devices, security will be even more critical. Ethernet-APL will enable more secure communications as it can leverage secured protocols such as the updated version of HART-IP, which includes all the elements required to secure communications among field instrumentation, the control system, and the asset management solutions.

Ethernet-APL will transform the industry by delivering faster, more secure, and easier integration of data from field instrumentation to support the deployment of open architectures. The success of Ethernet-APL will depend on the availability of simple and secure APL solutions based on proven system architectures facilitating the integration of both legacy and new technologies with minimum re-learning and the ability to deliver timely information to all the levels of the enterprise.

**Near plug-and-play automation**

The emerging data evolution extends to how plants connect and integrate subsystems into their automation. This broader integration of subsystems has been costly and difficult to plan because of the time, effort, and expense of establishing and maintaining those links. In addition, rapid market shifts in many industries today drive a need for more flexibility in the manufacturing process. One of the key methods of meeting this challenge is introducing new modular
process technology into automation, enabling plants to quickly shift manufacturing to meet global demand.

Module Type Package (MTP) unlocks the ability to bring a broader set of those subsystems more easily into plant automation.

Module Type Package (MTP) unlocks the ability to bring a broader set of those subsystems more easily into plant automation, providing end users a path to much greater flexibility. MTP—introduced by the User Association of Automation Technology in Process Industries (NAMUR)—will help industry integrate distributed control systems (DCS) and programmable logic controller (PLC) systems more easily by reducing the time and cost to integrate distributed process and reliability assets and equipment. Easier integration will increase speed to market and help industry meet customers’ individualized needs.

Much of the potential cost and delay in capital projects or in adding new equipment to existing processes comes from the effort spent on integration. MTP automates much of this integration by providing a framework for standardized equipment data models and description language to streamline interoperability.

One of the best ways to stay ahead of market shifts is to build modular production systems. However, unlocking flexibility typically means purchasing many different types of equipment and making them work together—often with complex custom interfaces. MTP compliance ensures new products will work with existing MTP-compliant products already in place. As the standard progresses, plants will more easily integrate equipment via standardized, pre-tested and pre-qualified interfaces.

The most comprehensive MTP solutions incorporate the control system as part of the process orchestration layer to operate and
supervise process equipment assemblies such as PLCs and machinery health and prediction devices (Figure 2). Moreover, asset monitoring technologies can also be designed with pre-configured MTP objects specialized for asset reliability data to enable seamless integration with a plant’s control system. In MTP-supporting asset monitor applications, users create measurement points and can then export an MTP-ready file to import objects directly into control and safety systems without additional configuration.

All these technologies are helping industry more quickly and easily move a wider spectrum of data into the control system. As a result, the control system becomes a critical repository for data, adding increasing value through the context provided by control and analytics. New opportunities for process optimization, improved product yields, and abnormal situation prevention through early fault detection, are possible.

Operator effectiveness is enhanced with embedded analytics and decision-making tools using this data, predicting—and potentially responding to—the impact of process changes.

Figure 2: Holistic MTP solutions provide the DCS in the process orchestration layer to operate and supervise process equipment assemblies such as PLCs and machinery health prediction devices. Courtesy: Emerson
The operator’s role becomes more supervisory, acting as process managers intervening in the process only if prompted or at the most critical points. Moreover, these elevated operators make better decisions.

**Access the goldmine of data**

If newly contextualized data is locked in the control layer, it is not very effective for the overall improvement of the business. A critical element of data evolution, then, is extracting contextualized data out into the enterprise. Edge solutions get the right data to the right place.

---

**Control system** edge solutions are designed to work with the control system by taking advantage of this existing hierarchies.

Control system edge solutions can store and contextualize data. New and existing plants put an immense amount of resources into defining the control system hierarchy—such as areas, units, and control modules—so that this configuration accurately reflects the real layout of a plant. This hierarchy information provides the contextualized data structure to enable advanced data analytics. Control system edge solutions are designed to work with the control system by taking advantage of existing hierarchies.

Data is available in the same hierarchy that operators are used to seeing in the control system, with any changes made to the control system automatically reflected in the edge. On the data service side, control system edge solutions leverage cloud and IoT technologies, such as MQTT, REST API, or OPC UA, for secure and efficient data transfer.

Not all the information from field devices is needed by process operators; some information is only relevant to analysts or maintenance personnel, while other information might be needed for more than one use case. For example, certain data used for process control might also be needed for optimization.
The automation system should effectively route the right plant data to all data users. Information should not necessarily pass through the process control system to avoid ineffective data flow. Instead, the system architecture should facilitate secure communication beyond the control system. Because of the critical assets control systems touch, much of the data needed passes through the control system, thus creating a step change in the amount of information required from control systems.

However, to maintain the highest levels of safety and security for processes, operators, and the organization, control system exposure to external systems and applications—particularly those exposed to the internet—is tightly controlled. Edge technologies can help provide data access without relinquishing this control.

**Edge solutions plus OPC UA equals secure access**

Edge gateway technologies provide isolation of the control system while still delivering data out to the edge (Figure 3). These gateways are not only easier to configure but are more secure, as entry into the control system is even more limited than with traditional solutions.

![Figure 3: Control System](image-url)

Edge solutions offer secure data transfer from the control system to on-prem and/or the cloud.

*Courtesy: Emerson*
Data generated and collected by a control system is needed by many plant- or enterprise-level applications, which may be deployed from in-plant networks to on-premise or public cloud. Users also require secure, easy access to control system data. Industrial edge technologies are developed to meet all these needs, and OPC UA is often selected for its ease of installation and enhanced security.

Different than the edge gateways for a single PLC or device, which normally handle data from an individual data source, edge solutions for control systems (or control system edge) must be capable of aggregating large amounts of data from all controllers and nodes in the system, and then transferring the data at sufficient throughput rate.

Secure control system edge solutions provide isolation of the control system while delivering data out to both on-premise and off-premise destinations. These edge solutions increase security because the applications connect to the edge server instead of the control system, minimizing the control system's external connections. The edge server connects to a control system through secure and protected protocols.

Further security can be achieved if one-way data transmission technology, such as a data diode, is used to connect an edge server to its control system. One-way data transmission disallows communications initiated from external applications to the control system. With all the control system information stored, the edge platform can be viewed as a data replica of its underlying control system. This design provides enhanced protection to the control system, while providing access to the full control system data.

Ultimately, control system edge solutions will provide all users—from the edge to the enterprise—the same experience. Whether it is access to active batch information, alarming, or even monitoring the process, users will access the same operator displays they are used to seeing on the control system. Thus, everyone in the organization will experience plant data in a format they are familiar with and already know how to navigate, whether they are in the plant, at home, or in a conference room at headquarters—all without impacting the control system at any stage of the process.
Evolving data across architectures

The data handling evolution is not just about finding ways to collect more data. Instead, it is a shift across the entire industrial infrastructure touching many points of the automation stack. Thinking about evolution holistically is the key—evaluating and implementing new technologies to break down silos and deliver data wherever it needs to be, while not separating it from the critical context built in by the control layer. Not every technology facilitating this evolution is readily available today, but the foundational technologies they build upon are already on the market, making them a critical element of any five or 10-year plan.

ABOUT THE AUTHORS

Juan Carlos Bravo is product manager for the DeltaV PK Controller and data integration for Emerson’s DeltaV DCS. He has 23 years of experience in the process control industry. He graduated as an electronic engineer from the ITESM-CEM (Instituto Tecnologico y de Estudios Superiores de Monterrey Campus Estado de Mexico) and earned an MBA from St. Edwards’s University in Austin, Texas.

Sergio Diaz is a DeltaV product manager at Emerson, responsible for influencing product strategy and supporting product development. At Emerson, Sergio has held different roles including field service engineer, test engineer, and upgrade team lead. Sergio holds both a BSc and a MSc in electrical engineering from the National Polytechnic Institute in Mexico.

Neil Wang is a DeltaV product manager at Emerson, influencing product strategies and supporting product development. He has held different roles, including project engineer, account manager, and strategic pricing manager. Neil holds a BSc and an MSc in electrical engineering from Hebei University of Technology in China, and an MBA from Emory University in Atlanta, GA.
Keep your process and plant safe with FS Functional Safety Series instrumentation from Moore Industries. You can be confident that they will help ensure the safety of your process and facility when you need it the most. Our Logic Solver, Signal Isolators and Transmitters are built to strict IEC 61508 standards, ensuring safe and reliable operation – particularly in environments where hazardous or emergency situations are likely to occur.

The rugged and reliable FS Safety Series Instruments from Moore Industries.

To learn more about our FS Functional Safety Series, Call (800) 999-2900 or go to: www.miinet.com/KeepItSafe
The search for reliable, practical information on building EtherNet/IP subnetworks on Ethernet for factory floor manufacturing systems is over.

By John S. Rinaldi, Real Time Automation

"I'll never allow Ethernet onto our factory floor." That was a common refrain for many factory managers in the earliest days of industrial Ethernet. Now it's such a universal technology that we expect wireless Ethernet service in the same fashion that we expect water, electricity, and a public toilet. Not only is Ethernet pervasive in our homes and street corners, but it's nearly universal in our factories with some believing that it should be the one and only factory floor communication media.

The most pervasive technology in North America for supporting factory floor manufacturing systems is EtherNet/IP. EtherNet/IP is an Ethernet application layer network technology promoted by ODVA (www.odva.org). It is the foundational architecture for manufacturers in industries as diverse as...
automotive, pharmaceuticals, and wastewater. In fact, it is hard to find an industry in North America that doesn’t rely on EtherNet/IP.

What’s been missing from the EtherNet/IP discussion is reliable and practical information on building EtherNet/IP subnetworks on Ethernet. This article attempts to fill that gap.

**Key principles**

There is a context and a set of key principles that provide the foundation for the recommendations that follow:

1. EtherNet/IP devices are certified by the [ODVA](https://www.odva.org) to conform to both the CIP and EtherNet/IP specifications.


3. Blended networks are strongly discouraged for machine control systems. Adding non-EtherNet/IP devices to an EtherNet/IP network to create a blended network eventually leads to process issues no matter how much bandwidth is available on the network.

4. Most of the traffic for devices in an EtherNet/IP control network must be EtherNet/IP control or traffic in support of the control traffic. Devices with no control traffic should not be connected to the control (EtherNet/IP) network.

5. A CIP device is not necessarily an EtherNet/IP device. CIP messages can be transferred over CAN, USB, RS-232 serial, Bluetooth, and other communication mechanisms. The recommendations that follow refer specifically to EtherNet/IP devices using CIP explicit and implicit messaging in an EtherNet/IP network as defined above.

6. To address security concerns, IP addresses for EtherNet/IP networks should be plant or company private.
Recommendation 1: Use fully switched, full-duplex Ethernet

Control system architects should ensure an EtherNet/IP network is a fully switched and full duplex network wherever and whenever possible.

Using a fully switched architecture and connecting EtherNet/IP-capable end devices to Ethernet switches, gives an end device exclusive access to the rest of the EtherNet/IP network. Because control system messages must be delivered as quickly as possible, the switches supporting the EtherNet/IP-capable end devices shouldn’t be contending with each other when forwarding those messages along the path to their destinations.

Using full-duplex communications mode for each point-to-point link within a switched EtherNet/IP network doubles the potential bandwidth of a cable and eliminates the possibility of collisions on that link (Figure 1).
Consistency in the configuration of the device duplex settings is important. The devices at both ends of a point-to-point Ethernet network link need to use the same duplex settings to have the link operate in a full-duplex manner. Monitoring the operational behavior of the network interfaces of the devices is the best way to ensure Ethernet communication on each link is optimal. Many managed switches offer features that can detect and alert on collisions and/or duplex mismatches.

The primary exception to using fully switched and full-duplex behavior in an EtherNet/IP network arises when sending EtherNet/IP traffic across a wireless Ethernet portion of an EtherNet/IP network. Wireless media is inherently a shared communication media. Wireless transmissions are always potentially subject to remote interference.

**Recommendation 2: Control system messages get priority, period**

An EtherNet/IP network is a control system network with an underlying Ethernet network. The most important traffic it conveys is control signal traffic. Control traffic should pre-empt any non-control traffic. Non-control traffic—even network management traffic—should defer to control system traffic on a control system network. In a temporary congestion situation, control traffic should unconditionally be preferentially handled over any other traffic on the network. The potential impact of even momentary traffic congestion on an EtherNet/IP network should be minimized. One way to do that is to prioritize the control signal traffic.

Most Ethernet managed switches have queues where messages are temporarily stored when an outgoing port is busy. There can be a number of these queues, some for high priority messages and other for lower priority messages. The priority queuing mechanisms they employ for each of the different queues are often configurable.

The priority of an Ethernet message is indicated by the value of the priority field in the Ethernet frame. There are eight possible priority values, with 0 indicating the lowest priority and 7 indicating the highest priority. These priorities are mapped to specific message queues. Multiple priorities are often mapped to the same queue.
Regardless of how many queues and queuing mechanisms are supported, every switch that supports prioritized transmission queues supports the ability to implement an exclusive priority mechanism. The traffic in the lowest priority transmission queue will only be sent if there is no traffic to send in any higher priority transmission queue for a port.

**Non-control traffic**—even network management traffic—should defer to control system traffic on a control system network.

Two priority queues are sufficient for EtherNet/IP networks: high and low priority. EtherNet/IP implicit message traffic should get assigned to the highest priority queue. All other traffic should be assigned to the low priority queue. No exceptions.

End devices that properly implement the EtherNet/IP specifications are able to explicitly tag traffic with a priority value. For end devices that don’t support that feature, there is sophisticated infrastructure equipment able to preferentially process EtherNet/IP implicit message traffic. These devices can be configured to assign implicit traffic (UDP protocol traffic using port address 2222) to the high priority outgoing message transmission queue.

**Recommendation 3: Use unicast communications**

Architect EtherNet/IP networks to use unicast communications wherever and whenever possible.

The EtherNet/IP specification allow for both unicast and multicast delivery of “real-time” data, but it was several years into its initial deployment before EtherNet/IP programmable controllers fully embraced and implemented unicast delivery of real-time control and safety traffic.

Since then, only a small minority of applications on EtherNet/IP networks are architected to use multicast communications. The advantage of multicast traffic is that it can be used to replicate traffic to tens, hundreds, or thousands of destinations. There are a minority
of EtherNet/IP networks where this is desirable. Overall, EtherNet/IP multicast Ethernet communications should be discouraged due to its many disadvantages including extra complexity, more complicated and expensive infrastructure equipment, and the inability to be routed.

Today, two EtherNet/IP capable devices can exchange unicast I/O messages across different subnets using a line speed Layer 3 switch. These EtherNet/IP capable devices can exchange unicast I/O messages clear across a factory by routing that traffic over the company network just as if they belonged to the same EtherNet/IP network and were physically located adjacent to each other.

Routing of unicast messages is underappreciated. In fact, too few control engineers take advantage of the ability to route unicast messages (Figure 2).

**Recommendation 4: Right-size your network**

It is important to architect an EtherNet/IP network for the optimal size of the control system it supports. The broadcast domain for that network must not cover the entirety of the Ethernet network, but only cover the EtherNet/IP network. To do that, right-size your EtherNet/IP network.

An EtherNet/IP network is an IP sub-network superimposed upon an Ethernet network. The definition of what constitutes an Ethernet
network has changed over time. The original Ethernet network transformed from a single cable network with a shared media access control mechanism to the advanced networks of today. Modern Ethernet network collision domains have shrunk to the size of a single cable connecting a device to a port on a switch. Full duplex operation on all the cables of a switched Ethernet network have eliminated the possibility of a collision on that Ethernet network.

It was the promise of a low-cost, high-speed and high-bandwidth, collision-free Ethernet network that led to the development of the EtherNet/IP specification. But beware, there is nothing in the EtherNet/IP specification that prevents you from using it on a shared media Ethernet network. There is nothing in the EtherNet/IP specification that prevents you from putting non-EtherNet/IP-capable devices on an EtherNet/IP network. It is your responsibility as an EtherNet/IP network designer to ensure the Ethernet network foundation for your EtherNet/IP-capable devices can support the control system applications you plan to run on them.

**The EtherNet/IP specification is a tool. It’s up to you to ensure that the tool is used properly and safely.**

In a programmable logic controller (PLC)-centric control system architecture, the best way right-size your EtherNet/IP network is to divide a potentially excessively large EtherNet/IP network into smaller networks at a point where the control signal interactions between networked devices only involve horizontal control signal communications (EtherNet/IP scanner/adapter communications) between peer-to-peer controllers.

To right size your network, adopt the rule that a 254-node EtherNet/IP device capable network will be the largest EtherNet/IP network you will deploy. If you have an EtherNet/IP network with more than 220 devices, separate that network into two EtherNet/IP networks of 200 end devices or less. The technique used to divide an excessively large EtherNet/IP network into two smaller networks is the same one recommended for separating a large switch network into multiple switches: Cluster the devices into groups that minimize the need to exchange control signal traffic between them.
Recommendation 5: Define a well-architected address space

The day may come when it is possible and advantageous to provide a globally uniquely address for every device on an EtherNet/IP network, but presently, there is little to no advantage to do so. In fact, it is much more advantageous to use a private, segmented addressing scheme that can be easily understood, implemented, and maintained by the team members of your controls department (Figure 3).

In fact, that is the definition of a well-architected address space. It is an address space easily understood and explainable to plant team members. It is an address space easily implemented without extraordinarily complicated router and switch configurations. And it is an address space easily maintained by your controls department.

Architecting an address space for an EtherNet/IP network is both an extremely important and complex endeavor. A well-architected address scheme should meet the following conditions:

1. It should take advantage of the company-wide private address space provided by IANA. Such an address space protects the EtherNet/IP network from unwanted messages from external networks and external networks from unwanted EtherNet/IP messages.
2. It should be consistent across the plant.
3. It should take advantage of switches supporting static routing.
4. It should be limited in scope. The number of devices in the network should be within the limits of what the least capable EtherNet/IP device can withstand in worst-case broadcast conditions.

5. It should be consistent with the requirements of your IT organization.

These conditions are not absolutes. Designers can have a well-architected EtherNet/IP address space that, for specific technology or organization reasons, violates one or more of these tenets of good addressing. But, in general, these tenets are the foundations for easily understood, easily implemented, and well-maintained EtherNet/IP networks.

Consider a few of these conditions in more detail.

**Use of private address space:** Designers should choose an EtherNet/IP address space that ensures a separation between the EtherNet/IP controls network and the corporate network and the Internet. This means taking advantage of the IANA non-routable, address ranges. Those ranges ensure your routers will not route any of these private addresses to a corporate network or the Internet and that no unwanted messages from the Internet will be routed to your control networks.

**Use of static routing:** Static routing and factory preconfigured I/O addresses (192.168.1.xxx) provide the designer with a host of advantages. This is especially true in situations where machines or machine sections are duplicated or PLC programs are often copied from one PLC to another. Operationally, it simplifies installation and maintenance for the trades people supporting the network as device replacement becomes a matter of setting three switches.

**Consistency across the plant:** It is advantageous to have specific address ranges for your switches, controllers, and I/O devices, and insist on consistency as new machines and devices are added to your plant floor. And it means all EtherNet/IP controllers use the same set of address ranges for device networks. Designers should duplicate EtherNet/IP I/O network addressing as much as possible across the plant. Addressing consistency of this type vastly improves understanding of the architecture by controls staff, enhances
troubleshooting, and makes copying/pasting of PLC programs from one machine to another much less cumbersome and complicated.

Final thoughts

Vendors of EtherNet/IP devices often advise users on building EtherNet/IP control systems. While they know nearly everything about the EtherNet/IP specification and much about how messages transfer between EtherNet/IP scanners and adapters, they know little about building practical, reliable EtherNet/IP networks in the field.

This article proposes a small set of philosophies that can serve as guideposts for control engineers tasked with architecting their next EtherNet/IP system.


ABOUT THE AUTHORS

John S. Rinaldi is chief strategist and director of WOW! for Real Time Automation (RTA) in Pewaukee, WI. John is not only a recognized expert in industrial networks and an automation strategist but a speaker, YouTube personality with over a million views, blogger, the author of more than 400 articles on industrial networking, and the author of six books.

John S. Rinaldi
Real Time Automation
http://www.rtautomation.com/contact-us/
https://www.linkedin.com/in/johnsrinaldi
YOUR ONE-STOP SHOP FOR
POSITION AND MOTION SENSORS

Industry-Leading Encoders, Inclinometers,
Linear Position Sensors: Built to Your Specs!

Pick the mechanical properties, communications interfaces and performance parameters
that are right for your project.

POSITAL's mass-customization manufacturing systems can build and deliver exactly
what you need.

Delivery within days, competitive prices.

Minimum order quantity - one!

POSITAL: The Versatility Champs

www.posital.com
How to Choose Between Standalone Encoders and Integrated Motor Feedback

By Christian Fell, POSITAL-FRABA Inc.

Designers of motion control systems for robots, manufacturing equipment and mobile machinery have options for providing digital feedback signals. Here is a look at the alternatives.

Rotary encoders: a key to motion control

Rotary encoders have been key components in motion and position control systems since the earliest days of digital controls, translating rotary motion into digital feedback signals for control systems.

Standalone encoders are self-contained devices with their own housings and shafts, bearings, and seals. They are available in a wide range of mechanical configurations and can be installed virtually anywhere in a machine where rotary motions need to be monitored.
An alternative approach is to use servomotors or feedback-controlled stepper motors that combine propulsion and position feedback into a single unit. In this case, integrated motor feedback is provided by a "kit" or modular encoder mounted inside or immediately adjacent to a motor’s housing, with rotary motions measured directly from the drive shaft. This can be an efficient solution for industrial motion control systems powered by electric motors, as it reduces the need for separate position transducers.

Let’s talk about the relative advantages of these two types of encoders.

**Standalone encoder versatility**

Standalone encoders are an excellent solution for machines that use non-electric prime movers like pneumatics or hydraulics. Because standalone devices can be installed close to the operational end of the machinery—not just on a motor—they can avoid loss of positional accuracy that might occur when a motor’s power is transmitted through long gear trains, belts, or other mechanisms. Standalone encoders can also be used with a draw-wire assembly or measurement wheel to provide linear motion measurements.

![Figure 1: Standalone encoder: self-contained unit built for versatility and durability.](image-url)
With many different mechanical configurations and communications interfaces available, designers are almost certain to be able to find devices that meet their requirements. For example, for harsh environments, standalone encoders are available with heavy-duty housings and seals that provide ingress protection ratings of up to IP69k. These units are protected against dust, water, and even the aggressive cleaning solutions and high-pressure jets used in pressure washing systems for food or pharmaceutical processing equipment.

**Integrated motor feedback encoder simplicity**

In contrast with standalone encoders, which are packaged as self-contained units, "kit" or modular encoders are designed to be built into—or attached to—a motor’s housing, measuring rotary motion directly from the motor’s drive shaft. Integrating the position feedback encoder with the motor eliminates the need for a separate encoder shaft, bearing, and seal so that kit encoders for integrated motor feedback can be more compact and less expensive than their standalone counterparts. This arrangement also reduces the number of separate components in the machine.

![Figure 2: A 22 mm integrated kit encoder for miniature motor.](image)
A servomotor is typically a brushless dc (BLDC) motor that has a built-in encoder for position feedback. Here, feedback serves two purposes: to monitor the rotary position of the motor’s shaft and to provide a commutation signal to control the current flowing to the motor’s stator windings.

**Standalone encoders** are an excellent solution for machines that use non-electric prime movers like pneumatics or hydraulics.

Kit encoders can also be used with stepper motors, providing closed loop position feedback. This improves accuracy by eliminating positioning errors due to skipped steps. (This can become a significant problem at higher speeds when the torque output from stepper motors is reduced and the likelihood of missed steps increases.) A big attraction of stepper motors is their relatively low cost, especially when compared to high-end servomotors. Inexpensive optical incremental encoders can improve positioning accuracy by verifying a step motion has been completed. For more demanding position control applications, cost-effective multiturn magnetic absolute encoders can be a better choice since these provide the controller with a complete picture of the rotary position of the motor’s shaft, including the number of rotations that have been completed.

![Figure 3: Feedback-controlled stepper motor with magnetic kit encoder.](image-url)
Measurement technologies

Several different measurement technologies are used for encoders—both standalone and kit. (Manufacturers sometimes offer the same measurement components in both their standalone and kit encoders. In this case, kit or modular products are, in effect, unbundled versions of the standalone designs.)

**Optical encoders:** are available in a range of configurations and performance levels. At the high end, precision absolute optical measurement systems can have accuracies of +/- 0.02 degree and excellent dynamic response. These are suitable for advanced servomotors and precision position control applications.

At the other end of the price/performance scale, low-cost incremental encoders based on optical measurement technology are available. While these have lower precision, they can provide feedback for inexpensive stepper motors.

While optical encoders can offer excellent accuracy, their internal components are vulnerable to contamination from dust, oil, and condensation. As well, to achieve maximum accuracy, code disks and photoreceptor arrays must be aligned very precisely, making these units vulnerable to shock and vibration.

**Magnetic encoders:** feature a small permanent magnet attached to the rotating shaft. The magnetic field from this is measured by an array of Hall effect sensors whose output is processed and filtered by software running on a tiny microprocessor built into the device. The result is good resolution and dynamic response in rugged, compact (as small as 22 mm diameter) units.

Magnetic encoders can be installed under normal factory conditions as they can tolerate moderate misalignments between the shaft and the measurement module. Further, magnetic encoders are available with multiturn measurement capabilities, with rotation counters powered by Wiegand energy harvesting technology. This elegant solution eliminates the need for backup batteries, or the complex system of code disks often used in multiturn optical encoders.
**Hollow-shaft kit encoders:** The kit encoders described above are often mounted on the back or non-drive end of the motor (see Figures 2 and 3). In some cases, it can be useful to position the rotation measuring elements at the drive end of a motor. Hollow-shaft encoders, which feature a large central opening, can be installed around the drive shaft or in other positions in the drive train. This can be advantageous when the drive system includes torque-amplifying reduction gears. Mounting a hollow-shaft encoder at the output end of a drive assembly will avoid positioning errors caused by backlash in the gear train.

**Bearing-less encoders:** are a relatively new concept. These retain the robust housing of standalone encoders, but with the rotating part of the measurement system (e.g., a permanent magnet for magnetic encoders) attached directly to the shaft of the host machine. This arrangement eliminates the bearings and shaft seals of conventional stand-alone encoders, saving space and reducing costs. The outer shell protects measurement elements from physical damage.

**Communications interfaces**

Standalone encoders are available with a wide range of communications interface options, ranging from analog and digital point-to-point connections, through fieldbus solutions, and on to industrial Ethernet systems. This makes it possible to integrate these devices into a wide variety of control systems, from simple one-axis motion controls to complex multi-parameter manufacturing automation systems. Encoders with advanced communications interfaces may also feature self-diagnostic capabilities that simplify maintenance and troubleshooting.

Integrated motor control systems (servomotors, feedback-controlled stepper motors) often require real-time controls. For this
reason, these systems usually use point-to-point (motor-to-controller) wiring layouts that avoid the latency delays that can occur in fieldbus or Ethernet systems where communications channels are shared by multiple devices. Several proprietary communications protocols are available, but for many users, the open-source SSI and BiSS protocol suites provide a reliable and cost-efficient solution.

SSI (Serial Synchronous Interface) and BiSS (Bidirectional Serial Synchronous) are digital interfaces that can support direct communications between motors and PLCs or other controllers. SSI connections offer good speed (clock rates up to 2 MHz), high resolution, flexible cabling, and reliable communication up to a few hundred meters (although baud rates are reduced for longer distances). SSI protocols provide basic error detection (broken wire, short circuit, data consistency). BiSS is an advanced version of SSI that supports real-time communications between control devices and sensors/actuators in servomotors, robots, and other automation systems. The interface also enables the controller to set operational parameters in slave devices. There are several BiSS variants, including BiSS C (continuous communications) and BiSS Line (designed for configurations that combine power delivery and data transmission in a single cable). Open-source SSI and BiSS interface standards are non-proprietary, with no-cost licences.

SSI and BiSS communications use point-to-point connections, typically RS-422. Several devices can be daisy-chained together for more efficient cable layouts.

ABOUT THE AUTHORS

Christian Fell, head of POSITAL’s North American operations, is also the company’s vice president for technology. Fell joined the FRABA Group in 2000, becoming an equity partner in 2007. He has a master’s degree in physics from the Gerhard Mercator University, Duisburg, Germany, and a diploma in medical physics from the Technical University of Kaiserslautern.
Industrial Cybersecurity is a Global Imperative

It's time to join forces. We are stronger together.

The ISA Global Cybersecurity Alliance is an open, collaborative body. We welcome members of all kinds:

- end-user companies
- asset owners
- automation and control systems vendors
- cybersecurity technology vendors
- IT infrastructure vendors
- services providers
- system integrators
- industry organizations
- government agencies
- insurance companies
- other stakeholders

Founding Members:

- Honeywell
- Johnson Controls
- Rockwell Automation
- Schneider Electric
- NOZOMI Networks
- PAS
- WALLIX
- xage Security
- MOCANA
- BAYSHORE
- radiflow
- senhasegura
- INL
- Wincsissec
- exida
- munio Security
- tenable
- DRAGS
- TiSafe
- AE Solutions
- tripwire
- Digital Immunity
- WisePlant
- Mission Secure, Inc.
- Nova Systems
- 1898 Solutions
- ACET Solutions
- CyberOwl

International Society of Automation
Setting the Standard for Automation™
How a Motion Control System Turned Edge Server

Technology that makes it possible to operate multiple virtual machines on a single hardware platform without impacting the controllers’ real-time core is the basis for new edge server systems.

Most of us will have encountered a product that was processed using a ProCom cutting control system at least once in our lives. It controls the cutting of the majority of foams produced worldwide, which are used in mattresses and furniture or in airplane and car seats. It is also responsible for numerous fabric cutting applications—regardless of whether it is a high-quality branded suit, discount jeans, or a mass-produced T-shirt. This position has been achieved by the CNC control system.

By Michael Reichlin, Real-Time Systems
and software provider since 1983 by specializing in cutting processes. The company started with foam contour cutting. The clothing market with textile cutting followed. With additional control and software solutions for plasma jet, water jet, and laser beam cutting, the company has become an expert in industrial cutting.

The company serves different cutting technologies with the industrial PC-based CNC300. The ProCom customers are mainly machine builders. Intelligent algorithms that have been developed over decades ensure an efficient cutting process and provide optimal parts nesting on the cutting machine. This guarantees maximum material utilization and high-precision cutting results. It is a particularly complex challenge, especially when it comes to 3-D foam contour cutting.

When cutting foam contours, a wide variety of contours is cut from a large block of foam with a rotating band knife, without switching the knife off and on again between the individual cutting jobs or removing it from the block. All parts to be manufactured are cut in a single work step. When it comes to the paths between the parts, it must also be considered that the parts that have already been cut do not come into contact with the band knife again and are damaged as a result. The software that users can use to optimize these cutting processes runs on the machine control hardware and can also be configured there as required. In some cases, it is also run at a CAM workstation for work preparation and then transferred to the control system, including detailed production planning for the respective day.

Focus on plasma, water, and laser beam cutters
ProCom supplies the motion control, including the graphical user interface (GUI) for machine operation with tool selection and all other machine-related functions. It is precisely this concept that has convinced machine builders in the foam and textile industries worldwide. ProCom also offers this approach to machine builders in the plasma, water, and laser cutting segments. The industrial end user is offered software that is tailored to the machine and achieves the best possible productivity. The efficient operation combined with a high
level of flexibility thanks to a wide range of functions with adjustable parameters is particularly impressive.

The company has recently developed a new solution platform for laser cutting especially for the Asian and the Chinese market. Studies show that around 50% of the forecast growth in APAC will be achieved in laser cutting. Falling production costs make laser cutting the technology of the future in many areas. A not insignificant market for ProCom is the steel market. Numerous machines for sheet metal cutting from Europe are a successful example. Whether decorative object or industrial sheet metal, with the complete package from ProCom, the best possible material efficiency is achieved in all applications. The complete package just fits.

How the motion control system became an edge server

Since a complete package consists of more than just a CNC controller, today, ProCom’s control solutions are based on hypervisor technology.
to distribute the individual tasks among dedicated virtual machines (Figure 1). However, this was not the case in the past. In earlier projects, the company implemented a control system with a dedicated CNC and PLC core and an industrial PC-based hardware platform and software as a human-machine interface (HMI). At the time, a hardware-based three-processor solution served as platform and architecture. The HMI was initially based on DOS, then OS/2 for a while, before switching to Windows and the various Windows generations.

Today, it is based on Windows 10 IoT Enterprise. Then and now, the On Time RTOS-32 real-time operating system coordinates the cutting movement of the servo axes, the integrated programmable logic controller (PLC) functionality and all safety monitoring functions needed for CNC machine control. Communication between the two discrete processors was based on the multiprocessor message exchange (MMX) protocol.

**Ongoing protocol changes**

For many years, ProCom controllers were not fieldbus-based. Instead, the servo axes were connected via the common ±10 Volt setpoint interface, which also handled the evaluation of the encoder signals including zero-pulse processing, which ProCom controls enabled as standard. With the advent of fieldbuses, the company took advantage of the fiber-optic-based digital Sercos I and later Sercos II interfaces in the mid-1990s. In 2011, a further development step was taken with the design of Ethernet-based communications. ProCom chose EtherCAT for the real-time capable protocol, having purchased the master stack. It was during this development phase that the company decided to move from a multiprocessor system with a dedicated card for the real-time processor, to a multicore-based x86 solution with one to two cores dedicated to the Windows world plus one core each to the PLC and CNC motion control functions. To implement this step, the hardware-based multiprocessor solution, which at the time had been in use for almost 30 years, needed to be virtualized on a multicore processor.
At this point, ProCom was faced with the essential question: “Make or buy?” A virtualization solution was required that separates the Windows world for GUI and work preparation functions from the real-time functions without affecting them. As part of research, the company came across Real-Time Systems, analyzed and tested the product intensively, and ultimately decided not to get involved in developing a hypervisor itself. The real-time hypervisor was fully developed, covered all the required functions, and had already sufficiently proven itself on the market. Since then, it has been in use on the ProCom controls. The real-time hypervisor also copes with significantly more complex tasks that have been added due to the requirements of Industry 4.0 and digitalization.

**Task complexity continues to rise**

Today, the ProCom system, which is scalable in performance via Intel Core processors, has an OPC-UA interface for communication with higher-level control systems that control larger system networks, or to transfer operating and machine data to manufacturing execution system (MES) and enterprise resource planning (ERP) connections. In addition, the company also offers its own

---

Figure 2: Edge computing par excellence: Thanks to real-time hypervisor support, ProCom was able to integrate the Clouver management cloud into the machine control system.
Industry 4.0 platform called Clouver, which offers numerous dashboards and tools for monitoring, management and maintenance of the machines and for which every ProCom controller on the market already has a suitable interface. For Clouver to receive all relevant data, it is necessary to be able to access the real-time platform (Figure 2). This is another point where the hypervisor plays an essential role as data must be collected in the real-time machine during the cutting process and then made available to the other stakeholders via the Windows world without interfering with the real-time processes. The need to handle all these tasks has turned the controller into a multifunctional system that resembles an edge computer as it is comprehensively networked both horizontally and vertically in all directions. As porting it toward a real-time-capable fog server would also be easy, the hardware could undergo further consolidation in the future.

The right virtualization decision

ProCom is extremely happy with its decision to buy the real-time hypervisor from RTS. Tasks have not become any easier in the past decade, and the motto to stick to one’s core competencies has clearly worked for them. “We feel in good hands with Real-Time Systems,” said Harald Müller, head of consulting and production at ProCom (Figure 3). “Our collaboration is always constructive. RTS are true experts with deep know-how and great products. The support works, the solution works, and our team that integrates the bought-in modules into our software solution has had absolutely no problems. And everything to do with regular services and updates is well organized.”
Intuitive tool for workload consolidation

As a software solution that is typically as easy or even easier to install than an operating system, the RTS real-time hypervisor is a convenient tool for developers to consolidate numerous individual dedicated solutions at the edge in a single multicore processor system without compromising real-time capability. The emerging embedded server technologies from AMD and Intel, which offer significantly more cores than current high-end embedded processors, will open an immense development field for hardware consolidation as well (Figure 3). It is therefore good to know that hypervisor solutions, which have proven themselves in the field for many years, are already available and capable.

Figure 3: Depending on the number of cores, the RTS hypervisor from Real-Time Systems can support many different system configurations.

ABOUT THE AUTHOR

Michael Reichlin is head of sales at Real-Time Systems, a German company with U.S. headquarters in San Diego. The company specializes in consolidating deterministic real-time operating systems (RTOS) with other, less critical applications on a single hardware platform.