January/February 2019

InTech®

A PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

Industry 4.0

IIoT

Smart sensors

Alarm management

Final control elements spotlight

Advanced process control: Indispensable process optimization tool

APC paradigm now more affordable, agile, scalable, and reliable

Setting the Standard for Automation™

www.isa.org/intech

Keep your system insight

with affordable, cloud-based remote access and data logging

StrideLinx Remote Access

Whether the job is down the street or across the country, with the StrideLinx cloud-based remote access solution you're always on site. Simply install and connect the StrideLinx VPN router to your machine/system, set up an account and begin using the 5GB of FREE monthly bandwidth to securely monitor, program and/or troubleshoot your remote systems from anywhere, any time.

Optional subscriptions are available to maximize your remote access capabilities:

- Cloud-based Data Logging - Unlimited cloud data storage for up to 7 years with active subscription
- Data Top Up - Increase monthly data traffic by 5, 15 or 50GB
- Service Level Agreement - Guarantees 99.6% availability, 4-hour max consecutive downtime per router
- Premium Branding - allows StrideLinx platform to be rebranded with custom company domain and contact/support information
- **NEW!** Cloud Notify/Alarming - provides customized "alarm" emails and push notifications when control limits are exceeded on HMI / PLC devices connected to the StrideLinx VPN router

StrideLinx
VPN Router
starting at
$450.00
(SE-SL3011)

Research, price, buy at:

www.automationdirect.com/stridelinx

FREE shipping - orders over $49
2-day shipping

2 YEAR WARRANTY

FREE Technical Support
Located in USA

VOTED Best in SERVICE 15 YEARS

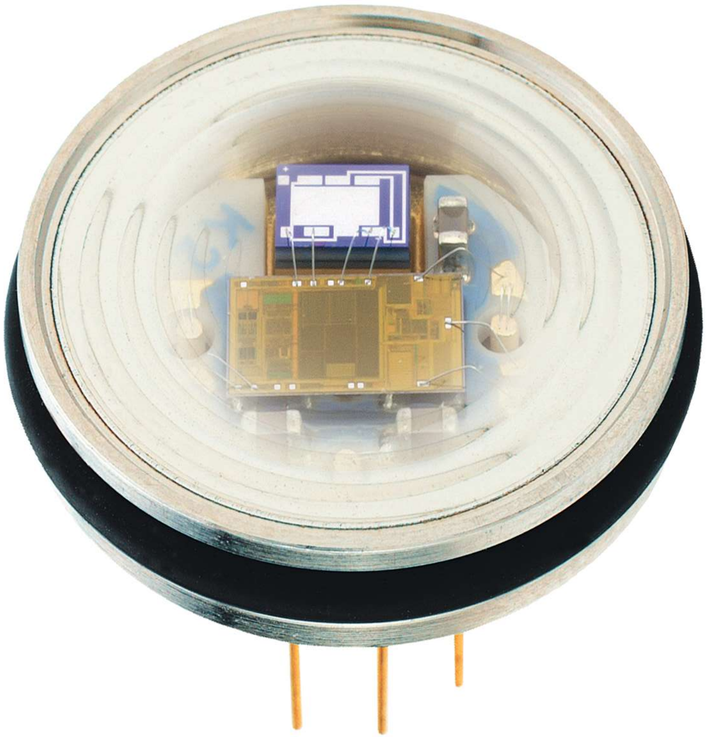
Order Today, Ships Today!

* See our Web site for details and restrictions. © Copyright 2019 AutomationDirect, Cumming, GA USA. All rights reserved.

AUTOMATIONDIRECT.com
1-800-633-0405
the #1 value in automation

kelleramerica.com

Change the way you look at pressure measurement



Embeddable OEM Pressure Transmitter

- Outstanding Total Error Band (TEB) accuracy
- Microprocessor-based signal conditioning
- Miniature hermetically sealed housing
- Pressure ranges up to 15,000 psi
- Ratiometric analog or I^2C digital outputs

oem pressure transmitters

KELLER

January/February 2019 | Vol. 66, Issue 1

www.isa.org

InTech

COVER STORY

SPECIAL SECTION: WATER QUALITY

PROCESS AUTOMATION

FACTORY AUTOMATION

SYSTEM INTEGRATION

AUTOMATION IT

DEPARTMENTS

COLUMNS

RESOURCES

www.isa.org/InTech

InTech Plus is ISA's online eNewsletter that connects automation professionals to all things automation. *InTech Plus* has technical content, educational training and videos, industry-related Q&A excerpts, and the latest and greatest on industry technology and news. *InTech Plus* focuses on a variety of topics, such as fundamentals of automation and control, certification, safety, cybersecurity, the Internet of Things, wireless devices, human-machine interface, pressure, level, temperature, and batch. All editorial content comes from a variety of sources, including ISA books, training course videos, and blogs and bits from ISA's cast of subject-matter experts. *InTech Plus* is powered by Automation.com, ISA's premier electronic publisher of automation content. Automation professionals can subscribe to *InTech Plus* at www.automation.com/subscribe.

Are you up to date on instrument calibration, cybersecurity, system migration, and industrial communications? Would you like to find out more about ISA events, training, membership, and more? ISA's YouTube channel is your resource for how-to videos on all facets of automation and control, and a great way to hear members talk about their real-life plant experiences and membership networking benefits. **www.isa.org/isa-youtube**

© 2019 InTech ISSN 0192-303X

***InTech*, USPS # 0192-303X, is published bimonthly in Research Triangle Park, NC by the International Society of Automation (ISA), 67 T.W. Alexander Drive, P.O. Box 12277, Research Triangle Park, NC 27709. Vol. 66, Issue 1.**

Editorial and advertising offices are at 67 T.W. Alexander Drive, P.O. Box 12277, Research Triangle Park, NC 27709; phone 919-549-8411; fax 919-549-8288; email info@isa.org. *InTech* and the ISA logo are registered trademarks of ISA. *InTech* is indexed in Engineering Index Service and Applied Science & Technology Index and is microfilmed by NA Publishing, Inc., 4750 Venture Drive, Suite 400, P.O. Box 998, Ann Arbor, MI 48106.

Subscriptions: For ISA members, 8.65% of annual membership dues is the nondeductible portion allocated to the *InTech* subscription. Other subscribers: $175 in North America; $235 outside North America. Multi-year rates available on request. Single copy and back issues: $20 + shipping.

Opinions expressed or implied are those of persons or organizations contributing the information and are not to be construed as those of ISA Services Inc. or ISA.

Postmaster: Send Form 3579 to *InTech*, 67 T.W. Alexander Drive, P.O. Box 12277, Research Triangle Park, NC 27709. Periodicals postage paid at Durham and at additional mailing office.

Printed in the U.S.A.

Publications mail agreement: No. 40012611. Return undeliverable Canadian addresses to P.O. Box 503, RPO West Beaver Creek, Richmond Hill, Ontario, L48 4RG

For permission to make copies of articles beyond that permitted by Sections 107 and 108 of U.S. Copyright Law, contact Copyright Clearance Center at www.copyright.com. For permission to copy articles in quantity or for use in other publications, contact ISA. Articles published before 1980 may be copied for a per-copy fee of $2.50.

To order REPRINTS from *InTech*, contact Jill Kaletha at 219-878-6068 or jillk@fosterprinting.com.

List Rentals: For information, contact ISA at info@isa.org or call 919-549-8411.

InTech magazine incorporates *Industrial Computing*® magazine.

InTech provides the most thought-provoking and authoritative coverage of automation technologies, applications, and strategies to enhance automation professionals' on-the-job success. Published by the industry's leading organization, ISA, *InTech* addresses the most critical issues facing the rapidly changing automation industry.

MOORE INDUSTRIES
WORLDWIDE
Demand Moore Reliability

Ever Wish Your Temperature Transmitters Could Talk?

349.70
BU1-2
FS FUNCTIONAL SAFETY SERIES
TDZ3
543.46
DEG C
THZ3 SMART HART TEMPERATURE TRANSMITTER
DUAL SENSOR
MOORE INDUSTRIES

RTD and Thermocouple sensor failure can be costly for any process or operation. Wouldn't it be great if your temperature transmitter gave you early warning of impending sensor failure? Moore Industries smart HART dual input temperature transmitters do just that with built-in features like Sensor Drift Detection and Sensor Corrosion Detection that alert you when your sensors are on the path to failure.

Bring predictive failure analysis right to the field with Moore Industries latest smart HART temperature transmitters.

Learn more about the Moore Industries Smart HART Dual Input Temperature Transmitters.
Call **800-999-2900**
or check **www.miinet.com/HART-Temperature**

Automation professionals, people are depending on you!

By Bill Lydon, *InTech*, Chief Editor

Automation professionals are major contributors to a manufacturing and process company's competitiveness and are vital for success. Low labor cost is no longer a winning manufacturing strategy, resulting in the growing implementation of automation in countries worldwide to become leadership producers. Modernizing manufacturing is vitally important in this and has spawned worldwide initiatives centered on automation, including Germany's Industrie 4.0, Made in China 2025, Japan Industrial Value Chain Initiative (IVI), Make in India, Indonesia 4.0, Latvia: National Industrial Policy Guidelines 2014–2020, Initiative for Polish Industry 4.0, Italy: Industria 4.0, and France: Industrie du futur.

Another driver for automation is the retirement of experienced workers, which is a major issue when trying to find manufacturing and process personnel to fill the vacated positions. This is a demographic issue, since almost all countries have experienced lower birth rates. The populations are aging, and there are fewer young people to enter the workforce. Ignoring the moral and ethical issues, there simply are not enough people who can be paid low wages to fill low-level manufacturing positions. Compounding the challenge is the need to convince young people there is a future in manufacturing.

Automation improves productivity, quality, the environment, and profits. Automation's positive impact on the environment may not seem obvious, but properly done, automation lowers energy requirements, optimizes raw material utilization, and lowers emissions.

The good news is automation creates better manufacturing and process plant environments that are more productive. This requires more educated workers to implement, run, support, and maintain automation systems. The challenge is to motivate and train young people to work with modern manufacturing technology that will yield them higher-paying and more personally rewarding jobs.

The challenge is to motivate and train young people to work with modern manufacturing technology that will yield them higher-paying and more personally rewarding jobs.

There are two big challenges that all of us would do well to address. First, younger people need to understand that manufacturing and process industries are exciting places where engineers apply technology and contribute to society and the environment in a positive way. The other challenge is to provide meaningful education, coaching, and management for younger people to facilitate their development in becoming automation professionals.

The International Society of Automation and the organization's media, *InTech* magazine and Automation.com, are focused on these goals.

What's in it for you?

It may be an old adage, but "a rising tide lifts all boats," meaning improvements in the general economy will benefit all participants. Participating in the development of young people to become automation professionals helps build stronger communities with positive outcomes.

We certainly invite you to join in this endeavor. ■

ISA *INTECH* STAFF

CHIEF EDITOR
Bill Lydon
blydon@isa.org

PUBLISHER
Rick Zabel
rzabel@isa.org

PRODUCTION EDITOR
Lynne Franke
lfranke@isa.org

ART DIRECTOR
Colleen Casper
ccasper@isa.org

SENIOR GRAPHIC DESIGNER
Pam King
pking@isa.org

GRAPHIC DESIGNER
Lisa Starck
lstarck@isa.org

CONTRIBUTING EDITOR
Charley Robinson
crobinson@isa.org

ISA PRESIDENT
Paul Gruhn, PE, CFSE

PUBLICATIONS VICE PRESIDENT
Victor S. Finkel, CAP

Advanced process control: Indispensable process optimization tool

APC paradigm now more affordable, agile, scalable, and reliable

By Allan Kern, PE

In this article, as in industry, advanced process control (APC) refers primarily to *multivariable* control. Multivariable control means adjusting multiple single-loop controllers in unison, to meet constraint control and optimization objectives of an additional set of related process variables.

Multivariable control is a central aspect of nearly every industrial process operation. Historically, operators adjusted single-loop controller set points and outputs (i.e., "the available handles") to control a superset of constraint and optimization variables (i.e., "controlled variables"). They did this based on experience, knowledge of the process, ongoing operating conditions, and input from the greater operating team, which includes supervision, process engineers, and production planning. APC endeavors to automate this task, in order to capture incremental gains in capacity, efficiency, quality, etc. Figure 1

FAST FORWARD

- APC progress has stalled, because its high cost of ownership limits its applicability. Most APC resources now go toward support and maintenance of existing applications, not new applications.
- Most APC benefits come from a minority of variables, while costs are compounded by the number of variables, which suggests applying the Pareto principle (80/20 rule) to APC controller design.
- Experience shows that detailed models and embedded optimizers are not always necessary for the essential role of multivariable control, which unlocks many new possibilities for APC.

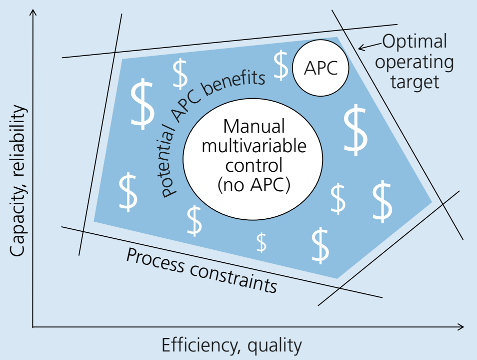


Figure 1. Manual versus automated multivariable control. Automated multivariable control can capture incremental earnings, because it automatically backs the process away from encroaching constraints and pursues receding constraints. With manual multivariable control, operators tend to keep the process farther from constraints and make moves less often, typically incurring an associated penalty in capacity, yield, energy, or quality.

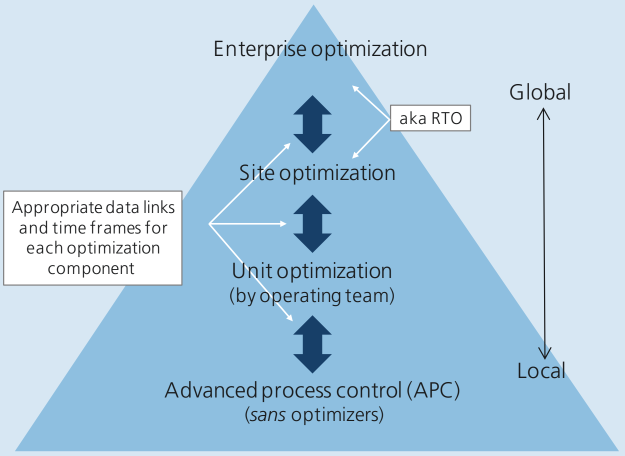


Figure 2. Updated process optimization paradigm. The essential role of APC is multivariable *control* (i.e., pushing constraint limits and pursuing optimization targets at the control system level), where the related process values—not the limits and targets themselves—are subject to change in real time. Updated limits and targets, which are few and infrequent, propagate from the upper layers of the pyramid as appropriate.

depicts the essential difference between manual and automated multivariable control.

The most common automated multivariable control technology in use today is model-predictive control (MPC). Prominent characteristics of MPC include the use of detailed process models, embedded optimizers, and a generally large-matrix approach to application design, i.e., dozens of variables and often hundreds of models. This combination was expected to be transformative for process control, but it has met with unexpected consequences in cost, maintenance, and reliability. Industry has so far stood by MPC, so that more agile, affordable, and "owner-friendly" alternatives have been slow to emerge and evolve.

Optimization

Within operating facilities, process optimization is carried out by many participants, such as production planning, process engineering, and operations. Together, these groups arrive at current constraint limits and optimization targets, and propagate them to the control systems via computer links, operating orders, word of mouth, etc. Most constraint limits and targets rarely change, while a handful change with operating conditions, such as feedstocks, equipment out of service, and time of year. On top of these activities, there may be similar sitewide and enterprisewide optimization layers (figure 2).

In this picture, the role of the embedded MPC optimizer comes into question. It may have made sense in 1985, when few other real-time optimization programs existed in industry, but today the entire optimization hierarchy is nearly as automated as it needs to or can be. This makes the embedded MPC steady-state optimizer largely redundant, while it continues to add cost and complexity to the MPC application.

MPC also incorporates "path" optimization, whose objective is to minimize transient cost and error as it moves the process from current conditions to optimal conditions. However, taking a simple straight-line path, while observing process speed limits along the way, may be a more effective strategy in most cases. As with driving a car, observing speed limits and arriving safely is usually more important than arriving quickly. Industry endorses this concept whenever it uses approaches such as move suppression, extended closed-loop response times, soft limits, and reduced optimization speeds. Why not just post a safe speed?

The essential role of APC at the control system layer is *control*, i.e., to push constraint limits and pursue optimization targets in the live process environment, where the related process values—not the limits and targets themselves—are subject to change in real time. Control needs to execute at high frequency, but optimization normally does not. This paradigm has the potential to simplify APC technology by eliminating embedded optimizers that are potentially redundant or unnecessary in most applications.

Process models

Model-based control requires reliable process models. In the original APC paradigm, this need was met by a plant test and subsequent model identification, with the resulting models expected to have an indefinite life expectancy. However, experience has shown that many models change frequently, even dynamically, for a wide variety of reasons. Over the years, the conventional wisdom regarding model life has been reduced to five years, and then to two years. Today industry is pursuing real-time model updates. But even this is unlikely to "square this circle," for the same reasons that derailed autotuning. Model change poses a fundamental conundrum for autotuning and model-based control.

To move forward, APC needs to embrace the idea that process models are basically a moving target. This has always been a fact of life in the single-loop tuning world, where the principles of preserving process stability and respecting a degree of the unknown have always taken precedence over minimizing transient error. In retrospect, there is no reason these principles should not apply to multivariable control, too. Indeed, MPC experience shows that these principles remain universal and indispensable.

The same insight can be gleaned from examining how operators historically carry out manual multivariable control, which they do without relying on detailed models or optimizers. By virtue of their experience and training, operators know important constraints, optimal targets, and appropriate handles; they make moves that safeguard process stability and respect the historical degree of uncertainty; and they monitor *actual* process response—not yesterday's or last year's response—before making further adjustments accordingly (figure 3).

The effectiveness of manual multivariable control has always been dependent on the amount of time and initiative the operator has available, and upon each operator's individual level of expertise. These—timeliness and consistency—are the hallmarks of automation.

Matrix design

In the original APC paradigm, where models were assumed to be reliable, having a larger matrix (more variables) and a denser matrix (more models) was considered the best practice, because in principle it resulted in a more complete solution. But in today's world, where models are understood to be variable, more models can translate into more problems, for both control and optimization. Industry has experienced this in the high maintenance and degraded performance of many MPC applications.

The extended operating team, especially operators and process engineers, normally know a priori how to effectively manage process constraints and pursue optimization targets, by virtue of their knowledge and experience. This suggests that existing (established and proven) operating practices can provide the best basis for matrix design. It will also normally result in a much smaller and less dense matrix than the traditional plant test paradigm, whose strategy is to cast a wide net.

A smaller matrix can be expected to reduce cost and maintenance proportionately, especially if the remaining variables and models are the essential ones, already proven in use by virtue of actual operation. In the traditional paradigm, the APC project goal is usually "optimization," based on a large-matrix strategy, but in the small-matrix paradigm, the central goal is "automation," based on existing, proven, manual multivariable control operating practices. This may sound less lofty, but it could be a more effective focus for APC going forward.

Lessons from feedforward

The primary limitation in figure 3, from a process control standpoint, is the lack of model-predictive feedforward control action, which has always been a cornerstone of the MPC paradigm and a key piece of the expected transformation (of process control into a more exact science). However, feedforward is the single-loop equivalent of model-predictive control, and its long history tells a different story.

The potential power of feedforward (to reject disturbances proactively) has always been well known. Feedforward function blocks have been available since industry's first distributed control systems (and in programmable logic controllers, analog, and pneumatic systems before that). Yet, historically, feedforward has found very limited usage, even at the much more manageable and selective single-loop level, due to the complexity, risk, and maintenance a feedforward model adds to any loop. Feedforward has a high bar and is generally warranted only where its benefits are substantial and a reliable

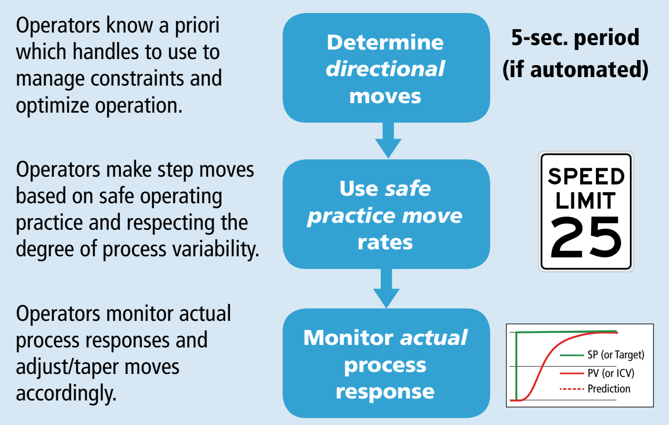

Operators know a priori which handles to use to manage constraints and optimize operation.
Determine *directional* moves
5-sec. period (if automated)
Operators make step moves based on safe operating practice and respecting the degree of process variability.
Use *safe practice move* rates
SPEED LIMIT 25
Operators monitor actual process responses and adjust/taper moves accordingly.
Monitor *actual* process response
SP (or Target)
PV (or ICV)
Prediction

Figure 3. Historical manual multivariable control method. Notably, this method does not require embedded optimizers or detailed models. Rate-Predictive Control (RPC®) and Model-less Multivariable Control (XMC®) technology are based on this concept.

model is possible. Using the installed base of control systems throughout industry as a guideline, perhaps one in 10 loops warrant the use of feedforward, and the rest will perform satisfactorily, if not more reliably, based on feedback control alone.

This calls into question the MPC paradigm of "wholesale" feedforward—literally hundreds of mass-produced feedforward models—and suggests it might be a source as much as a solution to the persistent maintenance and performance record of MPC. The top priority of APC—as with single-loop control—is to reliably close the loops, and not necessarily to use feedforward in doing so. Classic selective feedforward strategy is implicit in figure 3.

Updated paradigm

These perspectives point toward an APC paradigm that is more affordable, agile, scalable, and reliable, based on durable qualitative (not detailed) models, sans embedded optimizers, and with more intuitive and succinct matrix designs. Figure 4 compares the traditional and proposed paradigms.

In operating facilities, multivariable control applications come in all sizes—from a handful of variables to several dozens—so that a smaller footprint solution can bring progress on both fronts. It can provide more appropriate tools for the many applications that have remained below the radar of industry's large-matrix paradigm. And it can provide an alternative reengineering strategy for industry's many high-maintenance legacy applications.

The proposed paradigm derives from lengthy experiences and lessons under the traditional APC paradigm. To the extent this new paradigm has yet to fully emerge, industry may benefit from adopting it as a working vision going forward, to pursue these insights and lessons, encourage outside-the-paradigm thinking, move APC beyond its original paradigm, and bring about new and more viable and sustainable APC solutions for industry. ■

ABOUT THE AUTHOR

Allan Kern, PE (allan.kern@apcperformance.com), has 35 years of industrial process automation experience and has authored dozens of papers on more practical, reliable, and sustainable advanced process control solutions. Kern helps companies improve process efficiency, quality, and profits on site or with online consulting complementing in-house resources, helping bridge a skill shortage at many sites. He is the founder of APC Performance LLC and the inventor of patented Rate-Predictive Control (RPC®) and Model-less Multivariable Control (XMC®). For more information, visit APCperformance.com

View the online version at www.isa.org/intech/20190201.

RESOURCE
"The big story behind auto-tuning"
www.controleng.com/articles/pros-and-cons-of-autotuning-the-big-story

Traditional (largely obsolete) APC paradigm	Emergent APC paradigm
Incorporates detailed models, embedded optimizers, and large-matrix design practice.	Based on simple qualitative models, sans optimizers, and small-matrix design practice.
Wholesale use of feedforward model-predictive control.	Selective use of feedforward control.
Dominant focus on modeling and optimization.	Primary focus on multivariable control.
High cost and maintenance, limited life cycle.	Low cost, long low-maintenance life cycles.
Highly specialized, often third-party software and support.	Core competency. Locally owned by on-site DCS engineers.
Special budgeting and planning activities.	Falls within normal operating plans and budgets.
Complex DCS integration. Security and reliability issues.	Native DCS deployment.
"Wide-net" matrix design strategy, based on extensive plant testing.	Small-matrix design practice, based on existing operating practices.
Low agility, often an impediment to manufacturing flexibility.	High agility, complements modern flexible manufacturing criteria.
Goal is "optimization," based on large-matrix design strategy	Goal is "automation," based on existing proven operating practices.
Embedded steady-state optimizer, which is redundant while adding cost and complexity.	Uses optimization results from higher layers of pyramid.
Embedded path optimization to minimize transient error and cost.	"Straight-line" path optimization while observing process speed limits.

Figure 4. Compare and contrast the traditional APC paradigm versus a new working paradigm (vision or road map) for APC going forward.

Integrating IT into process manufacturing

Many in OT view IT moving into process plants as a good thing due to Industry 4.0, IIoT, and other initiatives

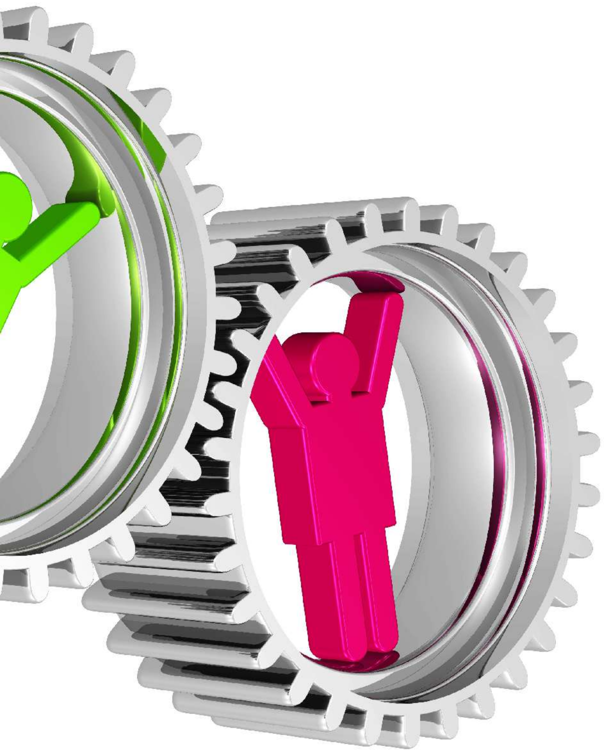
By Christopher Logue

Much of the discussion about the development of Industry 4.0 has concentrated on discrete industries. Manufacturers of all sorts of products, from cars to shoes, are discovering how integrating the entire manufacturing process—from design to aftermarket service—can be supported by one all-encompassing digital system. When applied well, these concepts are possible and very effective, but companies find there is much to learn when trying to implement them.

So, what is the situation with process manufacturers? What does Industry 4.0 mean to a refinery or fine chemical producer? Automakers show how a consumer can use a website to order the desired combination of options and have the car made exactly as specified with everything carried out automatically. How are such concepts relevant to a continuous processor or even batch manufacturer, with industrial customers instead of consumers?

Moving manufacturing in these directions may not be practical or even desirable in process industries. At the same time, the ability to create more comprehensive and integrated digital platforms to support production is very compelling. The connected enterprise elements of Industry 4.0 can be adapted and applied for process manufacturers. However, implementation has its challenges, and one of the most serious is how it drives the integration of existing plant automation systems and networks with business networks. It is the integration of corporate networks and plant networks, also known respectively as information technology (IT) and operational technology (OT).

These two sides have traditionally been separated, perhaps not like oil and water, but they



FAST FORWARD

- IT and OT personnel have often been at odds in process manufacturing plants and facilities.
- Industry 4.0 and the IIoT force IT and OT to work together, which can be difficult.
- New tools and techniques foster improved working relationships between the two groups.

have had their own domains, responsibilities, and ways of doing things. IT responsibilities center around corporate functions and business applications. Technologies and platforms need to stay up to date so the latest cybersecurity and enterprise analytical tools can be used.

OT responsibilities concentrate on keeping manufacturing running safely, reliably, and efficiently. Technology can bring a variety of benefits, but there needs to be a good reason to change something that works.

Setting priorities

The responsibilities of network managers of all stripes have been defined by three main areas of concern, which can be arranged into "triads" indicating relative levels of priority (figure 1).

1. network availability
2. system integrity
3. data confidentiality

IT managers tend to stress number three as paramount because of the criticality and sensitivity of company and customer data. System integrity is important to maintain, but if it is necessary to interrupt network availability to install a patch or make some other modification, it can be done within reason. Some contend this characterization is an oversimplification. They point out how availability can be enormously important for networks handling financial transactions and the like, but even these types of networks can be shut down for extended periods after hours and on weekends.

OT managers, on the other hand, do generally stress number one above the others, although two and especially three are not the distant followers they once were. Availability is necessary to keep production running, which is clear enough. Maintaining a high degree of system integrity is necessary to support availability, so those two priorities are linked.

Data confidentiality and cybersecurity long took a back seat. It was assumed, or at least hoped, that the relative isolation and proprietary peculiarities of manufacturing networks provided some protection—the old security-by-obscurity argument. The data that could be captured by a hacker would be effectively indecipherable anyway. This has changed with

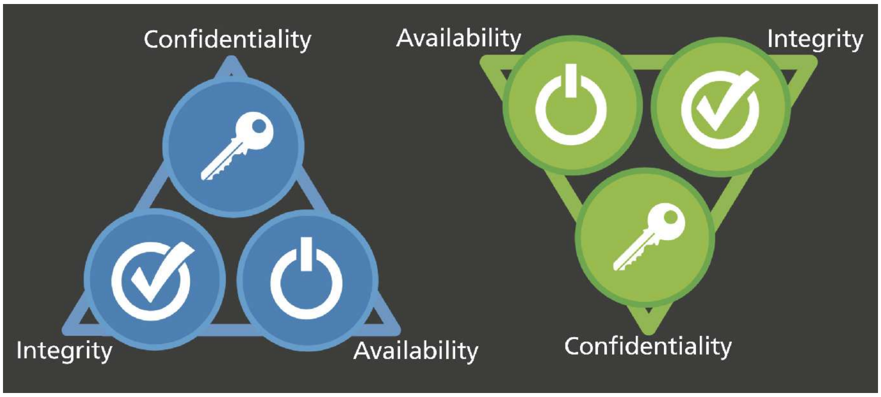


Figure 1. The triads representing the areas of concern for IT (on the left) and OT (on the right) are becoming less distinct as technologies and responsibilities become more similar.
Source: Cisco

the realization that cybercriminals can disrupt networks and hamstring manufacturing, whether they are trying to steal data or not.

Although the IT and OT triads still have their differences, they are not as pronounced as they used to be. Nonetheless, each department tends to be evaluated against its own set of success metrics. For IT:

- data security
- risk reduction
- cost savings
- data visibility

For OT, it is more about production:

- overall equipment effectiveness
- operational safety
- production uptime and availability
- product quality

Putting aside differences

So, when the two areas work together, what are the biggest adjustments that have to take place? To begin with, "working together" means IT people moving into the plant. Such togetherness is often imposed on the OT folks, like a shotgun wedding. Situations where individuals from the plant are brought in to work in IT are far rarer—OT stays off the carpet. OT tasks are more specialized and there are generally fewer of those people.

When IT people come into the plant for the first time, they are usually shocked by what they find. Many of the younger technicians have never seen some of the technologies they encounter. "This computer is still running Windows XP." "Where do I find a driver for a dot-matrix printer? I do not even know what that is." "What's Modbus?" "Is everything this old?"

Once the initial shock has worn off, the OT guide may have to restrain some of the new person's enthusiasm. "We can't replace that Windows XP machine, because the software on it is necessary to run this part of the production unit. It was developed by vendor X and has never been updated to run on later versions of Windows. If you update the OS, it won't work correctly anymore, and this part of the production will stop. We haven't rebooted this computer in four years, so don't touch it."

The OT guide will also have to remind the new person how interconnected things are in the plant, and how changing something in one area can ripple through and affect others. Gradually IT technicians begin to see and understand their actions in a larger systemic context rather than thinking of each task in isolation. The notion of how a change might affect safety or production will, hopefully, begin to sink in, and the larger picture will take shape.

Going in unarmed

For many IT technicians, moving into the plant means leaving their favorite networking tools behind. While standard security techniques, such as switchport security and intrusion detection on the backplane, are common approaches on corporate networks, they might not work in the plant. Switches may be configured to work with specific equipment and have specialized scan rates, throughput, or other settings. Changing something may interfere with a controller talking to a workstation.

Although not optimal for working with defensive strategies, leaving part of the network in a suboptimal state may have to suffice until a more comprehensive solution can be found. These situations demand balance and require working with all the stakeholders to avoid making a network more secure but unable to perform its primary function.

Once IT technicians have spent some time in the plant, they might be assigned a specific task that will mean using their new knowledge to find and extract some low device-level network data. Say the task is to create a soft sensor, using data from a group of five process instruments installed in a production unit to support calculating a value that can be used to help optimize the process. The instruments are all installed and operating, so the assignment is simply finding a way to extract the relevant data streams, so they can be sent to a controller with the new analytical algorithm. However, in the OT world things are not always as simple as they seem.

What's all this analog stuff?

The IT technicians begin to examine the situation and find a complex situation:

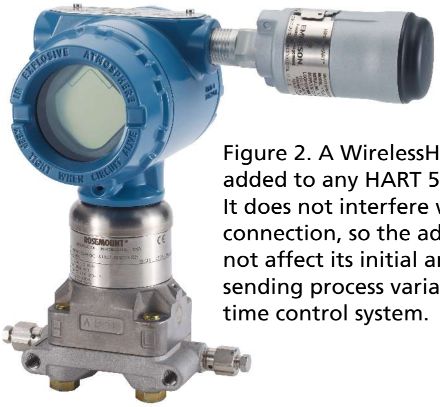


Figure 2. A WirelessHART adapter can be added to any HART 5 or later instrument. It does not interfere with the wired connection, so the added capabilities do not affect its initial and essential task of sending process variable data to a real-time control system.

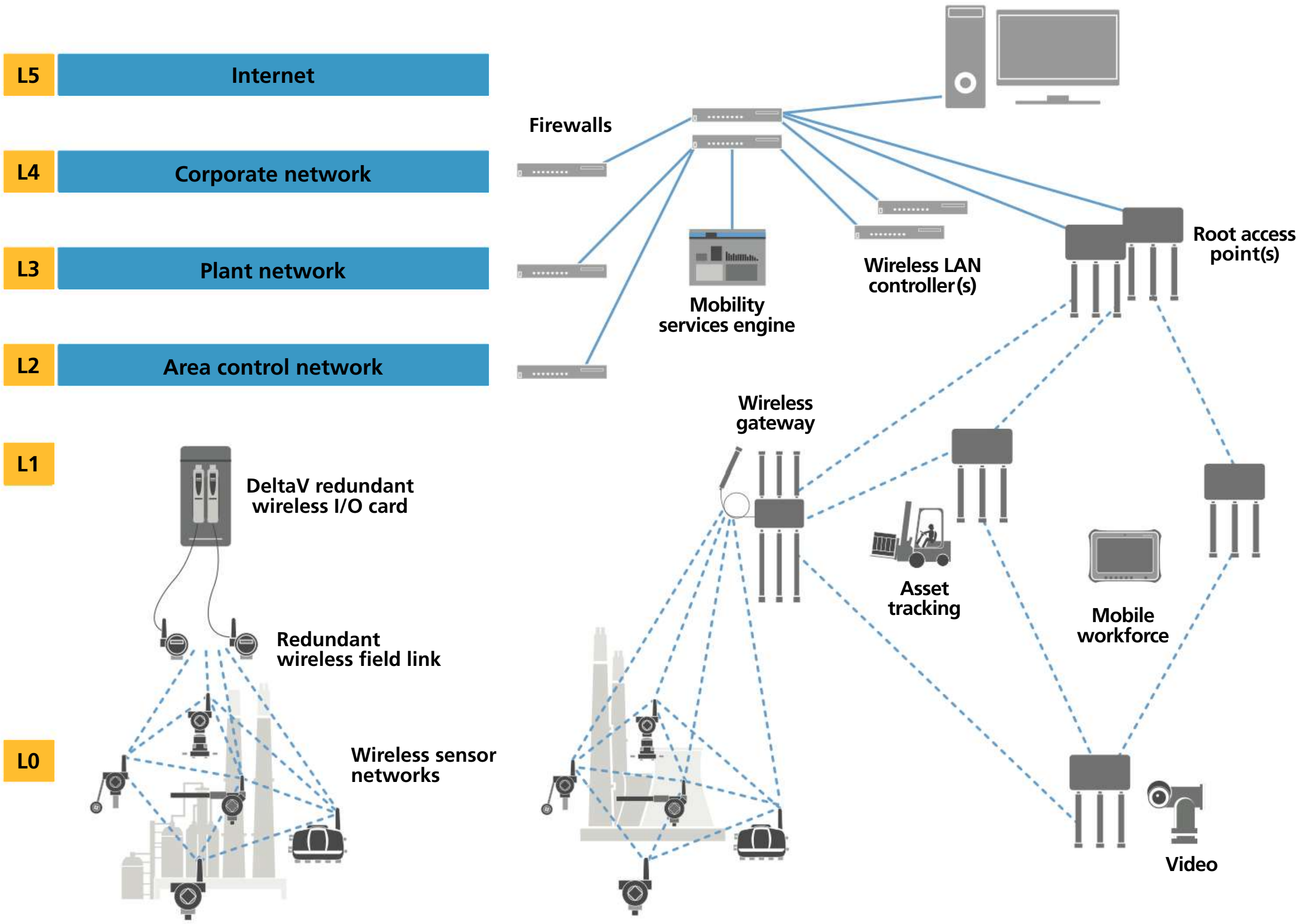


Figure 3. WirelessHART networks exist side by side with wireless Ethernet, and wired Ethernet can serve as backhaul for the wireless instruments.

- The instruments are all in place and connected to the distributed control system (DCS) I/O cards, sending their information continuously.
- The DCS was installed almost 20 years ago and uses standard dumb analog I/O, meaning all the instruments for the project are communicating using conventional 4–20 mA current loops.
- The DCS has a historian that was added about 10 years ago, and it serves as the main interface for connections to the corporate network. However, data streams from these specific instruments are not captured individually.
- The historian is not easy to modify, so it is not available to serve as the means to provide data for this project.
- The instruments themselves are working just fine, so there is no interest in upgrading them.

So, what does our IT team do? What does a signal of 17.54 mA even mean? The standard IT tools simply do not apply in this situation, so there is no way to talk to those instruments. What mechanisms are practical or even available to capture data from these five instruments?

One possibility emerges: something called a highway addressable remote transmitter, or HART. It is a new one for some technicians, but it means there is a digital signal superimposed on top of the analog signal. Digital sounds more promising than analog, but it is a long way from Ethernet. It is still a different protocol, and there is no mechanism to talk to the instruments. Or is there?

All the instruments involved here have HART capability, but the I/O for the DCS cannot handle this protocol, so it is no help at all. Still, there are mechanisms that can capture the HART data externally without affecting the basic performance of the instruments. Wired solutions are cumbersome and costly due to the cabling necessary to make the connections and the code written to operate them. The budget and schedule for this project will not cover such an approach.

Applying newer tools: WirelessHART

A more recent technology, developed after these devices were installed and operating, is WirelessHART. It can carry all the data, including primary and additional variables, diagnostic data, and configuration mechanisms. These instruments have no wireless capability, but a WirelessHART adapter (figure 2) can be added to send all the information via a wireless signal without interfering with the basic wired con-

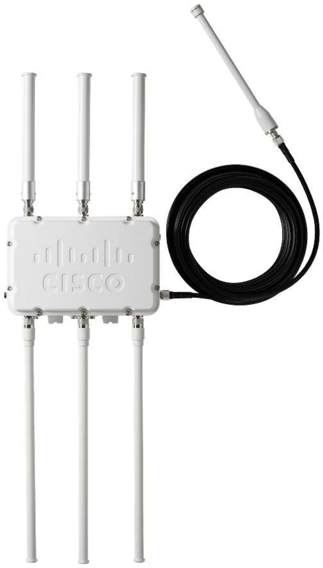


Figure 4. New industrial wireless routers have the capability to serve both WirelessHART and wireless Ethernet devices simultaneously.
Source: Cisco

nection to the DCS. Nothing about the existing setup has to change.

These wireless adapters communicate with a gateway, which captures the data and sends it wherever it needs to go using a wired Ethernet connection. Finally! Something an IT person can relate to. Here is a bridge to span the chasm between these two analog and digital worlds, and it can be done painlessly and without high cost or installation hassles.

Many plants already have a WirelessHART network infrastructure in place (figure 3), and it can operate without interfering with wireless Ethernet networks in the same space. In fact, there are wireless Ethernet routers that include radios to communicate with WirelessHART transmitters in addition to wireless Ethernet (figure 4). These two protocols are different, but they can work side by side very easily, with each supporting its respective types of devices.

These multiprotocol routers are simple and economical solutions that combine plant and field networks into a seamless architecture. The IT team can now use something familiar to quickly enable technologies that the OT team can implement to better meet their success metrics of improving productivity, safety, and operational efficiency. The routers also have world-class security and data reliability. Next-generation versions of these routers in development will bring even more capabilities and flexibility around implementation.

These types of communication make many Industrial Internet of Things (IIoT) implementations possible and practical. When IP-based networking extends farther through the levels of plant networks, and protocols such as WirelessHART can reach individual end devices, a company can realize a true connected enterprise. The assignment to gather data from five process instruments can be accomplished in a week instead of months.

Where there used to be a gap between the two sides, now there is barely a line, and in some places, it is not even visible.

OT as legacy

Anyone watching the development of industrial automation technology over the past 15 years has seen many technological changes. The notion of proprietary equipment, unique operating systems, and networking strategies is rapidly disappearing. Therefore, OT is looking more like IT all the time, and to most, this is not a bad thing.

Where there used to be a gap between the two sides, now there is barely a line, and in some places, it is not even visible. IP-based networking strategies are being used for industrial applications as issues such as determinism get worked out. The ease with which WirelessHART and wireless Ethernet can interface and work together is a prime example.

This convergence helps mitigate one major challenge for process manufacturers: personnel. The number of people with qualifications and experience to work with older systems is rapidly declining, and, as mentioned earlier, younger engineers do not see a great future in learning systems as they are being phased out.

Automation suppliers are taking advantage of the change as well. A DCS offered today is far less dependent on specialized hardware. In some respects, the new systems are far more upgradeable than their predecessors, to the extent that the thought of having to perform a system migration may no longer be necessary. Just as a personal computer purchased today may have its operating system upgraded multiple times over its useful life, with more configurability via software, industrial automation systems can be incrementally improved more easily.

In the meantime, for the majority of companies, maintaining the old and new will continue. Smart individuals will realize the importance of keeping a foot in both camps and learning all they can about how everything works together. An IT professional who understands how manufacturing works and what is necessary to support it will have opportunities for some time to come. ■

ABOUT THE AUTHOR

Christopher Logue (Christopher.Logue@emerson.com) is the global product manager for wireless technologies at Emerson Automation Solutions. He is an IIoT enabler for the implementation of new wireless technologies in process plants worldwide. Logue holds a BSME degree from the University of Villanova.

View the online version at www.isa.org/intech/20190202.

RESOURCES

"Industry 4.0 for process"
www.isa.org/intech/20170601

"Getting IIoT to live up to the hype"
www.isa.org/intech/201702web

"IT and OT convergence?"
www.isa.org/intech/201706talk

We understand you need insightful process information to help you run your plant efficiently.
MEASURED VALUE
+ ADDED VALUE
You make confident decisions backed by process data and a complete portfolio of services and solutions to support you.

IIoT remote monitoring

By Bill Dehner

Remote machine monitoring is becoming a common feature of automated equipment as part of Industrial Internet of Things (IIoT) implementations. The software and hardware required varies from vendor to vendor, but most use the same intranet- or Internet-based technologies.

The use of these maturing technologies is making it easier and less expensive to implement remote monitoring connections to machines and processes. These remote monitoring connections are usually made to programmable logic controllers (PLCs) and human-machine interfaces (HMIs) via internal intranets or the Internet, often via a virtual private network (VPN) router. On the other end of these connections are devices such as PCs, smartphones, and tablets. Each of these devices has built-in digital communications with Ethernet connectivity.

This remote connectivity goes beyond access for troubleshooting. In many cases, the remote devices are connected to the automation system to be eyes into the machine for optimizing operation, sending data and production information to engineering, and providing management with summary and analysis information. This article takes a closer look at the methods to remotely monitor a machine or process.

Remote access to HMIs

Many embedded and PC-based HMIs can provide remote access via PCs, smartphones, and tablets. The low cost and small footprint of an embedded HMI is a good example of common remote access connectivity via the HMI's web server to remote devices (figure 1). Because the HMI has web server functionality, web pages can be configured to reside in it, and these web pages can be accessed by any device capable of running a web browser.

Embedded HMIs provide much of the functionality of a PC-based HMI, including remote monitoring, and are designed for industrial use in harsh environments. The comments below apply to either solution. Ethernet and wireless technologies—along with defense-in-depth, authentication, and firewalls—are making remotely monitoring HMIs through smartphones and tablets part of an operator's, manager's, or engineer's daily routine.

A user can monitor several remote sites via a smartphone or tablet, allowing a proactive response to problems based on information pushed from the HMI (e.g., an email or text message). A "low parts detected" or "motor high temperature detected" message sent to operations and maintenance personnel provides real-time information that workers can act upon to reduce downtime and improve productivity. The data is pushed to users when necessary, with no need to open a browser and connect to the HMI, although this is often the next step to drill down for details.

Some HMIs can log and store data on a periodic basis or when triggered by events. As part of a remote monitoring daily routine or when a message or alarm is received, the user can access the HMI via a web browser to view additional information. This same information can be sent to interested users by email using file transfer protocol (FTP). This type of remote monitoring provides usable information related to both real-time and historical trends to help reduce cost and downtime, while increasing productivity.

FAST FORWARD

- Many HMIs can be remotely accessed via a web browser or an app running on a smartphone or tablet.
- Remote access to a PLC is often one-way only, from the PLC to remote devices, to prevent tampering with real-time control.
- Remote access via VPNs has a very high degree of security, and hosted VPN solutions simplify setup, use, and maintenance.

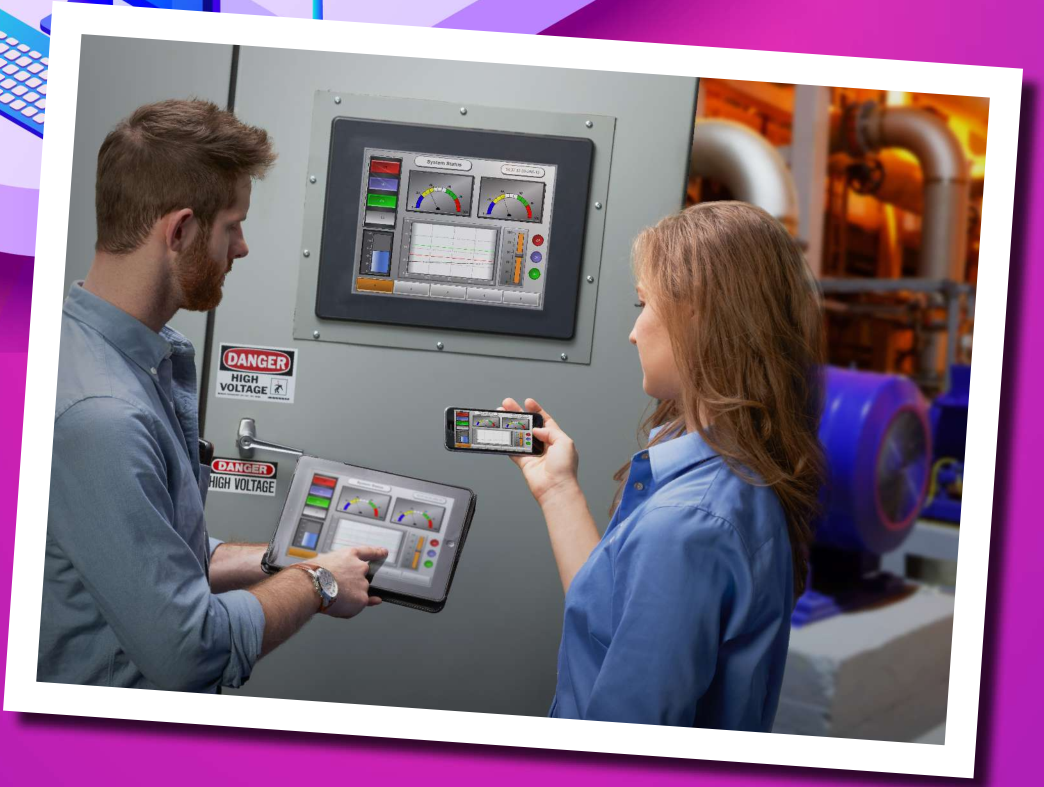


Figure 1. HMI remote access: This C-more HMI touch panel provides remote access functionality, as well as local control and monitoring.

There are several ways to remotely monitor PLCs and HMIs, but VPN connections are most secure

HMI mobile apps enable remote users to connect using Wi-Fi, cellular, and Ethernet connections. These remote users can operate and monitor the local HMI system with limited access to functions and controls of the HMI application.

Proper control, security, and safety procedures should be considered and implemented when using any remote access feature. Connecting an HMI on an enterprise network or the Internet exposes it to security risks. HMIs have many ways to control, limit, and log remote users. As a minimum in an HMI application, a user must log in and enter a password to access an HMI remotely. Also, default IP addresses, user names, or passwords should never be used.

For additional security, an encrypted VPN connection is recommended for remote connections. Using a VPN, which is discussed later, greatly reduces the chances of malicious behavior and unauthorized connections.

PLC remote control

As with the HMIs discussed above, remote access to local PLCs is possible via PCs, smartphones, and tablets. This remote access can provide control functions as well as access to logged data, or direct access to a PLC's tag data.

Note that much of the HMI monitoring is of data created, read, or collected by the PLC. It is the PLC that connects to most of the sensors, motors, valves, and other field devices to perform its control and monitoring functions. Therefore, access to a PLC often will provide connectivity to all the data required, with additional functionality in terms of control and access to PLC data not transmitted to the HMI. Like HMIs, many PLCs have remote access through features such as an embedded web server and push notifications.

PLCs often have some data handling capabilities built in, including data logging, a key requirement considering today's quest for more data storage. Some controllers include built-in and removable storage for many gigabytes of data, and remote access to same.

Connecting an OPC server running on a PC to a PLC's OPC client software provides a means of data interaction between the PC and standard databases found in mid- to enterprise-level platforms, such as material resource planning and enterprise resource planning systems. Remote access may include connectivity to this collected data to retrieve, update, add, and delete records in a standard database such as SQL Server, Microsoft Access, or ODBC.

Much of this peer-to-peer or business system networking and eventual remote access is enabled by a controller's communication capabilities. Some best-in-class controllers include seven or more communication ports, including USB, serial, and Ethernet (figure 2). EtherNet/IP and Modbus TCP/IP protocols are usually used to create remote connections among the Internet, PLC, and smart devices.

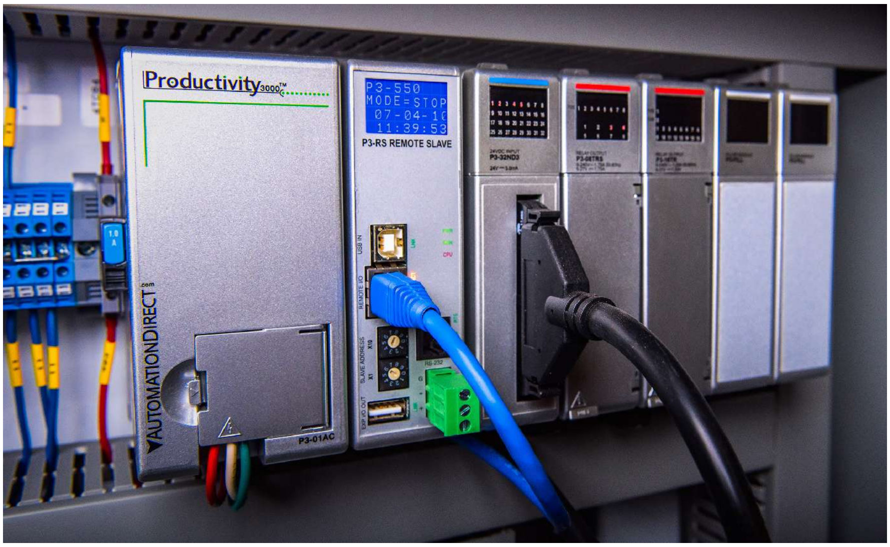


Figure 2. Modern controllers, such as this AutomationDirect Productivity3000, have data handling capabilities, including built-in data logging, and communication features for remote monitoring via email, web browsers, and mobile apps.

Email and web server functionality are standard features on many PLCs, allowing the controller to send an email with text or embedded data to email recipients via the PLC's Ethernet port. With built-in programming instructions, adding an IP address, email address, subject, message text or embedded data, and recipient email address is all it takes to send an email from the CPU module through an SMTP server. This gives technicians or operations simple monitoring of machine status or alarms.

Web server functionality is also available on some controllers for remote monitoring purposes. With an Internet connection and a device capable of hosting a web browser, remote users can view system tags, error logs, and event history. They can also view any data logged to the controller's internal memory, thumb drive, or MicroSD card.

This web server functionality can often be accessed by a remote monitoring app running on a smartphone or a tablet. Apps simplify remote Wi-Fi or cellular connections to smartphones and tablets from PLCs. Users can monitor the local PLC system via tags configured for remote access inside the tag database of the controller. Security log-on requirements are provided to protect the data, but that is not enough in some critical applications, where a VPN connection is needed for a higher level of cybersecurity.

VPNs and security layers

Leveraging the IIoT requires a secure remote access solution to collect, store, and share data. Cybersecurity is more important than ever as threats continue to rise, and as more systems are monitored and supported remotely.

For any automation system where an HMI or a PLC are connected to the Internet, a firewall should be used. A firewall is a common feature found in most routers, and it greatly reduces the

You probably already use Tadiran batteries, **but just don't know it!**

PROVEN

40

YEAR

OPERATING

LIFE*

If you have a smart automatic water, gas, electricity, or heat meter in your home.

If you have an electronic toll collection transponder, tire inflation sensor, or emergency E-CALL system in your car.

If you have a GPS tracking device on your trailer, container, or cargo.

If you have wireless sensors, controls, or monitors in your factories and plants.

If you use electronics with real-time clock or memory back-up in your office.

If you have never heard of Tadiran Batteries, it is only because you have never had a problem with our products powering your products.

Take no chances. Take Tadiran batteries that last a lifetime.

TADIRAN BATTERIES

Tadiran Batteries
2001 Marcus Ave.
Suite 125E
Lake Success,
NY 11042
1-800-537-1368
516-621-4980

www.tadiranbat.com

* Tadiran $LiSOCl_2$ batteries feature the lowest annual self-discharge rate of any competitive battery, less than 1% per year, enabling these batteries to operate over 40 years depending on device operating usage. However, this is not an expressed or implied warranty, as each application differs in terms of annual energy consumption and/or operating environment.

risk of unauthorized access. The use of remote access accounts and passwords, available in both HMIs and PLCs, is an important method of asset protection as well as another layer of security, but adding a firewall provides a more secure connection.

Another layer of security is a VPN connection. The encryption used in a VPN ensures that data cannot be intercepted, and that only authorized users can access the HMI, PLC, or other networked devices. A VPN is part of a defense-in-depth strategy to greatly reduce the chances of malicious behavior and unauthorized connections to automation systems.

VPNs are offered in two main configurations, traditional and hosted. A traditional VPN, best administrated by an information technology (IT) professional, connects a local VPN router and creates a secure VPN tunnel through the Internet to a software client or second VPN router. Traditional VPNs basically make the remote devices on a network appear as local devices, securely, but much configuration may be needed at both the local and remote sites, depending on specific needs. Remote access to a manufacturing plant where large amounts of data must be exchanged is a common use and was the only method available until the cloud and related cloud servers were developed.

With the advent of the cloud, hosted VPN solutions became available. Hosted VPN makes setup, use, and maintenance easier due to simplified network configuration, while still providing a secure VPN connection. A hosted VPN solution starts with the connected devices, such as a PLC or HMI, connected to a VPN router at the plant. This router also connects to the company (business) network and, through a corporate firewall, to a VPN server in the cloud. VPN clients, such as smartphones or tablets, then connect to the VPN server to remotely access data (figure 3).

What simplifies the hosted VPN solution is that once a VPN router is purchased, it connects to a cloud-based VPN server managed by others with minimal IT support needed. After configuration, this cloud-based server automatically handles the connections to remote clients, including verification of connection requests, and it also ensures all data passing through the VPN tunnel is secure.

As a hosted service, there can be monthly costs, but some solutions provide free monthly bandwidth, which is normally enough for troubleshooting and programming needs. Premium hosted VPN solutions, provided under various monthly subscription plans, provide extended data monitoring capabilities.

Remote monitoring in action

When it comes to PLC remote access apps, especially if no VPN is used, many users choose to implement only data monitoring to minimize the security risk, with no remote control allowed. Some call this concept a data diode, because it only permits access via one-way communication from the PLC to app, just as a diode only permits the flow of electricity in one direction.

In a water treatment research project at a university, significant data was being stored in a PLC for use by both students and professors. However, with more than a dozen personnel having access to the data remotely via an FTP, as well as direct access via a USB connection, data integrity was in question. Data was being logged, but also read, duplicated, and sometimes erased. The ease of remote access was therefore contributing to the corruption

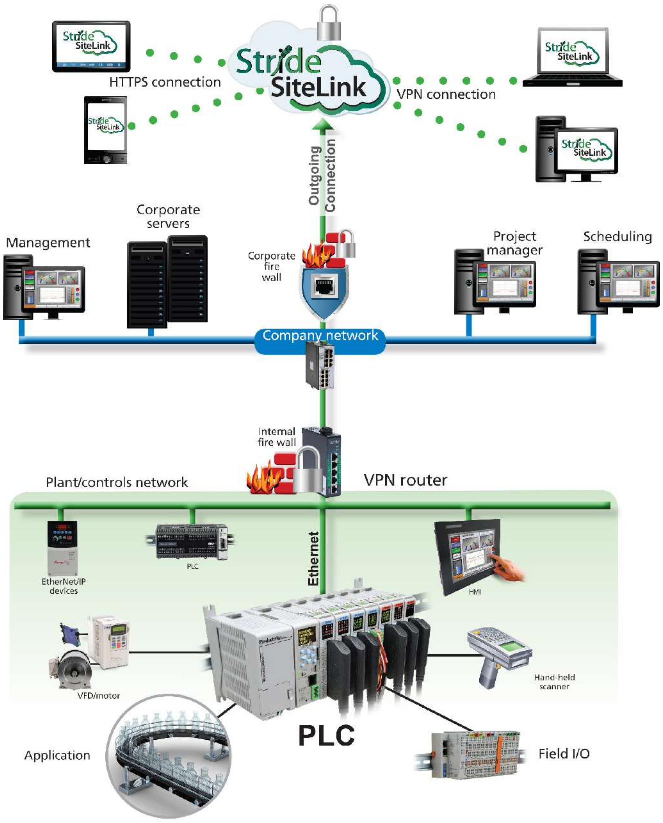


Figure 3. Hosted VPN Diagram: This diagram depicts a remote access solution implemented with the StrideLinx Secure hosted VPN.

Figure 4. HMI remote app: A dedicated HMI can provide local control as well as remote access at a reasonable cost.

and deletion of test data.

To both solve the problem and provide secure storage, a hosted VPN in the form of a secure, industrial VPN router and related services was implemented. Local data was still stored and used to quickly test and document process changes, but the hosted VPN stored large amounts of data securely in a database, including change control. VPN client applications had dashboards to easily trend the secure data and ensure access to accurate, raw data.

In another application, personnel at a large farm needed to monitor multiple pump stations remotely. They used HMIs for local operation, including troubleshooting and making changes to the pump control system and set points. Remote access to these HMIs was available via smartphones and tablets at any location with Internet access (figure 4).

Remote monitoring enabled quick notification and response to pump system problems, as well as to related process and equipment faults. The embedded HMI's remote access functionality provided low-cost and simple monitoring via smartphones and tablets.

For remote locations without Ethernet or Wi-Fi access, a cellular-hosted VPN router was installed. Adding a simple, secure client and mobile app, personnel could service, monitor, and troubleshoot the pump station remotely.

PLCs and HMIs can save data locally and format it as required, while providing some degree of security when this data is accessed by remote devices such as PCs, smartphones, and tablets. These types of IIoT-based solutions are common and work well in many instances, especially in applications where access is one way only, from the PLC or the HMI to the remote devices. For added security, often needed when control from remote devices to PLCs and HMIs is required, the use of firewalls and VPN access are a best practice. ■

ABOUT THE AUTHOR

Bill Dehner (bdehner@automationdirect.com) has spent the majority of his 14-year engineering career designing and installing industrial control systems for the oil and gas, power, and package handling industries. He has a BS in electrical engineering with an associate's in avionics from the USAF. He currently works for AutomationDirect as a technical marketing engineer.

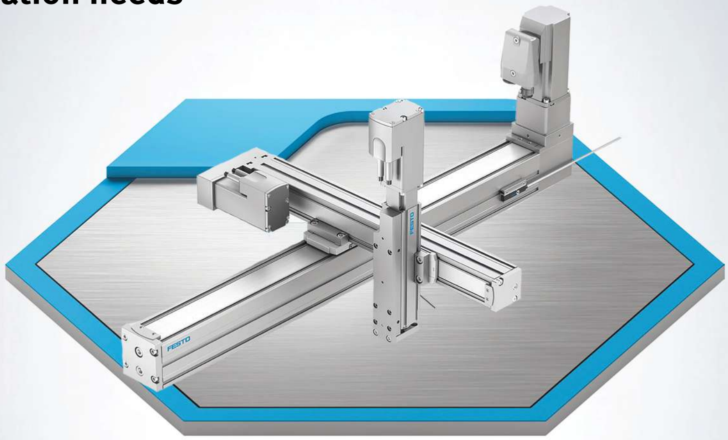
View the online version at www.isa.org/intech/20190203.

RESOURCES

"Remote access to automation system components"
www.isa.org/intech/20180205

"HMI remote-monitoring trends"
www.isa.org/intech/20160805

"New HMI alternatives improve operations and cut costs"
www.isa.org/new-hmi-alternatives-improve-operations-cut-costs



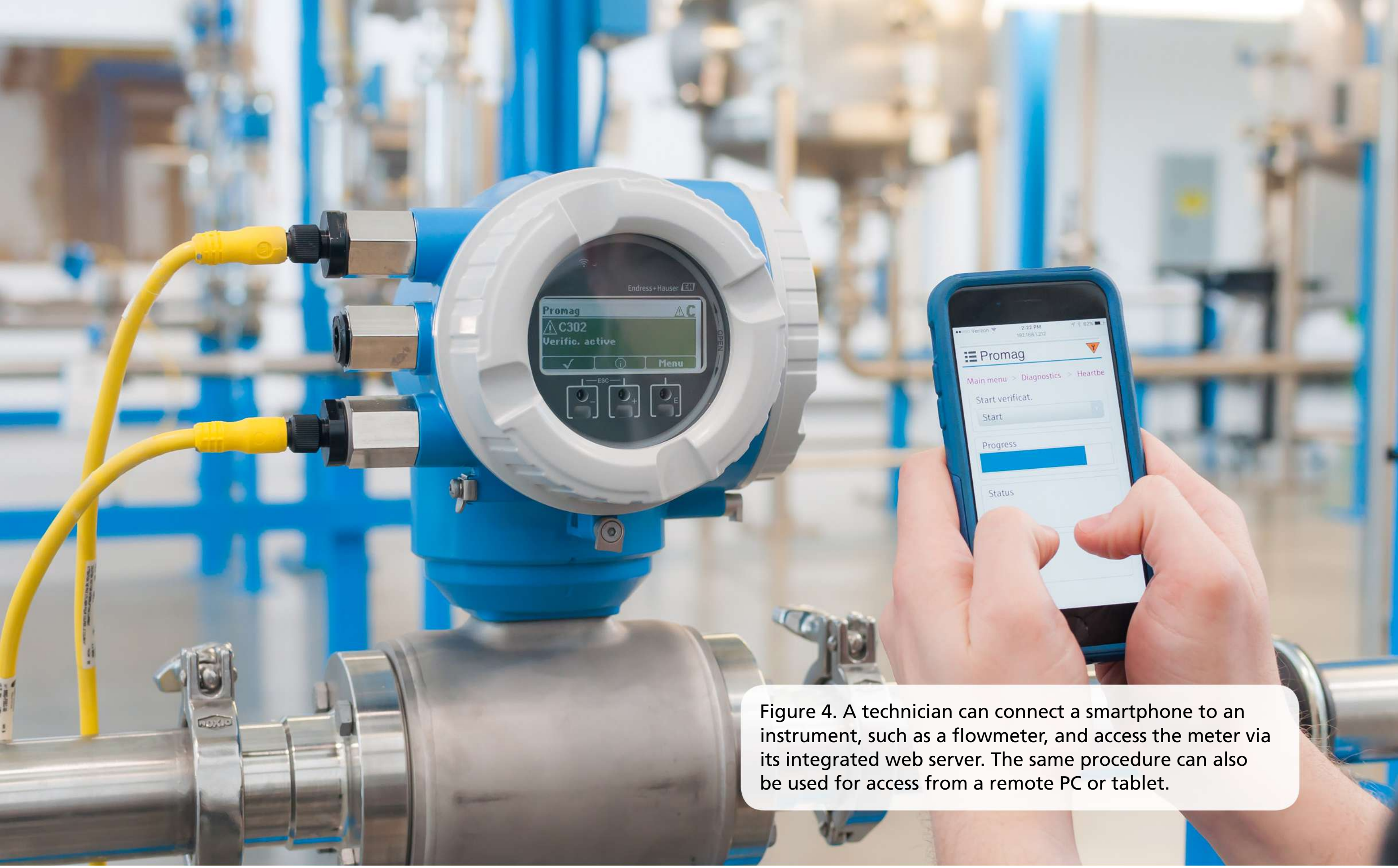


Figure 4. A technician can connect a smartphone to an instrument, such as a flowmeter, and access the meter via its integrated web server. The same procedure can also be used for access from a remote PC or tablet.

Smart transmitters enable smart sensors

By Steven J. Smith

Integrating digital technologies made instrument transmitters smart, with instrument sensors following in their wake

Process instruments consist of two main components: a sensor and a transmitter. The sensor is sometimes part of the instrument assembly, as with some pressure instruments, but is more often separate, as with analytical instruments, such as those used for pH measurement.

Before sensors could become smart, transmitters had to gain intelligence by adapting digital technologies. It would not have been practical, or sometimes even possible, to connect a smart digital sensor to a simple analog transmitter.

Industrial instrumentation has progressed significantly since the 1970s, when the vast majority of instruments simply had a single 4–20 or 0–20 mA (analog) output proportional to the process variable. Some sensors had the inherent ability to measure multiple process variables, but they required multiple analog outputs to access this additional information. With an analog transmitter with a single analog output, secondary variables remained stranded, as did data regarding the configuration or health of the instrument. The process variable was relegated to a dedicated analog signal transmitted from the instrument over two wires to an indicator or control system, with a multidrop configuration.

Working with these instruments required direct access to the device and manual adjustment by maintenance personnel. What was missing from this environment was any information about the instrument itself, or about secondary process variables, such as the temperature from a pH sensor.

HART emerges

In the early 1980s, instrument vendors realized the potential benefits of digital technology in instruments. There was a wealth of useful data contained in an instrument, including other measured process variables, device configuration, alarm limits, operating time, operating conditions, diagnostic information, and a broad range of device health data.

Obtaining this data from an instrument helps optimize the use of the device, and ultimately improves process performance, and HART communications emerged as one of the first ways to access this stranded data to make an instrument smart.

HART digital technology allowed communication with an analog instrument using a digital communication signal (Bell 202) transmitted over the same two wires as the analog output. This digital signal provided two-way communications between the instrument and a host without disrupting the output, allowing various pieces of data to be accessed. Using HART, personnel could talk to the instrument and perform configuration or diagnostics—all while it was making one or more real-time process measurements.

At the same time, various companies were making progress in the development of other digital technologies that would be transmitted over dedicated communication highways, each offering specific benefits. Various Fieldbus technologies emerged—including EtherNet/IP, Foundation Fieldbus, Profibus, and Modbus—and today these compose the majority of new applications for fieldbus communications.

In a similar fashion with respect to wireless digital communications, many technologies have been reduced to two clear leaders: ISA100 and WirelessHART.

Digital technology expands

The realization that instruments contained a vast amount of valuable data that could be bidirectionally communicated between instruments and control systems dramatically changed the way companies operated a process and managed assets—and it drove the rapid expansion of digital technology in the industrial environment. There are very few instruments today that are not smart, at least to some extent. From the 1980s to 2000, digital communication technologies emerged in industrial markets, and today are providing significant benefits.

FAST FORWARD

- Instrument transmitters gained intelligence through HART and other digital communications, then sensors became smart by integrating other types of digital technologies.
- Smart instruments provide a wealth of data to host systems, including secondary process variables, calibration information, and diagnostics.
- Smart sensors are the latest advancements in smart instruments, extending many smart transmitter benefits to the sensor level.

Around the same time, office computer networks were evolving. In 1989, the first prototype of the Internet was developed by Tim Berners-Lee and Robert Cailliau at CERN (the European Organization for Nuclear Research), eventually leading to the implementation of the World Wide Web. With networked computers and the Internet, there came Internet-enabled coordination and integration across the value chain, allowing suppliers to reach customers and business partners regardless of geography.

This Internet-enabled integration has also allowed enhanced access to process data from the point of measurement all the way to the business system level and beyond. Not only can one see process data critical to the operation of a process, but one can also access this key asset information.

As we move well into the second decade of this century, basic information technology has become more deeply embedded in industrial and consumer products, allowing them to become part of the Internet of Things (IoT). In one lifetime, process control migrated from pneumatics to electrical analog, and then to sophisticated digital communications extending out to the Internet. And most of today's smart instruments (figure 1) connect easily to digital communications systems, and in

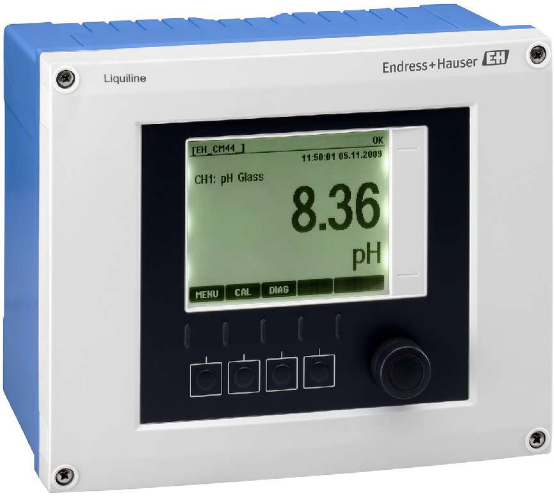
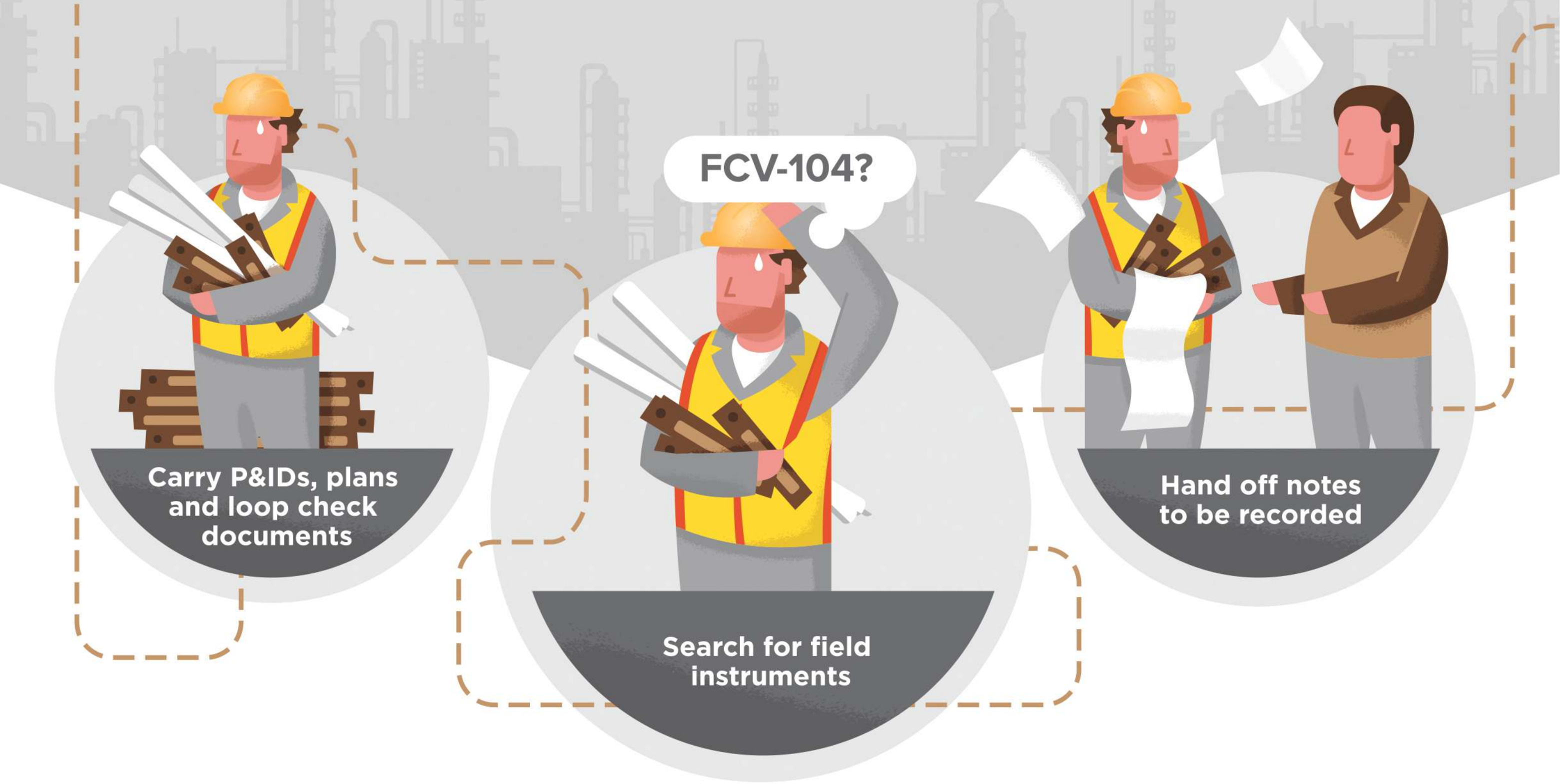


Figure 1. Information can now be communicated bidirectionally between instruments and control systems, dramatically improving the way companies operate a process and manage assets. The Liquiline transmitter is an example, communicating via EtherNet/IP, Modbus RS485, or TCP, PROFIBUS DP, and HART as well as a web server.

THE TYPICAL LOOP CHECK PROCESS MADE EASIER WITH eStart℠

The usual process for executing and tracking progress is costly and inefficient. The technician spends time identifying the location of field instruments, and the data from this effort is entered manually at least twice and by different individuals.



Carry P&IDs, plans and loop check documents

Search for field instruments

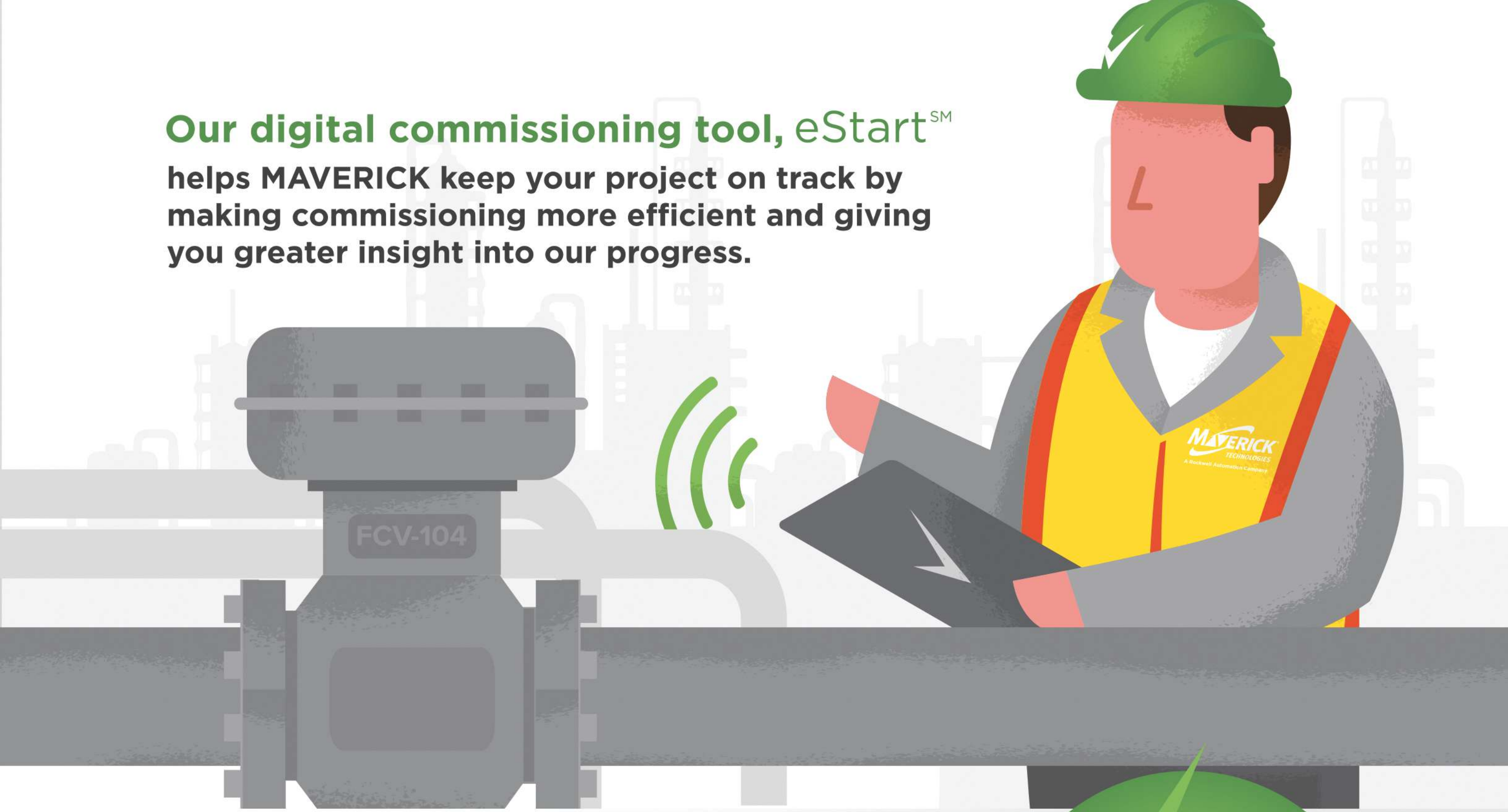
Hand off notes to be recorded

SURESTART
Safe. Smart. Systematic.

MAVERICK TECHNOLOGIES
A Rockwell Automation Company

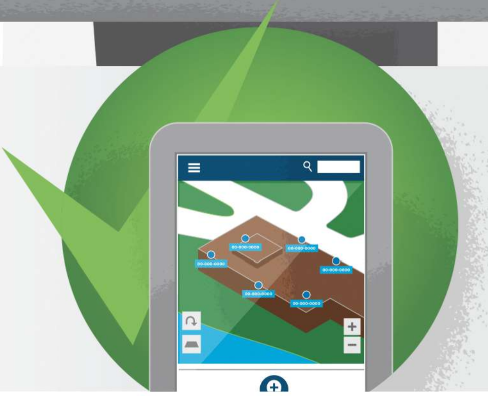
Our digital commissioning tool, eStart^{SM}

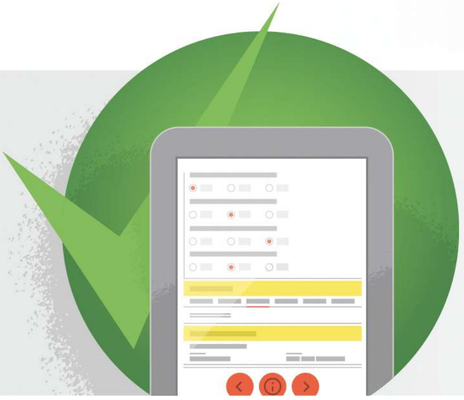
helps MAVERICK keep your project on track by making commissioning more efficient and giving you greater insight into our progress.



SAVES TIME

eStart's Near Me feature locates nearby instruments and identifies which stage of commissioning they're in. Digital folder creation not only reduces documentation time by up to 30%, but also keeps all electronic data at the technicians' fingertips.





REDUCES ERRORS

eStart automatically records the technician's name, date and time stamp, eliminating the need for double documentation, transcribing errors and piles of paperwork. Document once and done.

REAL-TIME TRACKING

Every time a step is completed, eStart automatically records the data, giving you real-time percent-complete updates so you'll always know where we are in the process and how close we are to completion.

mavtechglobal.com | 888.917.9109

REQUEST A
FREE DEMO
mavtechglobal.com/estart

some cases contain web servers and Ethernet ports for directly connecting to the Internet.

Smart instruments can acquire so much data, they need a high-speed digital interface to send it all. For example, some Coriolis flowmeters can simultaneously detect multiple measured process values, including mass flow, volume flow, density, concentration, and temperature. In addition to these measured variables, built-in electronics monitor instrument performance and report status and diagnostic values. Once smart instruments became widely accepted, mostly by adding the aforementioned features to the transmitter, smart sensors followed.

Smart sensors improve operations

Because digital information resides in the sensor and is communicated to the transmitter, health diagnostics can be performed, and the state of the sensor and transmitter health can be communicated to the host systems in real time. Real-time diagnostics and sensor-health data allow personnel to better manage a sensor. The need to clean and calibrate the device can be proactively managed, rather than reactively performed. In fact, some smart sensors can determine if they actually need to be cleaned and calibrated.

For example, calibration cycles for standard temperature sensors in critical service are every six to 12 months. This requires a technician to remove the sensor, take it to a lab for calibration, and then reinstall it. But one resistance temperature detector (RTD) sensor is able to determine if it needs a calibration when used in sterilize-in-place (SIP) processes (figure 2).

In SIP processes, steam at 121°C (250°F) is used to sterilize equipment. The sensor uses a reference material with a Curie point of 118°C (244°F). When the SIP process reaches 118°C, the reference sensor sends a signal. Simultaneously, the RTD measures the temperature. Comparison between these two values is used to determine if the temperature sensor needs calibration. If both sensors read a value close enough to 118°C, the RTD sensor is still in calibration.

Another example of real-time diagnostics and sensor-health data is a four-pole conductivity sensor (figure 3). This sensor uses four conductors to measure conductivity, and its four-pole design allows the sensor to operate over a broader range of measurement than two-pole conductive sensors. It uses digital sensor technology in the head of the sensor to digitize the measurement signal and provide a host of performance and diagnostic information.

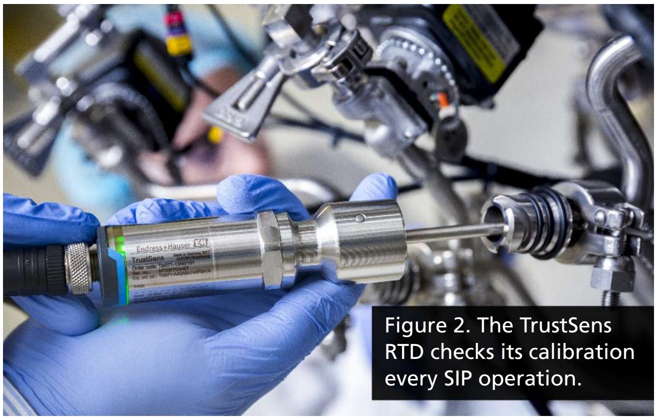


Figure 2. The TrustSens RTD checks its calibration every SIP operation.

One diagnostic function that makes this sensor particularly smart is electrode connection surveillance, which monitors the connection between the electrodes and the electronics. If there is a connection error, an error message is sent to the transmitter to notify the user of a connection problem within the sensor.

Accessing smart sensors

Maintenance personnel are stretched thin at many process plants and facilities, increasing the need for digital technologies, such as remote access to an instrument beyond the control system. By using digital communications, especially over an industrial Ethernet network, an instrument can become a "thing" in the Industrial Internet of Things.

Some more sophisticated digital transmitters have an embedded web server, permitting properly authorized access from any device connected to the Internet and capable of hosting a web browser, such as a smartphone (figure 4, page 24).

Two of the leading networks for local access to smart instruments from host systems are Modbus and EtherNet/IP. Common hosts are control systems and asset management systems.

Modbus is an open protocol, allowing any manufacturer to integrate the protocol into an instrument. Modbus is a serial, master-slave, protocol. The master requests information, and the slaves respond, with one master communicating with up to 247 slaves. Each slave in the network is assigned a unique ID. When a Modbus master requests information from a slave, the first data communicated is the slave ID.

Modbus can be difficult because one can use 16- or 32-bit signed and unsigned integers, ASCII strings; discrete on/off values, and 32-bit floating point numbers. To program a system for a device using Modbus communications, a significant amount of information is required about the slave device and its registers. A programmer has to obtain a Modbus map from an instrument manufacturer and carefully program the master to communicate properly with each slave device.

An improved version called Modbus TCP/IP is now available, whereby Modbus data can be framed in a TCP/IP packet, allowing the information to be more easily communicated over an Ethernet network.

EtherNet/IP is becoming one of the most widely used industrial protocols due to its ease of integration and operation. Like Modbus TCP/IP, EtherNet/IP data is transferred in a TCP/IP packet. Each device on an EtherNet/IP network presents its data to the network as a series of data values called attributes.

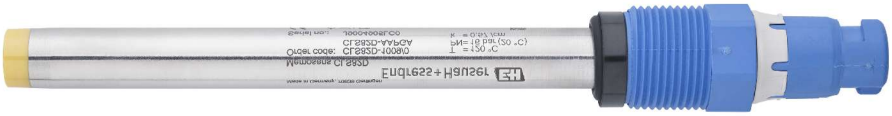


Figure 3. Technology is enabling real-time diagnostics and sensor-health data embedded in sensors. For example, the CLS82D four-pole conductivity sensor incorporates smart diagnostics.

Because EtherNet/IP uses the Common Industrial Protocol (CIP), consistent device access is possible with one configuration tool. Devices become "objects" on the network that are easy to integrate. Once on the network, an object has a profile that allows sensor data to be assigned within the profile, without the need for detailed programming information.

With digital sensors, digital transmitters, and control systems communicating, data can be easily and clearly communicated from the process to the host control system, and on up to the enterprise level. Data is no longer just the primary process variable, but also includes secondary process variables, sensor health, sensor performance characteristics, calibration information, and real-time diagnostics. All this information can be used to improve the process, optimize the performance of the instrument while extending its life, and maximize the productivity of maintenance personnel.

With the advent of the Internet, these digital devices and systems are being further transformed and becoming part of the IoT. This transformation will take us to places and bring capabilities we never imagined. Let's look at the journey of one industrial process measurement over the past 50 years to see how it has been completely transformed by digital technology: pH measurement.

Digital journey of one measurement

The fundamental measurement of pH has been used across a range of industrial processes for many years. It is a measurement of the hydrogen ion activity in a sample and represents the acidic or basic nature of a fluid. The pH range is defined from 0 to 14.

Determining a solution's pH began as a lab-based measurement. A sample was brought to a lab, and a benchtop pH system was used to measure the sample. The measuring system did not actually measure pH, but calculated pH based on a measured mV potential signal produced by the pH sensor. To do this, a benchtop pH sensor has two electrodes (a measurement electrode and a reference electrode, enclosed in separate glass cells) and, due to the effects of temperature on the measurement, a temperature sensor is also required.

Historically, with lab-based systems, the measuring electrode, reference electrode, and temperature sensor were three separate electrodes that were immersed in the sample while connected to electronics that measured the low-level mV signal and converted this value to pH. This was truly an analog system and an off-line measurement that required a significant amount of operator effort, with a considerable time lag between when a sample was collected and results were reported.

One of the first major changes in the measurement of pH was to integrate the three separate electrodes into one device, which resulted in a "combination" electrode. The sensor was still an analog device with hardwired connections to the transmitter and had all the inherent problems associated with a hardwired, low-level analog signal. The next significant improvement in pH measurement was the introduction of digital technology to the sensor, enabled by continuing advancements in miniaturization (figure 5). And, as with all smart sensors, it allows new pH sensors to provide more data, and to operate more reliably.

At the transmitter end of a pH instrument, the data communicated by a digital smart sensor can be read and sent out to a control or asset management host system, also using digital communications protocols. With the abundance of data residing in the sensor, and the ability to digitally communicate this data to a digital transmitter and beyond, users now have the information to better operate the process and manage the asset.

Although this example pertains to pH measurements, much of the discussion also applies to other process variables.

Digital advancing

Because of the technology advances in the past half a century, transmission from an instrument has evolved from just the primary process variable to a wealth of information accessible up to the enterprise level. In the future, digital technology will continue to provide more information from instruments, with access from anywhere in the world.

A pH measurement is no longer just the pH value, it also includes the temperature, quality of the calibration, number of calibrations, overall operating time, operating time over critical process conditions, and much more. Tools are available to turn this data into actionable information, with virtually no limitations when it comes to improving operations and efficiency. ■

Figure 5. Smart sensors can store measuring and operating data, including serial number, calibration date, number of calibrations, offsets, pH application range, number of calibrations, and hours of operation under extreme conditions.

ABOUT THE AUTHOR

Steven J. Smith (steve.smith@us.endress.com) is the senior product marketing manager – analytical for Endress+Hauser USA, responsible for technology application, business development, and product management of analytical products. He has a BS from the University of Wisconsin and an MBA from the University of Colorado. Smith has spent the past 30 years working in process instrumentation and control with Fortune 500 companies.

View the online version at www.isa.org/intech/20190204.

RESOURCES

"HART makes troubleshooting easy"
www.isa.org/automation-basics-hart-makes-troubleshooting-easy

"The Smart Evolution"
www.isa.org/the-smart-evolution

"Industry 4.0 for process"
www.isa.org/intech/20170601

ISA-18.2 technical reports for special applications

FAST FORWARD

- ISA18.2-TR4 provides guidance on how and when to use enhanced or advanced alarm methods.
- ISA18.2-TR6 has numerous examples for designing alarms for batch and discrete systems.
- ISA18.2-TR7 provides guidance for both vendors and users of packaged process equipment.

Applying alarm management

By Joseph Alford, Bridget Fitzpatrick, Doug Metzger, and Graham Nasby

As part of their support and guidance for using the standards they develop, ISA standards committees prepare technical reports that help automation professionals on a wide variety of topics. This article highlights three alarm management technical reports that have been published: ISA-TR18.2.4, *Advanced and Enhanced Alarm Methods*, ISA-TR18.2.6, *Alarm Design for Batch and Discrete Processes*, and ISA-TR18.2.7, *Applying Alarm Management when Utilizing Packaged Systems*.

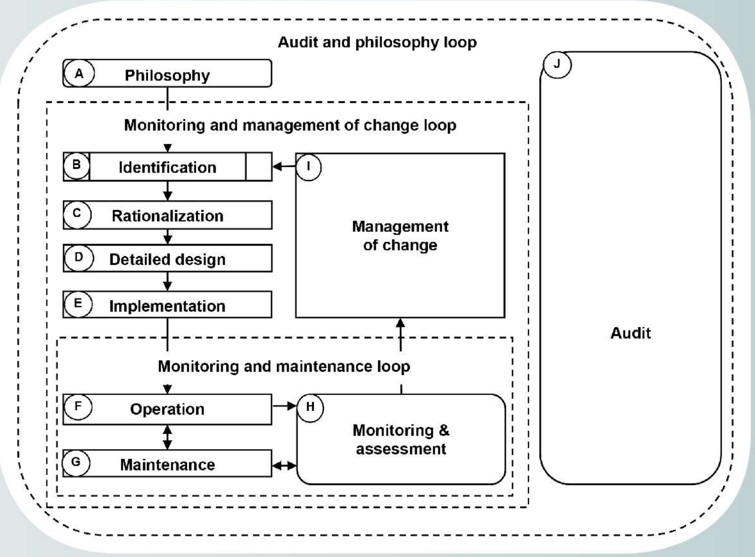


Figure 1. Alarm management life cycle (figure 2 from ISA18.2)

The ISA-18.2 standard

In 2009, the original version of ANSI/ISA-18.2, *Management of Alarm Systems for the Process Industries*, was published. It was further developed with ISA18 leadership into the IEC 62682:2014 international standard, which in turn was refined into the current ANSI/ISA-18.2-2016 standard.

Known as ISA-18.2, the alarm management standard is organized around the concept of the alarm management life cycle (figure 1).

As with most published consensus standards, the content of ISA-18.2 focuses on "requirements." It does not include guidance on how to satisfy those requirements. This is where the ISA-18.2 technical reports (TRs) are helpful. The TRs give guidance on how to best implement effective alarm systems using ISA-18.2. They also provide background information and examples that explain the purposes and rationale behind the requirements outlined in ISA-18.2.

The ISA-18.2 technical reports are as follows:

- TR1: Alarm Philosophy
- TR2: Alarm Identification and Rationalization
- TR3: Basic Alarm Design
- TR4: Enhanced and Advanced Alarm Methods
- TR5: Alarm System Monitoring, Assessment, and Audit
- TR6: Alarm Systems for Batch and Discrete Processes
- TR7: Alarm Management when Utilizing Packaged Systems

An eighth technical report, TR8: Alerts, Events, Prompts, and Other Notifications, is currently under development. Four of the technical reports, TR1, TR2, TR3, and TR5, are focused around specific ISA-18.2 life-cycle work processes. The other three, TR4, TR6, and TR7, cover how to apply alarm management in a number of special applications, and are the focus of this article.

TR4: Enhanced/advanced alarms

TR4 gives guidance on how and when to use enhanced and advanced alarm methods. In ISA-18.2, alarms are broken into two categories: basic alarms and enhanced/advanced alarms. Basic alarms typically consist of a set point or a trigger value, plus on-delay, off-delay, and/or deadband, but have no additional logic associated with them. The term "enhanced/advanced alarm" is used for alarms that use special features or programming. Although both basic and enhanced/advanced alarms are discussed in ISA-18.2, enhanced/advanced alarming methods are not required in all cases, and are discussed in less detail in the standard.

In general, application of the basic alarm practices in ISA-18.2 (as well as in TRs 1, 2, 3, and 5) will improve the validity and consistency of alarm design, avoid inappropriate alarms, and establish long-term viability for most alarm systems. However, the dynamic nature of some processes and related process complexities can lead to the alarm system objectives being only partially met using basic alarm design approaches. For example:

- Alarm floods, though reduced, may still occur. Individual process events can cause multiple alarms at roughly the same time for a single underlying process event.
- A process may have other operating states in addition to the normal steady state, or it may have multiple normal operating states. This means that alarms have to be designed to accommodate multiple operating states, each of which may need different alarms and/or alarm set points.
- Basic alarm capabilities may not deliver the alarm to the person who needs to respond to it on the operating team. Enhanced methods may be needed to route an alarm to the appropriate person.

The difficulty with using enhanced and advanced alarm methods is that they do add complexity to the alarm system and can be time consuming (and consequently costly) to implement. Thus, enhanced/advanced alarms should be reserved for only those situations that truly need them. It is important to first reduce the scope of any enhanced/advanced alarming effort by using basic rationalization and basic alarm design approaches as much as possible.

TR4 provides guidance and examples on the selection, design, and implementation of enhanced/advanced alarm methods. Specific situations in a number of areas are discussed, along with solution methods and examples. Some of the topics covered by TR4 include:

Dynamic alarm attributes: Various examples are provided for where alarm attributes are automatically and dynamically changed by the control system based on the current operating state of a process. In fact, both the advanced/enhanced alarming TR4 and the batch-process oriented TR6 have multiple examples of dynamic alarm attributes.

Information linking: Information embedded in the alarm itself (e.g., tag, description, and set point) may not always be enough to help guide the operator's response. Often the appropriate guidance has already been identified during the alarm rationalization stage but not built into the primary alarm presentation. Information linking within the alarm system can be used to present additional information to an operator when an alarm is triggered.

State-based alarming: A number of methods are discussed for handling alarms during changing the plant state and operating conditions in order to minimize alarm floods or inappropriate alarms. This can occur for planned operating states, such as startup, shutdown, batch phases, and different feedstocks; or it can occur due to unplanned events, such as a compressor trip. Techniques discussed include: first-out alarming, designed suppression, state-driven alarm attribute changes, and dynamically calculated alarm set points. Figure 2 shows an example of calculated alarm set points, which is touched on in TR4 and

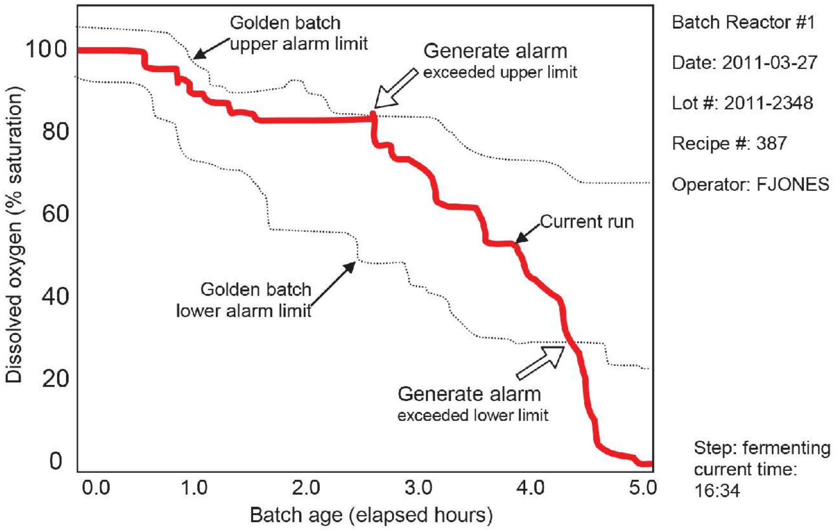


Figure 2. An example of advanced alarming for a batch process (figure 15 from TR6)

discussed more extensively in TR6.

Dynamic cause analysis and guidance: State-based alarming can often provide appropriate alarms at the right times and help avoid nuisance alarms. But there are occasions when the customary level of operator guidance (provided by typical human-machine interface systems) can be inadequate. TR4 provides an overview of how an extra layer of logic can be added to the alarm system to dynamically analyze abnormal situations and dynamically provide recommendations to the operator on how best to respond.

Alarm routing: Sending alarms to the right person can sometimes be difficult in large or complex plants. Simply sending alarms to a central control room is not always effective, as operators could be distributed through the plant, roam on foot, or even be located offsite. TR4 provides guidance and the pros and cons of several alarm routing techniques.

Use of alerts: ISA-18.2 defines alerts as notifications that share some of the characteristics of alarms but do not meet all of the criteria of alarms (e.g., may not represent abnormal situations or may not require a timely response). TR4 provides guidance on nonalarm notifications, as it is important to understand their relation to, and distinction from, alarms.

Application to alarm management life-cycle work processes: TR4 also discusses how the use of enhanced and advanced alarming methods fits within the various alarm management life-cycle work processes. If used, enhanced/advanced alarm methods have to be integrated throughout the alarm management life cycle—including testing/training, management of change, monitoring, and audit—to preserve the investment in the alarm system and to assure continued alarm system integrity.

TR6: Batch and discrete processes

Batch processes and discrete manufacturing present several unique challenges when it comes to implementing effective alarms. TR6 provides guidance for how to design and implement effective alarms for batch and discrete processes.

The special recommended alarm practices for many batch and discrete processes become apparent when understanding how most batch processes differ from more traditional continuous processes. Most batch processes consist of a sequence of time-varying steps, often representing a mixture of manual and automated operations. The existence of multiple time-varying steps (and phases), coupled with the need to start up, shut down, and occasionally to stop, pause, hold, and sometimes even abort the process, requires a different approach for alarming. Batch processes often consist of several different unit operations, each with its own equipment. The use of packaged equipment with batch processes is also very common.

Batch processes often have special requirements for logging and recordkeeping. In addition to typical process logging, alarm records often need additional details (e.g., lot number) to facilitate alarm record sorting, undertake alarm analysis, and prepare batch lot reports.

When rationalizing and designing alarms for a batch process, alarm settings often need to be dynamic, so the control system can automatically change alarm attributes and which alarms are active, based on the current step of the batch process. Dynamically changing alarm settings can be done based on the current step, a recipe, or even time elapsed into a batch step. An example based on the system state/step is shown in table 1.

System state	Temperature controllers	TIT1 low-temp alarm	TIT1 high-temp alarm
OFFLINE	Manual mode	suppressed by design	suppressed by design
Initial tank warm-up (System startup)	Ramp-up to 70°C	suppressed by design	suppressed by design
Normal at 70°C	Hold at 70°C	TIT1 < 65°C	TIT1 > 75°C
Normal-to-sani Temperature ramp-up	Ramp-up 70 to 85°C	TIT1 < 65°C	suppressed by design
Sani at 85°C	Hold at 85°C	TIT1 < 80°C	TIT1 > 95°C
Sani-to-normal Temperature ramp down	Ramp-down 85 to 70°C	TIT1 < 65°C	suppressed by design

Table 1. Example batch system that uses state-based alarming (Hot purified water system with nightly hot sanitization cycle)

Alarm routing is commonly used in batch processes, since process operators may be out on the plant floor and not in the central control room. For complex processes, a technical services group—which may not even be located in the same building—may also need to receive alarms.

TR6 also discusses how the ISA-88 batch control standards can be helpful when implementing alarms in batch-based systems. ISA-88 has both a procedural (recipe-based) model and an equipment model, which together, provide numerous software objects to which alarms can be attached and dynamically modified. In particular, TR6 provides several examples of how alarms can be implemented in the equipment model, and then how the procedural model can be used to dynamically change alarm attributes.

How alarms are tagged, logged, and presented to an operator presents some interesting challenges with respect to batch processes. In many industries, there is a need to also associate lot numbers, time since start of batch, recipe name, and other attributes with alarm records. This can be challenging to do in some control systems. Including automated linking support in the alarm system, such as attaching such data directly to the alarm records when they are created, can greatly reduce the effort to find, for example, all "product quality" classified alarms for a particular process step in a particular batch. Also, special alarm classes may need to be configured so alarms can be sorted and/or grouped in various ways as needed.

Alarm management nuances exist for discrete processes as well. For example, it is usually not practical to alarm every defective widget when hundreds or thousands of widgets per hour are being manufactured. Therefore, for discrete processes, alarms are often generated as the result of a statistical analysis of large numbers of samples (e.g., viewing thousands of widgets manufactured on an assembly line, or tens of thousands of tablets or capsules on a pharmaceutical finishing line). So alarms are often generated based on a statistical algorithm (e.g., statistical deviation within a lot) rather than a continuous analog signal (e.g., a temperature measurement exceeding its deadband). Furthermore, the generation of a "process measurement value" (PV) for use in a discrete process alarm algorithm can, itself, be challenging, as sensors for such information can include sophisticated vision systems, robotics, and RFID chips, with part of the challenge being to export the appropriate information from such sophisticated microprocessor-based sensor systems to a plant's central alarm system. The need for any such specialized alarm algorithms should be identified in a plant's alarm philosophy, with details determined during alarm identification and rationalization life-cycle activities.

TR7: Alarm management when utilizing packaged systems

Integrating packaged systems into centralized plant automation systems is often one of the most challenging tasks faced by automation professionals. From a process design point of view, packaged systems (PS) play an important role, as they are specialized pieces of process equipment with customized control systems that are specific to their function. However, packaged systems—due to their custom nature—are often the source of many headaches when it comes to integrating them into a plant's basic process control system and into a plantwide alarm system. It is not uncommon for a packaged system to use a completely different control technology platform than the rest of the plant, often causing a multitude of system integration challenges.

Common examples of plant equipment in the process industries that use packaged systems include: chillers, compressors, turbines, furnaces, batch reactors, packaging equipment, UV disinfection systems, and sump pump controllers, just to name a few. Though each is different in its function, they share a common feature of typically using individual control systems that are different from the centralized system (e.g., distributed control system) in the plant where they are installed.

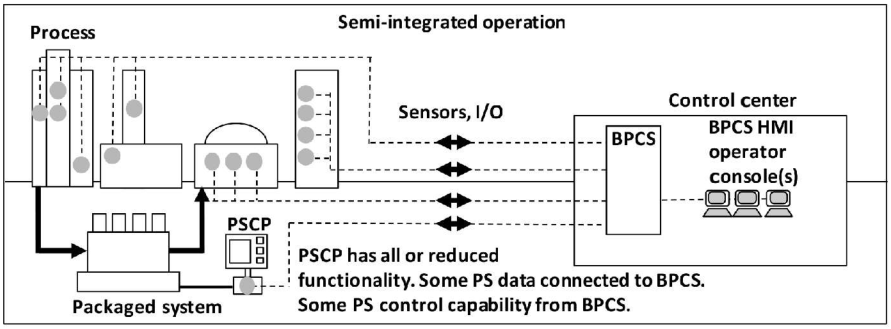

Process
Semi-integrated operation
Sensors, I/O
Control center
BPCS
BPCS HMI operator console(s)
PSCP
PSCP has all or reduced functionality. Some PS data connected to BPCS. Some PS control capability from BPCS.
Packaged system

Figure 3. Example of how a packaged system can be integrated into a plantwide control system

TR7 begins by defining what packaged systems are and the various pros and cons of packaged systems from a system integration perspective. The TR also establishes a set of standard terminology that can be used to clearly define the various forms of packaged system control systems. For example, the location, role, and placement of packaged system control panels, which typically include alarm information, can be implemented in many ways, and the pros and cons of various commonly used configurations are discussed.

Commonly used techniques to interface PSs into plantwide alarm systems are covered, including best practices, and, again, the pros and cons of various approaches. Frequently encountered challenges with interfacing PSs are also covered, with the goal of helping the reader avoid many of the common issues when it comes to integrating packaged systems within a plant's larger overall control system.

There are a wide variety of methods that can be used to interface a PS with a plant's alarm system (and a plant's overall control system). There are also several ways to apply the ISA-18.2 alarm management life cycle to packaged systems. TR7 provides a framework of how to effectively cover packaged system alarms within a facility's alarm philosophy. The TR then discusses the unique details of packaged systems one by one, and how this in turn relates back to the alarm philosophy, complete with examples.

The text of TR7 includes a discussion of how using packaged systems impacts each of the work processes of the ISA-18.2 alarm management life cycle. The design-oriented alarm management work processes of identification, rationalization, detailed design, and implementation are covered first. The TR has a step-by-step method of how to develop packaged systems alarms, which includes leveraging the knowledge and expertise of the packaged system vendor, as well as the needs of the end user. Specific emphasis is put on resolving alarm management issues during the design process, rather than waiting until fabrication or commissioning of packaged systems.

The TR then covers some of the more operations-oriented aspects of alarm management, namely operation, maintenance, and alarm system performance monitoring and assessment. A strong emphasis is put on how changes to the alarm system with respect to packaged systems and packaged system interfacing must be made carefully as part of a management of change process. Making changes with packaged systems can sometimes be difficult because of warranty and commercial considerations, so the TR gives advice for project leaders about talking to vendors and end users about the benefits of applying alarm management to packaged systems. Lastly, the TR7 technical report provides guidance on how to audit alarm management processes when packaged systems are involved.

Helpful guidance

Every process facility is different, so there is no "one size fits all" approach to doing alarm system design. For plants that make use of complex processes, batch processes, discrete manufacturing, or packaged equipment, the ISA-18.2 technical reports provide helpful guidance on how to best implement and maintain effective alarms.

Further reading

The ISA-18.2 alarm management standard and supporting technical reports are available at www.isa.org/standards. ISA members may view the standard and TRs online at no cost as part of their ISA membership benefits. ■

ABOUT THE AUTHORS

All four authors served as cochairs of ISA-18.2 technical report working groups for TR4, TR6, and TR7, and are voting members of the ISA18 alarm management committee.

Joseph Alford (jmalford5@earthlink.net) is an independent automation consultant. He previously spent 35 years with Eli Lilly in automating their life science processes. He is a Fellow of both ISA and AIChE and a member of the Process Automation Hall of Fame.

Bridget Fitzpatrick (bridget.fitzpatrick@woodgroup.com) is the managing director of the ISA18 committee. She is the process automation authority for Wood in Houston, Texas. Fitzpatrick is also an ISA Fellow.

Doug Metzger (doug.metzger@cox.net) is principal consultant with DPM Consulting. He previously held the role of Engineering Fellow at Honeywell Process Solutions, where he worked for 35 years.

Graham Nasby (graham.nasby@guelph.ca) is the water SCADA & security specialist with City of Guelph Water Services. He is also the cochair of the ISA112 SCADA Systems standards committee.

View the online version at www.isa.org/intech/20190205.

RESOURCES

ISA-18.2 Alarm Management standard
www.isa.org/isa18-2-alarm-management

ISA-TR18.2.4-2012, *Enhanced and Advanced Alarm Methods*
www.isa.org/isa-tr1824-2012-enhanced-and-advanced-alarm-methods

ISA-TR18.2.6-2012, *Alarm Systems for Batch and Discrete Processes*
www.isa.org/isa-tr1826-2012-alarm-systems-for-batch-and-discrete-processes

ISA-TR18.2.7-2017, *Alarm Management when Utilizing Packaged Systems*
www.isa.org/isa-tr1827-2017-alarm-management-when-utilizing-packaged-systems

ISA Alarm Management standards committee
www.isa.org/isa18

Online water quality and control system

Effective method to monitor and control water quality to blend groundwater in small quantities with the surface-water supplies and conform to all regulatory drinking water standards

By Diep Nguyen, PE, Jeff Gilman, PE, Todd Reynolds, PE, and A.J. Cottengim

FAST FORWARD

- An online water quality and control system is an effective way to monitor and control water quality.
- SCADA system reliability is key to online data collection and calculations.
- The online water quality and control system conforms to EPA water quality surveillance and response system guidelines.

The San Francisco Public Utilities Commission (SFPUC), the municipal water supply agency for the city and county of San Francisco, Calif., began mixing groundwater from a local aquifer with the city's customary surface-water supply sources in April 2017. San Francisco had not used groundwater as a drinking water supply for more than 90 years. The planning, engineering design, and construction for this renewed groundwater use was accomplished under the San Francisco Groundwater Supply Project (SFGW Project), a part of the agency's capital program to diversify the city's drinking water supply sources and increase their reliability.

Due to differences in water quality between the groundwater and surface water, the SFGW Project opted to blend groundwater in small quantities with the surface-water supplies in two city reservoirs. This blending or mixing allows the city to continue to surpass all regulatory drinking water standards, as well as to ensure that changes in taste or odor are not noticed. A specialized project team developed and executed an online monitoring and control system to satisfy the project's water quality requirements. The team includes SFPUC project management staff. The team members for the water quality control system included personnel from DTN Engineers, Kennedy/Jenks Consultants, and Tesco Controls.

Background

SFPUC is a purveyor to water retail customers in the city and county of San Francisco, as well as to 26 wholesale customers that serve Alameda, San Mateo, and Santa Clara counties in the greater Bay Area. From the mid-1930s until recently, SFPUC's municipal supply came from the Hetch Hetchy Regional Water System, a system that combines the surface-water resources of the Hetch Hetchy Reservoir in the Sierra Nevada mountain range with five reservoirs in the Bay Area. On average, 85 percent of SFPUC's water has been supplied by the Hetch Hetchy Reservoir, and the five Bay Area reservoirs have provided the remaining 15 percent.

Beginning in the mid-2000s, SFPUC embarked on the Water System Improvement Program (WSIP), a $4.8-billion-dollar, multiyear capital program to upgrade SFPUC's regional and local water systems. WSIP's primary goals included:

- seismically strengthening the regional water system by rebuilding existing facilities in vulnerable areas, such as fault zones and beneath San Francisco Bay
- maintaining the high quality of the drinking water supply by rebuilding water treatment plants and constructing new water treatment facilities
- increasing the reliability of San Francisco's water supplies by adding water wells under two groundwater projects

These two groundwater projects are the SFGW Project and the Regional Groundwater Storage and Recovery Project (GSR Project). The SFGW Project is located wholly in San Francisco, while the GSR Project is located in northern San Mateo County, south of San Francisco. Both projects tap groundwater from the Westside Basin aquifer. The SFGW Project is designed to supplement the city's drinking water at all times and is the focus of this article. The GSR Project will provide groundwater during droughts or other emergencies to both wholesale customers in the project area and to San Francisco. With groundwater supplies, SFPUC's customers are less vulnerable to disrupted services, whether from a major earthquake, drought, or other future unknowns.

The SFGW Project consists of six groundwater well facilities, each consisting of a well and pump station, and five miles of a new groundwater transmission pipeline constructed for the project (figure 2). Five of the wells supply groundwater directly to the Sunset Reservoir via the new groundwater pipeline, where it is mixed with the Hetch Hetchy Regional Water System supply. The sixth well, located near Lake Merced, connects to the SFPUC's Lake Merced Pump Station, where the groundwater is mixed and distributed to both the Sunset and Sutro Reservoirs. In addition to mixing with the surface-water supplies, the groundwater is treated using chlorination and pH adjustment.

Four of the well facilities (phase I in figure 1) are complete and currently pumping groundwater to the Sunset and Sutro Reservoirs. The remaining two well facilities (phase II in figure 1) will begin pumping to the Sunset Reservoir by 2021. The average groundwater production will increase incrementally, with a goal of 1 million gallons per day (mgd) (1,120 acre-feet per year) during the first year and 4 mgd (4,480 acre-feet per year) when all six wells are operating. The full 4-mgd production rate represents a blend of approximately 13 percent groundwater in the Sunset Reservoir.

The quality of groundwater from the Westside Basin aquifer is different from the surface-water supplies from the Hetch Hetchy Regional Water System. The resulting groundwater-surface water blend, therefore, is also different from what customarily has been served to SFPUC customers. The key water quality variations are in general mineral content, pH, nitrate, hexavalent chromium, and manganese.

- The general mineral content of the groundwater—primarily total dissolved solids, hardness, and alkalinity—is higher than San Francisco's main supply from the Hetch Hetchy Reservoir.
- The pH of groundwater from individual wells ranges from 7.6 to 8.0 (slightly alkaline). This range is lower than the pH of SFPUC's treated surface-water supply, which is maintained at a range of 8.8 to 9.4 for optimal corrosion control. (This is required by the drinking water Lead and Copper Rule, which is enforced by the State Water Resources Control Board.)
- Nitrate and hexavalent chromium concentrations in the groundwater are higher than in the surface-water supply. Nitrate has a health-based drinking water standard (primary maximum contaminant level [MCL]). In addition, the state of California is in the process of adopting a primary MCL for hexavalent chromium, expected in 2019.
- Manganese is often found in groundwater throughout the San Francisco Bay Area at concentrations higher than the aesthetically

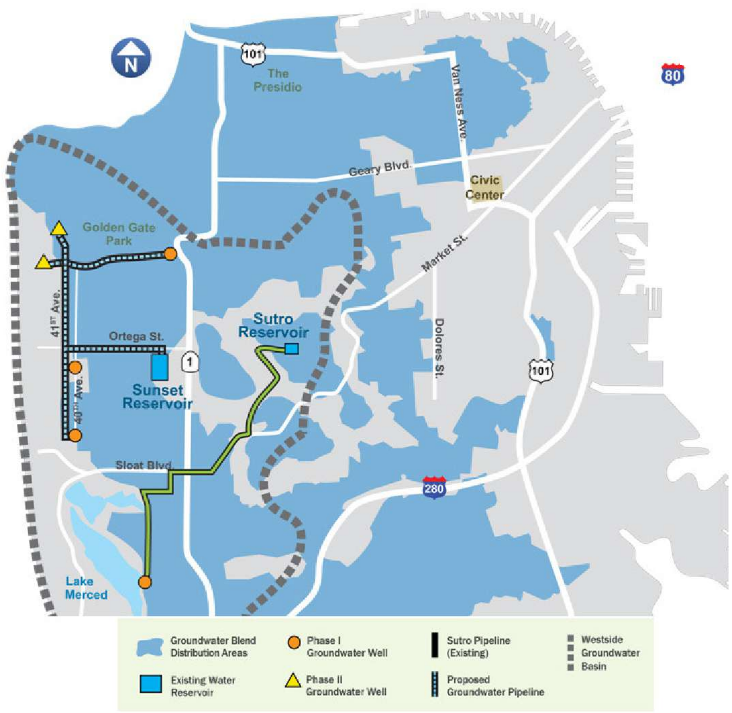


Figure 1. SFGW project elements

based drinking water standard (secondary MCL). It has not, however, consistently been found above the secondary MCL in the SFGW Project wells.

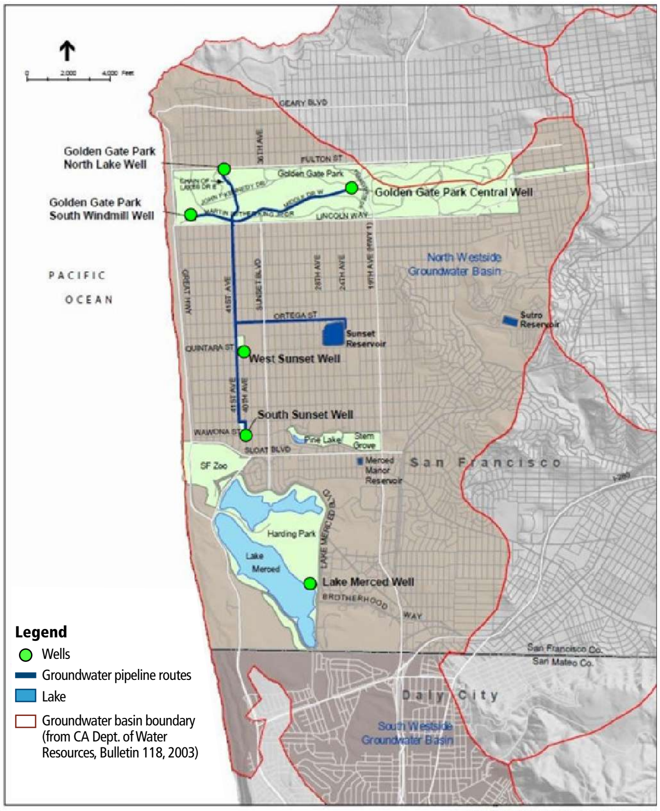
As a result of the water quality differences described above, the SFGW project team developed an online water quality and control system to carefully monitor and manage the chemical treatment processes and mixing of groundwater and surface water. The major functions of this online water quality and control system are:

- monitoring individual well production rates, mechanical and electrical systems in the well facilities, and chemical treatment processes
- calculating the blended water quality in real time
- controlling the well production to ensure that the blended water quality of key regulated parameters (nitrate, hexavalent chromium, and manganese) continues to surpass the state drinking water standards
- collecting and archiving data needed for monthly regulatory reporting, to demonstrate compliance with drinking water standards

Distribution of the groundwater blend is based on the elevations and pressure zones of the Sunset and Sutro Reservoirs systems.

Control system hardware and software

The control system for the online water quality control is a subset of the city of San Francisco's existing supervisory control and data acquisition (SCADA) system. This SCADA system is a network of computers and programmable logic controllers (PLCs) using the AT&T virtual private network (AVPN) as the main backbone (figure 3). The main controller (poll master) of the online system is at the Lake Merced facility and consists of a hot backup PLC communicating with the other main controller and remote PLCs located at each well or treatment facility. Essential signals, such as water flows, chemical flows, and water qualities (e.g., pH, chlorine), are collected at these facilities and sent to the main controller for control decisions.



Source: SFPUC Final Environmental Impact Report (2013)

San Francisco Groundwater Supply Project

Figure 2. SFGW project wells and reservoirs

The SCADA system uses Wonderware as the human-machine interface (HMI) software. The PLC uses Unity Functional Blocks with detailed annotation for each logic algorithm.

SCADA system data collection

Field instruments, such as flowmeters and water quality analyzers, continuously feed online data to the local PLC, which also monitors and controls motorized equipment such as pumps. Some of the most critical signals for the Online Water Quality Monitoring and Control System are the water flow rate signals. A flowmeter in the pipeline senses flow and generates an electrical signal back to the PLC. The PLC is then calibrated to determine what the current water flow is based on the strength of the signal.

Safety measures have been taken in the PLC to ensure that the information received from the equipment is correct. This is true for both discrete signals, such as pump run and pump fail, and analog signals, such as flows and water qualities (e.g., pH, conductivity, chlorine residuals).

Human interfacing

There are two different methods for the operators to interface with the SCADA system. First, a local operator interface (LOI) is a touchscreen associated with the site (figure 4). This screen shows a graphical representation of the equipment at the site that changes as physical inputs and outputs change. This screen also provides a location for operators to change set points and manually measured values. Any process signal associated with the online system is displayed on this LOI screen.

The second method of interaction occurs through a SCADA system with any online data displayed simultaneously on computers located at any of the four operation control centers (OCCs) on the respective computer's screen. This is the "mission control" of the water system. SCADA allows for all of the same interaction and graphical elements as the LOI, but over a much larger scale. SCADA's computing power allows it to take historical records of data for future review.

Peer-to-peer communication

One of the more difficult elements of a PLC network is maintaining proper communication between each PLC. For this reason, the Online Water Quality Monitoring and Control System uses an industry standard called a poll master. The poll master acts as a leader and initiates a conversation with each of the other PLCs. The poll master becomes a central brain having access to all information in the system. Any necessary information from one PLC is passed to the others through the poll master. If a communication failure is detected between two PLCs, alarms are immediately generated. A well site that loses communication with the poll master enters a fail-safe mode and shuts down; simultaneously an alarm is generated and sent to SCADA to inform operators, so that the corrective action can be taken.

Action by PLCs

Each individual PLC measures the water flow leaving its station. Using the flow rate (usually in gallons per minute [GPM]), the PLC can calculate the total number of gallons being supplied to the system. This flow total is then communicated to the poll master.

The poll master uses the daily flow totals from each site, as well as the set points entered by the operator at either the LOI or SCADA, to calculate the current levels of water quality. If the water quality is outside of compliance parameters, alarms are generated and sent to SCADA. The appropriate wells are automatically shut down by the poll master.

Each cycle of logic takes only about 60 milliseconds. Calculations in the PLC are checked and rechecked every cycle, meaning operators are informed of water that is not in compliance moment by moment.

Water quality objective

As aforementioned, the new groundwater source has higher hardness and naturally occurring minerals, such as iron and manganese, including the regulated constituents hexavalent chrome (chrome-6) and nitrate, than the surface water sources. The water quality objectives for the SFPUC Groundwater Program are to treat and blend the groundwater sources to meet drinking water quality regulations, and just as importantly, to maintain the high-quality and "good tasting" water to which San Francisco residents are accustomed.

Groundwater treatment approach

The groundwater quality from the 15 wells varies. Some wells do not require any treatment; some have minimal chemical conditioning systems; and some have more extensive treatment systems. For example, several well stations include filters to remove iron and manganese, and many wells add chlorine to match the disinfection residual in the imported surface water. In all cases, the relatively low flows of groundwater are blended into generally much higher flows of surface water, such that customers should not be able to notice a change in the aesthetic qualities of the water.

In the SFGW system, the groundwater is connected and blended directly into the large Sunset Reservoir. In the RGSR system, where groundwater is blended with treated surface water in four SFPUC transmission pipelines, the blending must take place before the water reaches the first customer on that pipeline. Figure 6 shows a schematic of the blending system configuration for a SFPUC RGSR Well Station.

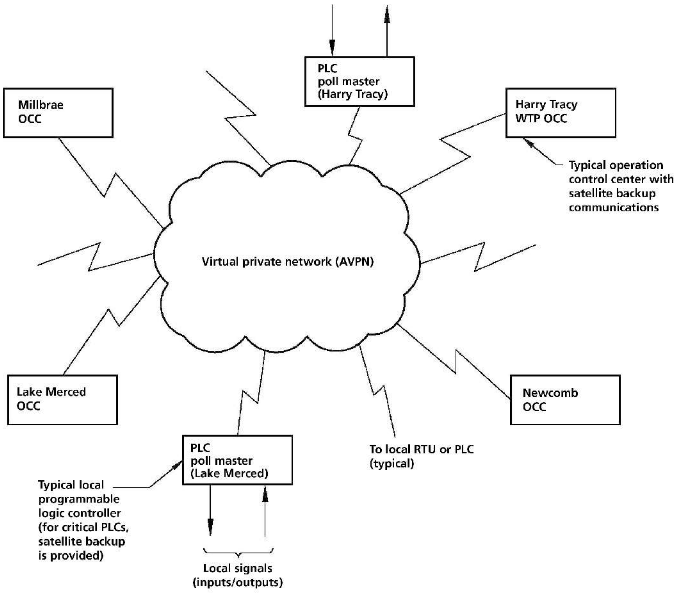


Figure 3. SFPUC Water SCADA simplified network diagram

The RGSR Well Station transmission pipeline blending system includes the following components:

- Well head compliance sample tap: for raw groundwater sample collection.
- Well station flowmeter: measures groundwater flow rate into the transmission pipeline.
- Transmission pipeline flowmeter: measures flow rate for blending calculations and the direction of the surface water

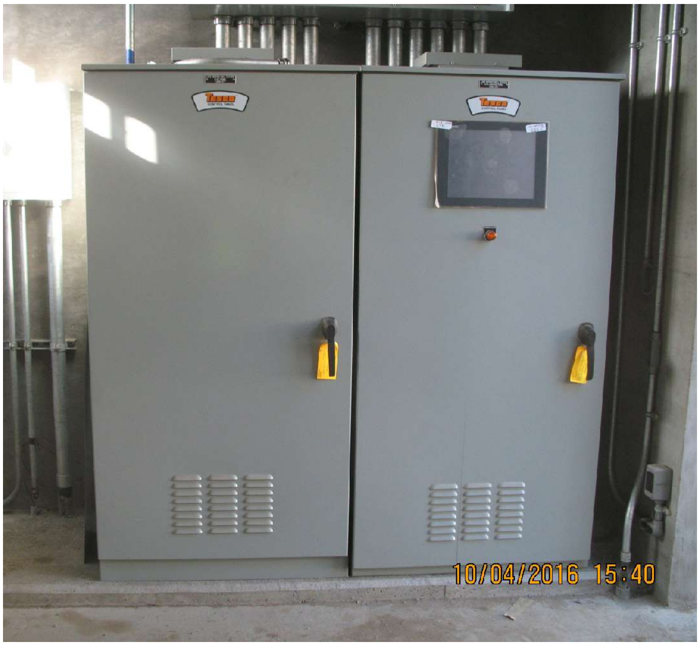


Figure 4. Lake Merced PLC master controller. The PLC is a redundant CPU with hot backup connected to AVPN network with redundant fiber-optic cables.

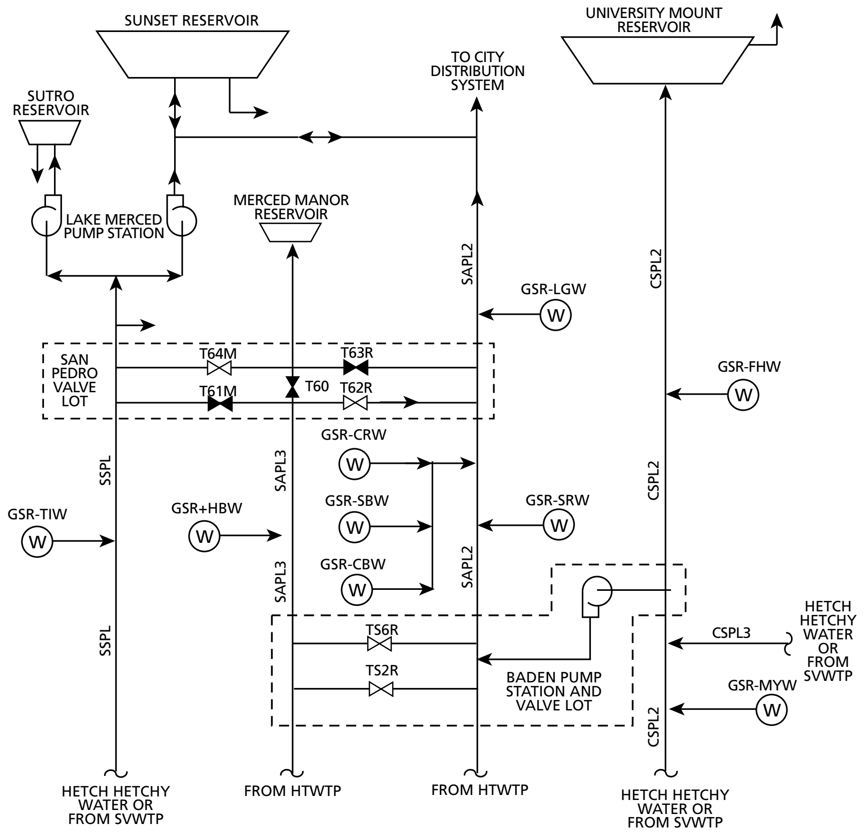


Figure 5. Groundwater is also blended with imported surface water in the four major transmission pipelines to the city of San Francisco.

flow in the transmission pipeline.

- Connection point to the SFRWS transmission pipeline: point on transmission pipeline where chemically treated groundwater from the well station is introduced.
- Blending treatment zone: section in the transmission pipeline where the chemically treated groundwater and the surface water are mixed. The blending zones range between 400 and 580 feet, depending on the particular conditions at the station.
- Compliance sample point: where water quality samples are monitored for compliance, located downstream of the blending zone but upstream of the first customer turnout.
- Distance to first customer turnout: a minimum of 100 feet from the compliance sample point for each well station to the first customer turnout.

System water quality monitoring and control

The water quality of the SFPUC blended water is monitored and controlled at each well station transmission line compliance point and as an overall system.

Water quality analyzers and flowmeters at each well station continuously monitor the system and calculate the blended water quality at the transmission pipeline compliance points. Some water quality parameters, such as pH and chlorine residual, can be monitored in real time with online analyzers. Some parameters, such as chrome-6 and nitrate levels, are calculated based on mass balance calculations for the system.

The SCADA system monitors and calculates the combined water quality from multiple wells that contribute to a common transmission pipeline. As the flow rates of surface water and groundwater change, the SCADA system adjusts the calculations to automatically update the calculated water quality parameters. Online analyzers for pH, conductivity, and chlorine residual also provide real-time feedback for adjustments to the well chemical feed systems. The SCADA system also generates alarms and automatically shuts down affected groundwater wells when the monitored or calculated water quality parameters exceed a predetermined set point. This ensures that the blended water quality will always meet SFPUC's water quality objectives to maintain high-quality, "good tasting" water for customers.

Preliminary functional startup tests successfully showed that the online water quality and control system operates very effectively in monitoring and controlling the water quality for the ultimate purpose of delivering high-quality drinking water to the city of San Francisco res-

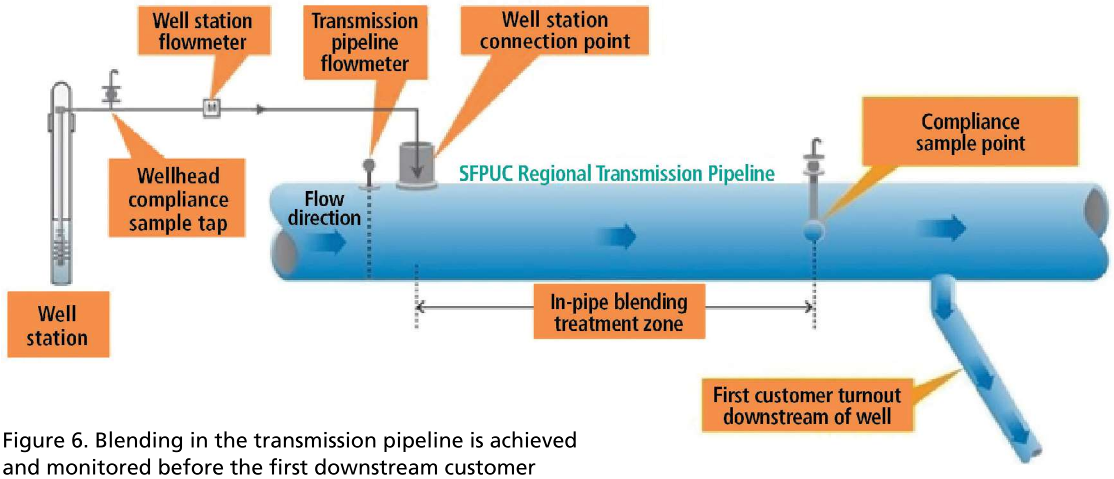

Well station flowmeter
Transmission pipeline flowmeter
Well station connection point
Wellhead compliance sample tap
Flow direction
SFPUC Regional Transmission Pipeline
Compliance sample point
Well station
In-pipe blending treatment zone
First customer turnout downstream of well

Figure 6. Blending in the transmission pipeline is achieved and monitored before the first downstream customer

Gruhn is 2019 society president

Paul Gruhn, PE, CFSE, and ISA Life Fellow, will serve as ISA president in 2019. In this role, he will lead the ISA Board of Directors, which is responsible for governing, setting policy, and establishing the strategic direction of the organization. "I'm honored to be the 2019 society president," said Gruhn, a globally recognized expert in process safety and safety instrumented systems who has played a pivotal role in developing ISA safety standards, training courses, and publications. "Like any organization over the last 30 years, ISA has naturally had its ups and downs. To grow and remain relevant, we must adapt to both the changing times and the changing demographics of our industry."

Gruhn is a global functional safety consultant with aeSolutions, a process safety, cybersecurity, and automation consulting firm. He serves as a co-chair and long-time member of the ISA84 standard committee (on safety instrumented systems) and continues to develop and teach ISA courses on safety systems. He also developed the first commercial safety system modeling program. Gruhn has written two ISA textbooks, numerous chapters in other books, and dozens of published articles. ■

In memoriam

Former ISA president **Thomas J. Harrison, PhD, PE**, a retired electrical engineer and professor, died 18 December 2018. Harrison earned a BS and MS from Carnegie-Mellon University and a PhD from Stanford University. He spent 29 years with IBM in a variety of engineering and engineering management positions at the San Jose and Boca Raton IBM Laboratories and at IBM's Academic Information Systems in Tallahassee.

Harrison was an active ISA member, especially in standards. He was S&P vice president on the ISA Executive Board and was ISA president in 1986. Harrison was also a professor of electrical engineering at the FAMU-FSU College of Engineering and department chairman from 1988–1995. He published more than 50 articles and invited papers, contributed to four books and encyclopedias, and wrote two books. He held four U.S. patents and received IBM's Outstanding Invention and Invention Achievement awards. He also lectured extensively throughout the world, including invited lectures in many foreign countries. ■

idents. Functional startup tests also prove that the highly reliable SCADA system has been the most important element of the control system that operates 24/7 with highly competent SF staff contributing to the success of this project. ■

ABOUT THE AUTHORS

Diep Nguyen, PE (diep@ieee.org), is a principal engineer of DTN Engineers, Inc., and a licensed EE, CSE, and FPE in California. He is a Life Member of ISA and IEEE.

Jeff Gilman, PE (JGilman2@Earthlink.net), was a SFPUC senior project manager with more than 40 years of experience. He is a licensed geologist and hydrogeologist in California.

Todd Reynolds, PE (ToddReynolds@KennedyJenks.com), is a vice president of Kennedy/Jenks Consultants, a consulting engineering firm for environmental projects.

A.J. Cottengim (ACottengim@TescoControls.com) is a senior PLC programmer with Tesco Controls Inc., a system integrator and manufacturer based in Sacramento, Calif.

View the online version at www.isa.org/intech/20190206.

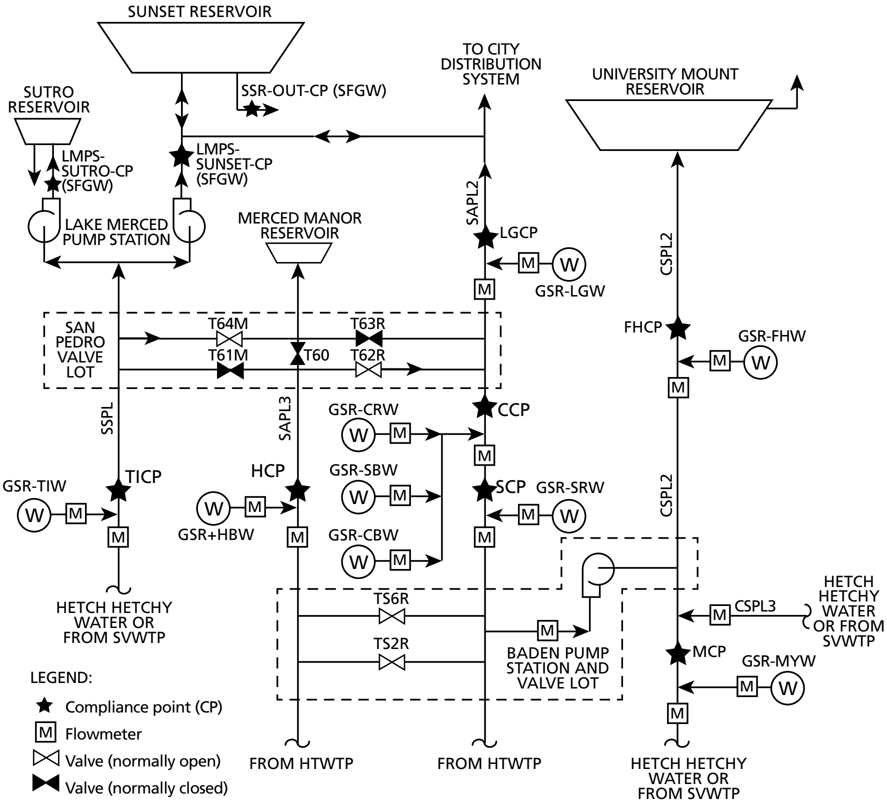


Figure 7. Water quality is monitored and controlled at compliance points (stars) and in the regional system and in the Sunset Reservoir in the city.

ISA Certified Automation Professional (CAP) program

Certified Automation Professionals (CAPs) are responsible for the direction, design, and deployment of systems and equipment for manufacturing and control systems.

CAP question

After attending operator training, participants are asked to evaluate the training session by filling out a questionnaire. Which statement best describes the importance of evaluating operator training sessions?

A. It indicates how well participants liked the training.
B. It helps to measure program effectiveness and areas for improvement.
C. It provides records of who participated for ongoing monitoring.
D. It provides compliance records for training mandated by federal, state, and local regulations.

CAP answer

The correct answer is *B*, "It helps to measure program effectiveness and areas for improvement." The intent of training is to have all participants apply the knowledge and skills they learn from training to their jobs. Evaluation helps to determine what final outcomes occurred because of attendance and participation in the training. It also helps to determine how to improve the training when the learning experience has fallen short.

Reference: Trevathan, Vernon L., *A Guide to the Automation Body of Knowledge, Second Edition,* ISA, 2006.

ISA Certified Control Systems Technician (CCST) program

Certified Control System Technicians (CCSTs) calibrate, document, troubleshoot, and repair/replace instrumentation for systems that measure and control level, temperature, pressure, flow, and other process variables.

CCST question

All of the following instrumentation bus networks can be implemented with a single pair of wires, except for?

A. Foundation Fieldbus
B. DeviceNet
C. AS-i
D. HART

CCST answer

The answer is *B*, "DeviceNet." Foundation Fieldbus (FFB), Actuator-Sensor Interface (AS-i), and Highway-Addressable Remote Transducer (HART) instrument bus networks all operate over a single pair of wires. The power for the transmitter and the communication signal are both carried over that single pair of wires.

DeviceNet requires a separate pair of wires for power and signal, with an additional shield/ground wire. DeviceNet, then, typically requires five conductors (two pairs and a shield/ground).

Reference: Goettsche, L. D. (Editor), *Maintenance of Instruments and Systems, Second Edition,* ISA, 2005.

New CAPs and CCSTs

Qualifying for and passing one of ISA's certification exams is a noteworthy accomplishment. The exams are rigorous and require a solid command of various disciplines in automation and control. Below is a list of individuals who have recently passed either our Certified Automation Professional (CAP) or one of the three levels of our Certified Control System Technician (CCST) exam. Congratulations to our new certification holders! For more information about the ISA CAP and CCST certification programs, please visit www.isa.org/training-and-certifications/isa-certification.

Certified Control System Technicians

Name	Company	Location
Level 1		
Daniel G. Williams	TAI Engineering	U.S.
Michael M. Doogah	Polk County Utilities	U.S.
Everett H. Smith	Federal Reserve	U.S.
John D. Knott	None	U.S.
Thomas M. Anderson	North Davis Sewer District	U.S.
Kylee G. Nelson	North Davis Sewer District	U.S.
Joshua G. Cox	Mallinckrodt Pharmaceuticals	U.S.
Michael A. Genovese	None	U.S.
Kevin D. Howard	None	U.S.
Michael D. Milbut	None	U.S.
Nathan V. Hutchins	None	U.S.
John G. Hermes	The Coca-Cola Company	U.S.
Matthew R. Carney	Duke Energy	U.S.

Level 2		
Lee P. Griswold	Newmont	U.S.
Austin David Carley	None	U.S.
Marlo P. Esparza	None	U.S.
Gary Mike Waters	United Water Idaho	U.S.
Timothy C. Secrest	None	U.S.
Joshua A. Smith	None	U.S.
Matt A. Hayes	None	U.S.
Justin M. Kovalski	None	U.S.
Jason W. Gerard	None	U.S.
R ick M. Mirolla	None	U.S.
Edward V. Keen	None	U.S.

Harnessing automation in new ways: The future of manufacturing depends on it

By Mary Ramsey

For dozens of years, automation has revolutionized manufacturing around the world. Companies leverage automation technology to increase productivity, eliminate variation in products, improve quality, increase speed, and prevent injuries and accidents.

Manufacturing, in the U.S. and around the world, is poised for a step change that will forever alter the way we produce goods and services. Are we ready to create our own future?

We live in a world that is constantly evolving, and the future of manufacturing rests on our ability to advance technology to keep pace with global demands. Rapid-fire development in robotics, artificial intelligence, and machine learning are giving us the opportunity to pair human capital with technology in new and exciting ways. While manufacturing was once a series of simple, repetitive tasks done by humans, automation has taken over those roles and allowed workers to advance their skills and develop more fulfilling, engaging professions. Productivity has skyrocketed, and quality has dramatically improved, which allows companies to stay competitive in the marketplace.

The age of automation brings infinite opportunities. We can improve upon traditional control systems while maintaining the integrity, safety, and security of operations; and we can leverage the Internet of Things (IoT) to collect disparate data and correlate it to anticipate problems through predictive and preventive measures.

With each opportunity comes challenges to improve and maintain safety and cybersecurity within manufacturing operations. Critical applications and infrastructure, such as power and water, face increasingly difficult demands to harden their security and ensure the safety of their employees and the communities that they serve.

The role of consensus-developed standards in this new world cannot be overstated—standards that industry develops and believes in will enable us to navigate these open interoperability technologies safely and securely.

In addition to the standards that identify the specifications and best practices necessary to leverage new technology, we will also need to invest in our human capital. Our companies are facing significant skill gaps—we are losing experienced employees to retirement, and we are asking new employees to quickly and efficiently learn existing processes along with cutting edge and next-generation technologies.

This strain on the workforce results in an ever-increasing need for quality real-world training and assessment programs. Comprehensive training paths, along with certificates and certifications in critical areas like safety and security, are invaluable tools for industry. These programs enable companies to quickly measure readiness, and they offer individuals an opportunity to evolve their skill sets to match the documented needs of industry.

ISA has been the trusted advisor in standards-based training and certification for decades, and we intend to lead the way in developing and promoting these training and assessment programs that companies need. We invite you and your companies to partner with us on this journey. ■

RESOURCES

ISA/IEC 62443 Cybersecurity Certificates

This certificate recognition program increases awareness of the ISA/IEC 62443, *Security for Industrial Automation and Control Systems*, standards and the critical area of how security relates to the industrial automation and control system life cycle. The certificate programs are designed for professionals involved in information technology and control system security roles who need to develop a command of industrial cybersecurity terminology and an understanding of the material embedded in the ISA/IEC 62443 standards to assess, design, implement, and maintain a cybersecurity program for their organizations. ISA/IEC 62443 cybersecurity certificates are awarded to those who successfully complete a designated training program and pass a comprehensive exam.

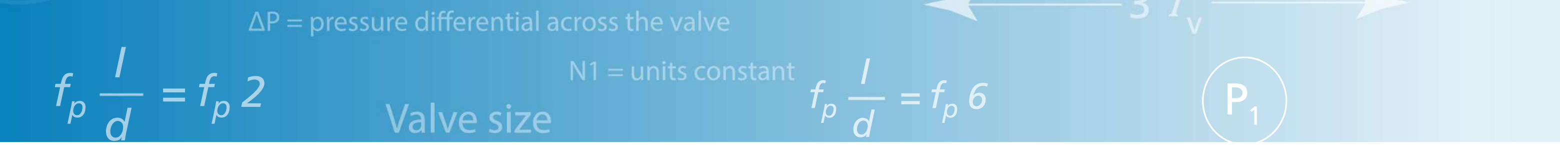
ISA84 Safety Instrumented Systems Certificates

ISA and the Automation Standards Compliance Institute (ASCI) offer three certificate programs that will increase knowledge and awareness of the ISA84 (IEC 61511), *Functional Safety—Safety Instrumented Systems (SIS) for the Process Industry Sector*, standard. Each certificate program includes specialized training on ISA84 and an exam that is offered through the Prometric testing centers.

For more information, visit www.isa.org/training.

ABOUT THE AUTHOR

Mary Ramsey is the executive director of ISA.


ΔP = pressure differential across the valve
$f_p \frac{l}{d} = f_p 2$
N1 = units constant
Valve size
$f_p \frac{l}{d} = f_p 6$
P_1

Understanding the rated capacity of full-bore ball valves

By Marc L. Riveland
and Andrew Kinser

Depending on the methods ball valve manufacturers use to determine their published rated flow capacities, the resulting value may be different, even for virtually identical valves. Rated flow capacity of a valve is typically expressed in terms of some type of flow coefficient, currently usually, C_v and K_v. They are equivalent but differ in value due to the units for flow rate and pressure they are associated with. The ISA and IEC standards recognize both coefficients. Equations are written in terms of a generic coefficient, C, and units constants, N, that account for the specific coefficient and units. The preferred method of evaluating these coefficients is by conducting a flow test.

Full-bore ball valves (FBBVs) in the full-open position present some challenges. First, they typically do not fall within the scope of conventional control valve sizing methods. One of the criteria imposed by these standards to maintain stated accuracy is that:

$$\frac{C}{N_{18} d^2} < 0.047 \qquad (1)$$

Where C = flow coefficient (C_v or K_v); d = internal diameter; and N_{18} = units constant (table 1). Note that C_v is the resulted coefficient when using U.S. standard units, and K_v is the resulted coefficient when using metric units.

Values of this expression for typical published FBBV C values range from 0.10 to 0.25, clearly exceeding the threshold value. A second challenge related to the ultrahigh capacities of these valves is that they may exceed the flow capacity of the test lab.

Attempting to represent the flow capacity of an FBBV in terms of control valve standard methods is confounding and can be very misleading, especially when comparing different ball valve units. Based on the control valve C method, published data suggests that a much bigger FBBV is needed to match the desired capacity of an isolation-type valve. In reality, the two valve types should be the same size.

Engineers specifying FBBVs should ask the supplier how the rated C was determined to make sure they purchase the correct size. While the flow coefficient C has conditional utility, it is important to understand the definition and evaluation methods for this term as presented in the standards. Following are two different approaches to evaluating the flow coefficient of a line size FBBV in the full-open position.

Table 1. Numerical constants N

Constant	Flow coefficient, *C*		*Q*	*P, ΔP*	*d*
	K_v	C_v			
N_1	1 x 10^{-1}	8.65 x 10^{-2}	m^3/h	kPa	
	1	8.65 x 10^{-2}	m^3/h	bar	
		1	gpm	psia	
N_{18}	8.65 x 10^{-1}	1.00			mm
		6.45 x 10^2			in

Standards-based method (empirical)

This method is based on actual flow testing of the FBBV according to industry standards. The test method prescribes a test manifold, along with the methods for measuring flow rate and pressure drop to allow direct calculation of the flow coefficient. The test manifold includes the valve and lengths of straight pipe upstream and downstream of the valve. The inlet (P_1) pressure is measured two pipe diameters upstream of the valve, and the outlet (P_2) pressure is measured at six pipe diameters downstream of the valve.

The flow coefficient at test conditions is calculated from the following equation:

$$C = \frac{Q}{N_1}\sqrt{\frac{G_L}{\Delta P}} \qquad (2)$$

Where Q = volumetric flow rate; G_L = liquid specific gravity (water = 1.00); ΔP = pressure differential across the valve; and N_1 = units constant (see table 1). Note that the pressure drop used in equation 2 includes the additional losses associated with the eight diameters of straight pipe. This effect is typically minimal for most control valves within the scope of the standard, because the valve produces the dominant loss compared to the piping loss. However, the FBBV is essentially a very short piece of straight pipe, and the test piping losses can actually exceed the losses strictly attributable to the valve in some instances.

Flow model–based method (analytical)

The basis of the analytical approach for computing the flow coefficient C is to start with an estimate of the static head loss coefficient K_L associated with the

FBBV. The loss coefficient estimate may be as simple as assuming the FBBV behaves as a straight pipe and determining friction losses, or a more complex approach based on using a specific handbook model. An example of the latter is offered by Crane, which suggests using the loss coefficient model:

$$K_{bv} = 3f_{bv} \qquad (3)$$

Where K_{bv} = velocity head loss coefficient for the ball valve and f_{bv} = turbulent pipe friction factor associated with the ball valve. The friction factor may be evaluated from a number of methods and resources but will generally fall in the range of 0.01 to 0.02.

The conversion to flow coefficient *C* is given by the derived equation

$$C = \frac{0.047N_{18}d^2}{\sqrt{K_{bv}}} \qquad (4)$$

Where *d* = inside pipe diameter (or in this case ball valve diameter). This analytical method does not include the effects of upstream and downstream test piping integral to the empirical method.

Comparison of methods

To make a meaningful comparison between the two evaluations, the effects of loss from piping must be treated the same in both models. One approach is to use the analytical method, but to employ a modified model that includes the effects of straight pipe, as shown in figure 2.

1. Convert reported flow coefficient to a loss coefficient.

Rearranging equation (4):
$$K_{bv} = \left[\frac{29.9d_1^2}{C_v}\right]^2 \qquad (5)$$

2. Add line losses. The equivalent loss coefficient for a given length of pipe of is:
$$K_p = f_p\frac{l}{d} \qquad (6)$$

Where *l* = length of straight pipe; *d* = inside diameter of pipe; and f_p = pipe turbulent friction factor. Therefore,

$$K_{total} = f_p\frac{l_1}{d_1} + K_{bv} + f_p\frac{l_2}{d_2}$$
$$= 2f_p + K_{bv} + 6f_p \qquad (7)$$
$$= K_{bv} + 8f_p$$

3. Convert back to the flow coefficient. Calculate the revised coefficient based on the total loss:

$$C_v = \frac{29.9d_1^2}{\sqrt{K_{bv} + 8f_p}} \qquad (8)$$

Published C_v values for two different ball valve designs are shown in table 2. Even though the two valves are different brands, the flow paths through them are virtually identical, so the flow coefficients should be nearly equal. However, brand "X" considers only the losses in the valve, so the flow coefficient is considerably larger than brand "Y," which is tested and includes the test manifold piping losses.

Use the analytical adjustments discussed above to make a more meaningful comparison. Flow coefficient values can be estimated considering only the losses in the valve (equation 4). As shown in table 2, these results are a close match to the values for brand "X."

When the analytical piping losses are also considered (equation 8), the resulting capacity is much closer to the tested brand. From this comparison, it can be concluded that even though the published flow coefficient values for these values are very different, they will both pass the same flow rate under the same conditions.

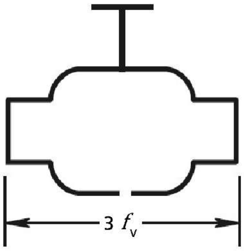


Figure 1. Ball valve loss model

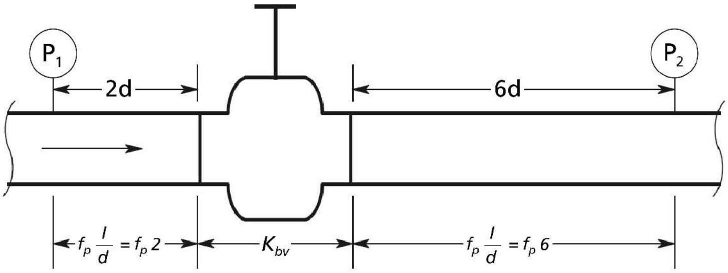


Figure 2. Modified loss model including piping losses

Flow capacity

Representing the flow capacity of full-bore ball valves in the wide-open position presents some challenges. The flow coefficient is very sensitive to whether or not associated test piping frictional losses are included. Published values for different manufacturers may be based on different approaches. To ensure a correct selection, understand how the the valve manufacturer determined the flow coefficient. ■

ABOUT THE AUTHORS

Marc L. Riveland is retired from Emerson Automation Solutions. Riveland is chairman of the ISA75.01 working group on control valve sizing and is on other ISA75 working groups and IEC TC65B WG9.

Andrew Kinser (Andrew.Kinser@emerson.com) is the manager of test and evaluation engineering at Emerson Automation Solutions.

Table 2. Comparison of published and calculated flow coefficients

			Published C_v		Analytical method[†] C_v	
Valve size	f_p	***d*, inches**	**Brand X**	**Brand Y**	**w/o piping loss**	**w/ piping loss**
8	0.014	7.981	9,000	6,040	9300	4,810
12	0.013	12.00	22,500	12,300	21,800	11,500
16	0.013	15.25	37,200	19,900	35,200	18,700

[†] Assume $f_{bv} = f_p$. Actual value may be less than the pipe friction factor because the interior surface is machined.

United Nations commission to integrate ISA/IEC 62443 into Cybersecurity Regulatory Framework

The United Nations Economic Commission for Europe (UNECE) confirmed at its annual meeting in late 2018 that it will integrate the widely used ISA/IEC 62443 series of standards into its forthcoming Common Regulatory Framework on Cybersecurity (CRF). The CRF will serve as an official UN policy position statement for Europe, establishing a common legislative basis for cybersecurity practices within the European Union trade markets.

At the same time, the UNECE's Working Party on Regulatory Cooperation and Standardization Policies recognized the ISA99 standards development committee for its leading role in conceiving and developing the widely used standards.

The ISA/IEC 62443 standards are developed primarily by the ISA99 committee, with simultaneous review and adoption by the Geneva-based International Electrotechnical Commission (IEC). ISA99 draws on the input of cybersecurity experts across the globe in developing consensus standards that are applicable to all industry sectors and critical infrastructure, providing a flexible and comprehensive framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACS).

UN recognition of ISA99 capped a year in which two major standards in the ISA/IEC 62443 series were completed:

- ISA/IEC 62443-4-2, *Security for Industrial Automation and Control Systems: Technical Security Requirements for IACS Components,* provides the cybersecurity technical requirements for components that make up an IACS, specifically the embedded devices, network components, host components, and software applications. The standard, which is based on the IACS security requirements of ISA/IEC 62443-3-3, *System Security Requirements and Security Levels*, specifies security capabilities that enable a component to mitigate threats for a given security level without the assistance of compensating countermeasures.
- ISA/IEC 62443-4-1, *Security for Industrial Automation and Control Systems: Product Security Development Life-Cycle Requirements,* specifies process requirements for the secure development of products used in an IACS and defines a secure development life cycle for developing and maintaining secure products. The life cycle includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management, and product end-of-life.

In addition, another standard in the series is nearing completion. ISA/IEC 62443-3-2, *Security Risk Assessment, System Partitioning and Security Levels,* is based on the understanding that IACS security is a matter of risk management. That is, each IACS presents a different risk to an organization depending upon the threats it is exposed to, the likelihood of those threats arising, the inherent vulnerabilities in the system, and the consequences if the system were to be compromised. Further, each organization that owns and operates an IACS has its own tolerance for risk.

ISA/IEC 62443-3-2 will define a set of engineering measures to guide organizations through the process of assessing the risk of a particular IACS and identifying and applying security countermeasures to reduce that risk to tolerable levels. A key concept is the application of IACS security zones and conduits, which were introduced in ISA/IEC 62443-1-1: *Concepts and Models*. The new standard provides a basis for specifying security countermeasures by aligning the identified target security level with the required security level capabilities set forth in ISA/IEC 62443-3-3: *System Security Requirements and Security Levels*.

For information on viewing or obtaining any of the ISA/IEC 62443 standards, visit www.isa.org/findstandards. For information on ISA99 and the ISA/IEC 62443 series of cybersecurity standards, contact Eliana Brazda, ISA Standards, ebrazda@isa.org or +1-919-990-9200. ■

Updated fire and gas technical report completed by ISA84

A newly revised technical report has been completed by the ISA84 standards committee, Instrumented Systems to Achieve Functional Safety in the Process Industries. ISA-TR84.00.07, *Guidance on the Evaluation of Fire, Combustible Gas, and Toxic Gas System Effectiveness,* is intended to help address detection and mitigation of fire, combustible gas, and toxic gas hazards in process areas. Fire detection and mitigation within nonprocess areas are outside the scope of the document.

Fire and gas systems per this technical report are a subset of industrial automation and control systems that are used in the process industries to detect loss of containment of hazardous materials from a process and initiate a response to mitigate the release impact. Loss of containment can be a small leak or a catastrophic release. It can be detected by measuring the presence of the released materials or inferred from the effects of the release.

For information on viewing or obtaining this or any of the ISA84 standards and technical reports, visit www.isa.org/findstandards. ■

Path to OT success on the plant floor as described by users

By Stephen Malyszko, PE

These articles typically contain words of wisdom and advice from industry consultants or subject-matter experts. The content of this article, however, is from actual users who recently answered a series of questions by Malisko's IIoT lead, Mark Fondl. The responses that follow are in the user's own, unedited, words.

What are some pointers when explaining the different needs of the manufacturing networks to upper management?

"With today's typical level of automation, as the network goes—so goes the plant."

"If you lose your email it's annoying. If you lose your manufacturing operations, it's career limiting."

"We have told management that our most critical needs are: (1) uptime, (2) reliability, (3) security. However, IT has told their management that their most critical needs are: (1) security, (2) reliability, (3) uptime. Trying to get these priorities aligned between the groups has been an extreme challenge."

Suggest an approach to create a collaborative environment between information technology (IT) and the controls groups.

"Garner a mutual understanding that the control and IT networks are different. While some standards may apply equally across both environments, other standards may have a higher or lesser degree of importance or necessity in the other environment. Common differences lie in the level of architecture that the two groups are focused on. The IT systems, standards, support structures, and policies are typically more established than in the controls realm. As the need to integrate plant floor/controls data systems across the business, the controls group does not often have the same level of knowledge or infrastructure as the enterprise level. Adopting and learning the IT standards and policies are not a nice to have but a must."

"This has been one of the greatest struggles within our organizations. Unfortunately, this relationship is still extremely adversarial. My best advice is to have a single point of confluence where the IT and controls group meets. All needs from the controls group goes to a single person, who then figures out what IT group needs the information and funnels all technical requests back to the controls group. Get all needs and requests in front of each group with as much advance time as possible."

What should others know about security and the positive and negative effects it may have on performance or supportability?

"Higher security increases mean complexity of system architecture. However, [it] can provide higher reliability if designed correctly. Higher security has not impacted network performance; however, [it] has increased cost due to time required to approve access for contractors needing to support systems."

"From a security position, keeping firewalls and level 3 switches as impenetrable as possible is important."

Is it important that plant floor people be involved in support of the networks?

"Yes, especially process systems and packaging integration."

"Yes, they are ultimately the customer; they should have some say in the services to be provided."

"Plant floor people accept responsibility for the health of equipment in plant processes. Plant tech is the nervous system that assures that equipment runs safely and reliably. Establish agreement that asset care includes plant tech. Establish the role for plant floor personnel. Much of the support of plant tech is provided by remote resources. Remote support can be efficient and cost effective. Plant floor people are an essential part of effective support."

Is it important to create a demilitarized zone (DMZ) or boundaries in the networks?

"Yes, to limit who has access to systems they're not authorized to access or trained to support."

"Yes. Protocol changing across DMZ boundaries makes it more difficult for outside attacks on a specific protocol. When implemented with a firewall, it also provides additional visibility and auditing along with troubleshooting capabilities."

"Creating a DMZ helps keep unwanted network traffic from flooding the controls network and interfering with machine-to-machine communications."

Can you discuss the importance of using outside resources to help you and why?

"If you're not current with industrial network technologies, you may inadvertently install COTS-grade equipment and will pay dearly for saving a few pennies."

"The biggest issue is they have done multiple installations and learned from other's mistakes. In other words, experience."

"Deployment of industry best practices and ways to optimize cost and resource requirements."

What are the key capabilities you look for in a system integrator on your network designs or deployment?

"Are they smart enough to listen to me before they tell me how good they are?"

"OT and IT capability under the same roof."

"Solid understanding of network fundamentals (how is it constructed/configured and what makes it work), experience with similar or applicable applications, and ability to view application from design, installation, and maintenance viewpoints."

"Deployment of industry best practices following CPwE methodologies focused on cell, area deployment with server infrastructure on different VLAN/networks." ■

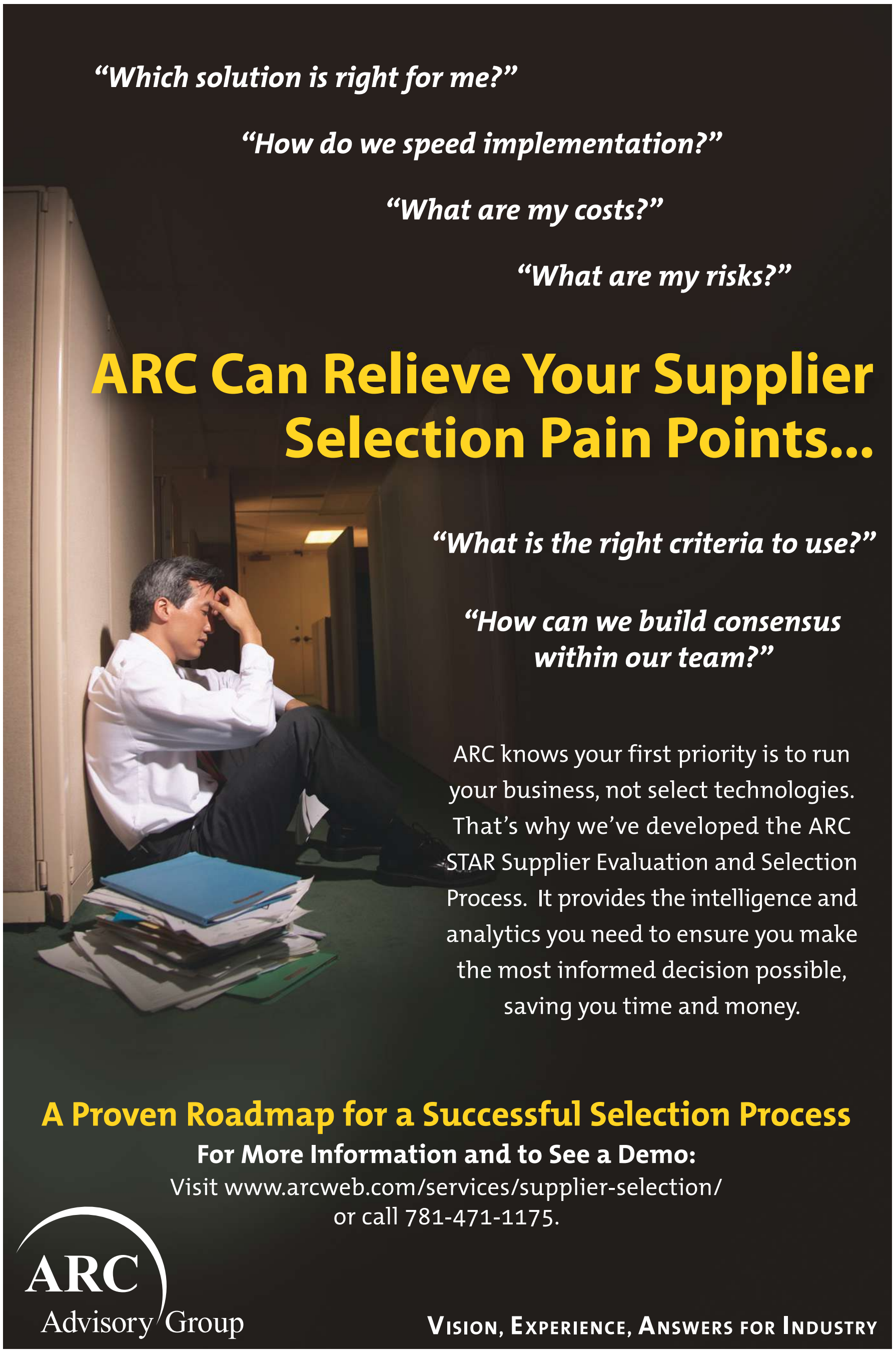
ABOUT THE AUTHOR

Stephen Malyszko, PE, president, CEO, and cofounder of Malisko Engineering, Inc., has spent his entire 40-year career developing systems for manufacturing automation. Contact +1 314-881-5410 or www.malisko.com for more information.

ad index

InTech advertisers are pleased to provide additional information about their products and services. To obtain further information, please contact the advertiser using the contact information contained in their ads or the Web address shown here.

Advertiser	Page #
Allied Electronics www.alliedelec.com	**Cover 4**
ARC Advisory Group www.arcweb.com	**48**
Assured Automation www.assuredautomation.com	**35**
Automation Direct www.automationdirect.com	**Cover 2**
Endress + Hauser www.us.endress.com	**17**
Festo www.festo.com	**23**
Inductive Automation www.inductiveautomation.com	**Belly band**
ISA www.isa.org	**35**
Keller America www.kelleramerica.com	**3**
MAVERICK www.mavtechglobal.com	**26–27**
Moore Industries www.miinet.com	**6**
ProComSol, Ltd. www.procomsol.com	**10**
Stratus Technologies www.stratus.com	**insert at 11**
Tadiran www.tadiranbat.com	**21**



Contact *InTech* today:

Richard T. Simpson
Advertising Sales Representative
Phone: +1 919-414-7395
Email: rsimpson@automation.com

Chris Nelson
Advertising Sales Representative
Phone: +1 612-508-8593
Email: chris@automation.com

Kelly Winberg
Advertising, Classifieds Section
Phone: +1 267-718-8197
Email: kwinberg@comcast.net

Chris Hayworth
Advertising Materials Coordinator
Phone: +1 919-990-9435
Email: chayworth@ISA.org

View and download the InTech media planner at **www.isa.org/intechadkit**

Reprints

Foster Reprints will work with you to create a customized reprint package, including hard copy reprints, eprints, and mobile-friendly products.

Contact Jill Kaletha at 219-878-6068 or jillk@fosterprinting.com.

datafile

Datafiles list useful literature on products and services that are available from manufacturers in the instrumentation and process-control industry. To receive free copies of this literature, please contact each manufacturer via their provided contact information.

USB HART MODEM

The HM-USB-ISO USB HART modem meets industry standards for USB and HART connectivity. The small size, light weight, and durability of the HM-USB-ISO make it ideal for portable use. Operating power is derived from the USB connection. An easily installed Virtual Serial Port driver allows use in any Windows-based application.

It is the lowest cost USB Modem certified by the FieldComm Group to meet the HART communication specifications.

ProComSol, Ltd, Process Communications Solutions
Tel. 216.221.1550; Fax 216.221.1554
sales@procomsol.com; www.procomsol.com
Toll Free 877.221.1551

Sample of Jobs Available at Jobs.isa.org

See more at Jobs.isa.org, where you can search for available jobs or advertise positions available within your company. ISA Members post resumes at no charge.

Manufacturing engineer

Arthrex, Inc.: The engineer in Sandy Springs, S.C., will design, develop, implement, and improve manufacturing processes to produce medical device products and systems. The engineer will provide manufacturing engineering expertise to create, document, and implement required procedures and documents. The position requires a BS in engineering, science, or mathematics; three or more years of manufacturing process improvement experience; proven experience leading projects; the ability to work independently and effectively with cross-functional teams, and a thorough understanding of manufacturing processes. Medical device manufacturing experience is preferred . . . see more at Jobs.isa.org.

Senior electrical engineer

Raytheon: The Electrical Subsystems Directorate Product Technology Center in Huntsville, Ala., is seeking a senior electrical engineer with strong digital electronics design and analysis skills. Desired candidates are willing to collaborate, innovate, and work with a team to generate and use technology to design digital electronics circuits that implement missile guidance and video and digital signal processing. The engineer will contribute to the design, analysis, simulation, test, and integration of digital electronic modules and CCAs for missile applications. The engineer must be experienced in all aspects of circuit card design as evidenced by multiple successful design completions. The position also requires frequent use and application of technical standards . . . see more at Jobs.isa.org.

Process improvement manager

Corning Optical Communications LLC: The process improvement manager, located in Keller, Texas, will be responsible for supporting the identification, development, deployment, and execution of best-practice processes to facilitate product life-cycle management. He or she will be a project leader in developing new or in improving existing PLM processes. The position requires domestic and international travel and requires an MBA and BS in engineering (any discipline) or related field, three years of engineering experience working for a business-to-business large-scale manufacturer, and at least two years of experience designing, implementing, and monitoring workflow using Windchill . . . see more at Jobs.isa.org.

Mechanical engineer

Lockheed Martin Corporation: The company's Rotary and Mission Systems business in Moorestown, N.J., seeks an entry-level mechanical engineer who will contribute to a wide variety of projects. The ability to take responsibility for increasingly difficult tasks, complete them on schedule, and document the results is expected. A strong candidate will demonstrate an interest and ability to learn new tools and technologies, strong oral and written communication skills, strong problem-solving skills, and the ability to work independently and in a team environment. A BS in mechanical engineering or a closely related technical field and a GPA of at least 3.0 is required. Familiarity and experience in mechanical design engineering (PRO-E, CREO, Catia 4), circuit card layout, design for manufacturability, or geometric dimensioning and tolerances is desired . . . see more at Jobs.isa.org.

Modulating actuators

The company has extended its CMA range of compact modulating actuators with sizes specifically meant for automation of larger linear control valves. The actuator is capable of a maximum 4,500 lbf (20 kN) seating thrust. The new sizes increase the CMA range modulating thrust performance to 3,000 lbf (13 kN) with a 114.3 mm (4.5 inch) stroke length for the automation of larger valves with higher pressure ratings.

The CML-1500 and CML-3000 models, including those with hazardous area approvals, are watertight to IP68 for temporary submersion (7 meters, 72 hours). The optional reserve power pack uses supercapacitors to give the actuator enough stored energy to perform predetermined action on mains power failure, such as moving to the fully closed position, the fully open position, or anywhere in between. Manual operation is available as standard.

The electric solution is suitable for a variety of applications found in sectors such as power generation, chemicals, petrochemicals, and the majority of other process industries. The sizes are designed for linear valve control with modulating duty, generally in remote locations, such as oil pipelines and remote gas extraction stations where power supplies are limited. Single-phase or DC electrical power is all that is required for control valve actuation.

Rotork, www.rotork.com

Eccentric plug rotary control valve

The K-Max eccentric plug rotary control valve incorporates cam action and low-friction plug operation for tight shutoff in a variety of flow control applications, including high- and low-pressure steam systems; clean, dirty, and corrosive liquids and gases; and erosive and abrasive slurries.

With bidirectional flow capability, the valve can handle mediums that are normally flowed to open and flowed to close. The plug action allows the plug to break free of the seat ring upon initial rotation of the shaft. The valve has a rangeability of 100:1 for precise throttling over a wide range of flows. It also has a self-aligning orbital seat, which allows orbital movement of the seat ring to provide self-alignment with the plug at assembly.

Leslie Controls, www.circor.com

Variable frequency drive

The ACQ580 variable frequency drive (VFD) for the water and wastewater industries optimizes wire-to-water or air efficiency. It also works to improve flow and reliability in municipal pumping and aeration applications.

The VFD includes elements that are specifically designed for municipal markets. For example, the pump clean feature dislodges debris from impellers, while the sensorless flow calculation provides flow measurement without a flowmeter. The soft pipe fill mode reduces water-hammer damage, while the quick-ramp protects submersible pumps. The ACQ580 is compatible with the company's Ability condition monitoring service, which gives customers real-time data about the status and performance of the monitored equipment from any location.

The VFD also has dry-run protection that prevents pumps from running without water and embedded PID controllers that automate flow, pressure, level, and dissolved oxygen. Multi-pump control manages operation of up to eight pumps simultaneously. The device also includes integrated safety features, such as safe torque-off and a maximum speed limit to protect against over speeding.

ABB, www.new.abb.com

Valve positioner

The Sipart PS100 is a positioner that can be initialized quickly at the touch of a button, automatically adjusting itself to the attached valve. If required, it is possible to optimize the positioner for a specific application with one further touch of a button. Just as some cameras have portrait, sport, or night mode, the positioner can be set to different modes for adjustment, open/close operation, and other applications.

The device is fitted with a display so users can see its status at a glance. With its four-button operation and Namur NE107 support, the device can be configured. The valve positioner is available in two enclosure variants: polycarbonate and aluminum. It uses contactless technology to detect the position of the valve. Equipped with a corrosion-resistant silencer, the device is suited to applications in the chemical and power sectors.

The Sipart PS2 has some new features. Optional pressure sensors improve the valve diagnostics and process monitoring, increasing the degree of utilization and availability of the plant. The positioner supports digitalization in plants. The company's valve monitoring app gives users all the information they need to follow a predictive maintenance approach by performing cloud-based analyses of valve data. It makes control and analysis options available to users so that they can detect when service tasks need to be carried out in good time before faults occur.

Siemens, www.siemens.com

Can stronger cybersecurity collaboration help us “future-proof” connectivity?

By Gary Williams

Cybersecurity is no longer an emerging trend or fad. It is an increasingly essential aspect of every business function and operation. This is especially true in industry. There is an increased demand for stronger cybersecurity and for initiatives, including the U.S. Cybersecurity and Infrastructure Security Agency Act and European Union Network Information System Directive and GDPR regulation. We know the demand has been amplified for industrial companies when legislation is coupled with mandatory requirements in standards like IEC62443 and ISASecure.

New legislation and requirements to remain compliant with prevailing standards mean end users must invest in technology, which can do more than help secure the operation. Today’s systems and solutions, especially in the age of the IIoT, can contribute additional operational value by increasing efficiency, reliability, and ultimately profitability. Obtaining and applying real-time data from connected assets, such as temperature, flow, pressure, and device status, to improve operations and business performance demonstrates the substantial value of connectivity.

But with such a wide variety of vendor systems and solutions controlling the operation, and because there is not a simple plug-and-play solution that covers every element of the operational technology (OT) environment, end users are fighting battles on multiple fronts: they must engage several vendors for solutions within their operations and connect and use those solutions to improve performance, all while keeping their operations safe and secure.

So, while adopting modern technology has many benefits, it has a downside too. Increasing connectivity expands the number of entry points for would-be attackers. Every new connection, no matter the medium, increases cyberrisk. In an OT environment, those risks can have potentially catastrophic consequences. In a cybersecurity breach, disaster can strike on several levels: interruption to production, damage to the environment, and even loss of life.

This means that as cyberthreats within the OT space increase, industry as a whole must collaborate more to future-proof all this connectivity. End users have to collaborate across their supply chains; providers need to collaborate with other providers. We must acknowledge that end users alone are not responsible for cybersecurity, nor can they face cyberthreats alone. Cybersecurity needs to be addressed by an array of stakeholders, including vendors, integrators, standards bodies, and governments.

Even though end users have to measure and mitigate risk, well-publicized, recent cyberattacks have shown that vendors need to work together to address ever-increasing threats. At a granular level, vendors are best equipped to measure the risk of connecting competing systems. If this risk is measured collaboratively by control systems and solutions vendors, it can be mitigated earlier in the supply chain rather than at the time of the FAT/SAT.

This collaboration must cross competitive barriers and unite the experts who develop standards and have the expertise to strengthen the cyber landscape, reflecting an understanding that cybersecurity goes beyond market share and the bottom line. Collaboration between vendors and other industry bodies will inevitably lead to a better understanding of how to reduce and mitigate cyberthreats, so vendors can ensure security is considered from concept to delivery. But the initiative cannot end there. It must also include IT systems and providers. For example, we must educate telecommunication and mobile device providers, so they too have a stake in helping secure the critical systems and mobile workforce that rely on communications infrastructure.

The financial argument for working together is compelling. Continual, better collaboration between and among end users and vendors, including IT and network providers, results in better, more secure business performance at the top and bottom line. Just think about this: In the GDPR-driven regulatory environment, a breach could result in fines of up to 4 percent of the global revenue or €20 million, whichever is higher. There is a simple, clear business case to be made for collaboration.

Continuously protecting every business function and operation from cyberattack has become a fact of life. That is not going to change. Therefore, it is time to think about new approaches that future-proof connectivity. All stakeholders must begin working openly together, not only to ensure end users become and remain compliant with legislation and standards, but so they can use all the great technology available to them to run a secure and profitable operation. If we are going to effectively leverage connectivity while continuously protecting our most critical operations from cyberthreats, we must unite to reexamine, develop, and reinforce best practices, policies, and procedures. The time is now. ■

ABOUT THE AUTHOR

Gary Williams (gary.williams@se.com) is senior director, cybersecurity services offer management, for Schneider Electric’s Industry business. He is responsible for cybersecurity guidance and support to a variety of external and internal stakeholders. Williams has more than 40 years of experience in designing and implementing communications networks for industrial, military, and law enforcement applications.

SOLA
Power Supply
SDN 5-24-100P
24 VDC / 5 A

Ignition®
by inductive automation
The Unlimited Platform for SCADA and So Much More
See the possibilities at inductiveautomation.com/ignition

Simplifying Edge Computing

from the Control Room to the Edge

Stratus ztC Edge

	Intel Core i7, 4 hyperthreaded cores
	32 GB
	512 GB SSD
	HDMI Ethernet: 4 x 1 GbE (2 available for user applications) USB: 8 x USB 2.0
	Stratus Redundant Linux (with virtualization)
	–40 to +60 °C (0 to +50 °C if using provided AC adapter)
	10% to 95%, non-condensing
	3 Grms (5-500 Hz: X, Y, and Z directions)
	280 mm (11.02 in) x 190 mm (7.48 in) x 76 mm (2.99 in)
	4.6 kg (10.2 lbs.)
	CCC, CE, FCC, ICES, RoHS, UL, VCCI
	DIN rail, wall, or table top
	9 to 36 VDC
	35W

OT and IT pros turn to ftServer because it's:

- **Simple** to deploy, manage and service with conventional or virtualized environments
- **Protected** with fault-tolerant operation and hot-swappable components
- **Autonomous** with self-monitoring and remote management

Learn more or request a demonstration today.

stratus.com/ft
800.787.2887