the journal
from Rockwell Automation PartnerNetwork™
JUNE 2021

Bad Maintenance Follows You Everywhere

Using data collection and analysis, you can move from reactive to proactive maintenance.

HOW ELI LILLY TRANSFORMED IT/OT TO DRIVE RESULTS

PID CONTROLLER TUNING SOFTWARE HANDLES COMPLEXITY

Q&A: LESSONS FROM THE COLONIAL PIPELINE CYBERATTACK

SPECTRUM CONTROLS

Universal Industrial Gateway

Enabling The Connected Enterprise

Use all 12 Protocols at the same time!

EtherNet/IP-PCCC

EtherNet/IP

Modbus RTU

Modbus TCP

Modbus ASCII

Hostlink

DF1-CIP

DirectNET

DF1-PCCC

CCM

PPI

S7comm (ISOTCP)

2nd Ethernet Port Added
Same Great Price

No Programming Software
No I/O Tree Changes
No Ladder Logic to Program

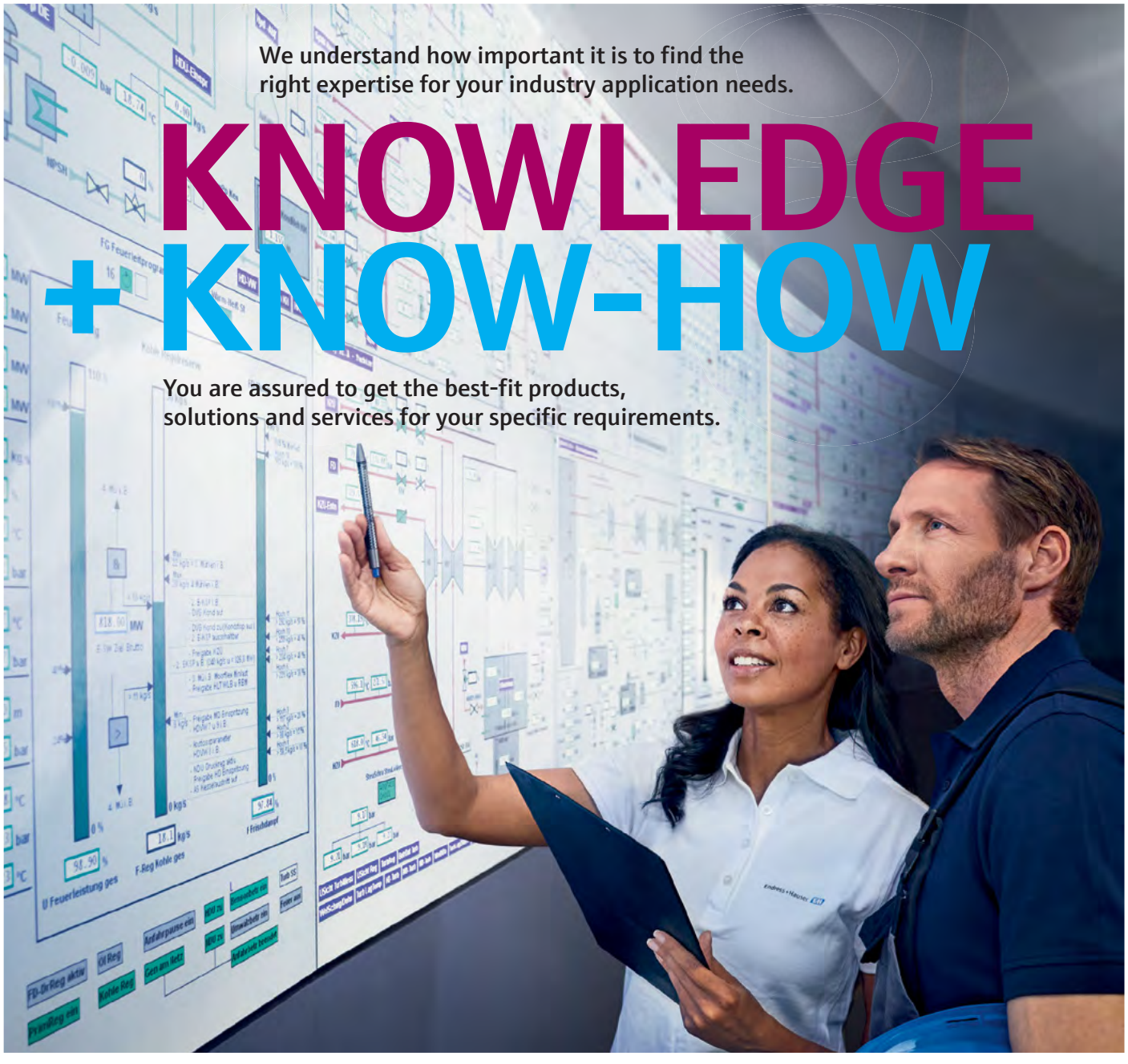
spectrum@spectrumcontrols.com
spectrumcontrols.com

SILVER Technology Partner
A ROCKWELL AUTOMATION PARTNER

We understand how important it is to find the right expertise for your industry application needs.

KNOWLEDGE + KNOW-HOW

You are assured to get the best-fit products, solutions and services for your specific requirements.



Micropilot FWR30 – The cloud connected radar level sensor

- Transparency – full and secure access to information on asset and inventory status, from anywhere at any time
- Simplicity – from procurement to operations, simplified commissioning, handling and processes
- Flexibility – suitable digital services defined by user needs, scalable from Netilion Value via Netilion Inventory to SupplyCare Hosting
- Reliability – precise measurement with wireless high-end 80Ghz sensor technology

Do you want to learn more?
www.us.endress.com/fwr30

Strategic Alliance
A ROCKWELL AUTOMATION PARTNER

Endress+Hauser
People for Process Automation

10

Bad Maintenance Follows You Everywhere

Using data collection and analysis, you can move from reactive to proactive maintenance.

INDEX

16

22

24

DEPARTMENTS

ADDITIONAL RESOURCES

VIDEO

Generation 3 Planetary Gearboxes Deliver Peak Performance

STOBER Drives shows the Generation 3 planetary gearbox series designed to provide peak performance. They're compact, provide improved machine performance, and can be paired with a geared motor.

https://youtu.be/rLKmk4vKrmQ

PODCAST

How Wearable Computers are Changing the Workforce

In this Automation Chat podcast, Andrew Chrostowski of RealWear shares how head-mounted devices are helping with workforce challenges, efficiency and safety. Also learn about typical applications.

https://youtu.be/FsrfGrcXR2E

FEATURES

the journal
from Rockwell Automation and our PartnerNetwork™

JUNE 2021, VOLUME 28, NO. 3

JOURNL-BR063A-EN-P

PutmanMedia®
1501 E. Woodfield Rd., Suite 400N
Schaumburg, IL. 60173, 630-467-1300

What Publishing & Maintenance Have in Common

As we were working on this issue's stories about maintenance and reliability, I realized publishing and industrial maintenance have an attribute in common: it's easy to spend a lot of time on unplanned tasks and "whack-a-mole" issues that pop up every day.

The types of issues we handle for publishing are different from industrial maintenance, of course — you don't have to pester an advertiser to send their advertisement materials before we submit the issue to the printer, or suddenly figure out a new printing schedule because of a paper shortage. In the maintenance function, you never know what will unexpectedly wear out, break down or jam.

Another commonality between publishing and industrial maintenance is that it's smart to understand these activities are necessary to the product's financial success. If those late advertisement materials don't come in, we can't run the ad, and we lose revenue. That's an example of an event we can't predict.

In industrial maintenance, you have the huge advantage of using condition monitoring to track equipment performance in real-time and predict machine failure so your organization can fix issues before they cause downtime. You'll learn a lot about the benefits of real-time maintenance data via the IIoT in this issue of *The Journal*.

One last thing, if you'll indulge me. In an effort to embarrass my boss.... congratulations, Mike Brenner, who has been promoted to Vice President in addition to his Group Publisher responsibilities. Very much deserved, indeed. You're the best, Mike.

Until next time...

Theresa Houck
EXECUTIVE EDITOR

News Noteworthy

System Integrators Win CSIA Awards

Several Rockwell Automation Solution Partners and Recognized System Integrators received awards from the Control System Integrators Association.




The Control System Integrators Association (CSIA) revealed its 2021 award winners during a virtual event held earlier this year. Four of the five honorees are Solution Partners and Recognized System Integrators in the Rockwell Automation PartnerNetwork™ program.

The 2021 Integrator Member of the Year Award was given to Omnicon S.A. from Cali, Colombia. The award recognizes a CSIA integrator member that has participated in the advancement of the association and profession.

The 2021 Rising Star Award was given to Jeff Winter, senior director, strategic initiatives of Grantek Systems Integration in Burlington, Canada. This award recognizes members who are relatively new to the field who have demonstrated attributes of a future leader, innovative approaches and commitment to the industry.

[from top down] Eduardo Acosta, Omnicon S.A.; Jeff Winter, Grantek Systems Integration; Joe Martin, Martin CSI; Keith Flaherty, Hallam–ICS

Joe Martin, President, Martin CSI, Plain City, Ohio, received the 2021 Charlie Bergman "Remember Me" Award. It recognizes individuals who have participated in association activities, published articles in industry publications, and served in leadership roles of the association.

The 2021 Social Responsibility Award was given to Hallam–ICS from South Burlington, Vermont. This award recognizes a member that has achieved extraordinary results in corporate social responsibility and sustainability programs.

Founded in 1994, the CSIA is a not-for-profit, global trade association that seeks to advance the industry of control system integration. Control system integrators use their engineering, technical and business skills to help manufacturers and others automate their industrial equipment and systems.

Rockwell Automation Announces CFO

Nicholas Gangestad has been named CFO and senior vice president at Rockwell Automation.

Nicholas Gangestad has joined Rockwell Automation as senior vice president and chief financial officer. He reports to Rockwell Automation Chairman and CEO Blake Moret.

Gangestad comes to Rockwell Automation after a long career with 3M, where he most recently served as the company's CFO and oversaw all aspects of the financial organization including compliance, financial planning, treasury and tax. Before his promotion to CFO in 2014, Gangestad served as 3M's chief accounting officer, corporate controller, and also held global financial management roles overseeing teams and developing talent in Canada, Latin America and Asia Pacific.

He received an undergraduate degree from Augsburg University in Minneapolis and an MBA from the University of Minnesota.

He replaces Steve Etzel, who has served as interim CFO since November 2020. Etzel is a 30-year company veteran who postponed his previously announced retirement to fill the interim role. He will retire after a transition period. ●

PARTNERNETWORK BRIEF

Claroty Names Rockwell Automation Partner of the Year. Rockwell Automation Digital Partner Claroty announced its inaugural Partner of the Year Awards, which recognize the top-performing partners that are having the greatest impact on the growing adoption of The Claroty Platform worldwide. Rockwell Automation won in the company's global region category.

Bad Maintenance Follows You Everywhere

Using data collection and analysis, you can move from reactive to proactive maintenance.

ROCKWELL AUTOMATION

Dave Mayer

SERVICES PORTFOLIO LEAD

If you're like most industrial automation maintenance professionals, you're trying to improve asset utilization to get more out of your company's already-made investments, while reducing risks and costs. You might be looking ahead to the ideal future state, where digital transformation allows all your plant operations to be connected to the enterprise.

Unfortunately, it's also true, if you're like most maintenance pros, that you're probably spending more time addressing unplanned downtime, excess inventory or a host of "whack-a-mole" issues that arise on a given day. Not to mention worrying about the potential of hidden threats hanging over the plant floor, such as legacy devices staring down obsolescence, back-ordered spare parts, depleting human resources and more.

The good news is, you don't have to be — and you don't have to do it all on your own.

Step #1. Get the Most From Your Operations

Creating an effective asset management strategy can help you improve asset availability, overall equipment effectiveness (OEE), and reduce your maintenance, repair and operations (MRO) spend. This entails evaluating three key areas — even at a baseline — to help you get ahead of issues before they arise so you can optimize your production assets:

1. **Assess:** Take an inventory of your assets to help you understand ongoing needs against surpluses and shortage.
2. **Plan:** Evaluate your most critical assets and greatest obsolescence risks to begin developing a modernization strategy.
3. **Manage:** Gauge the performance of your assets to mitigate potential unplanned downtime.

Using data collection and analysis, you can gain critical insights into your asset life cycle, inventory and overall plant operations.

Using data collection and analysis, you can gain critical insights into your asset life cycle, inventory and overall plant operations, to move from being reactive to proactive.

Consider this scenario. A large oil and gas company with several offshore platforms for drilling and exploration needed visibility into the obsolescence status of its equipment. The company conducted an initial Installed Base Evaluation™ (IBE®) to analyze its plant software and hardware assets, and their condition, to understand and pinpoint life-cycle risks by area, line, machine and panel.

Using the data-driven results, the maintenance team implemented a cost-effective maintenance, repair and

operations strategy for ongoing maintenance, and a timeline for spare parts and upgrades. This allowed the team to keep systems up and running smoothly, while mitigating equipment failure risks that could lead to unplanned downtime or worse.

Step #2. Prioritize and Plan

Taking those initial three steps can also help you prioritize urgent, medium- and long-term needs, whether in one plant or across multiple plants all vying for limited resources. You can more easily identify the proverbial low-hanging "increase operational efficiencies" fruit that offers high value with low effort to achieve. As a result, operations maintenance and engineering teams can align around a defensible MRO, modernization strategy and investment plan.

Without this asset modernization step, you risk taking measures before you're ready or when it's too late.

Take, for example, a recent case in which operations managers at a U.S. millwork manufacturer eagerly prepared to digitally transform their operations so they could glean data-driven insights to help maximize plant operations and inform enterprise-level decision-making. Surely, digital transformations offer companies untold advantages.

However, in this case, had the team skipped the IBE, they would have run forward with a dated network foundation replete with unmanaged switches and incapable of the information-enablement future.

Without proper planning, you risk taking measures before you're ready or when it's too late.

TRANSFORMING THE VALUE OF MAINTENANCE

With a combination of aging assets and pressure to increase efficiency and reliability, companies need to improve operations, better manage their workforce and cut costs. One area to look is maintenance.

Traditional maintenance has involved scheduled, hourly work on equipment, many times in reaction to something. When something failed, a new part was ordered, or a note was made on a clipboard to record the event. This type of reactive maintenance means increased costs and unscheduled downtime.

However, long considered a cost center, maintenance can drive profitability by improving quality, effectiveness, safety and other areas.

As a part of an overall asset management strategy, managing the maintenance tasks through specialized software and other tools can help reduce manual entry of device readings and share vital information with other production areas.

For example, information coming out of controllers, drives, switches and data centers can provide an alert about a failure or record the number of failures over a period of time.

Engineering, maintenance and storeroom personnel also can access historical data and know which assets might be nearing end of life, or be able to detect patterns in their equipment. They can see usage and costs, making them more efficient in managing labor, time and capital.

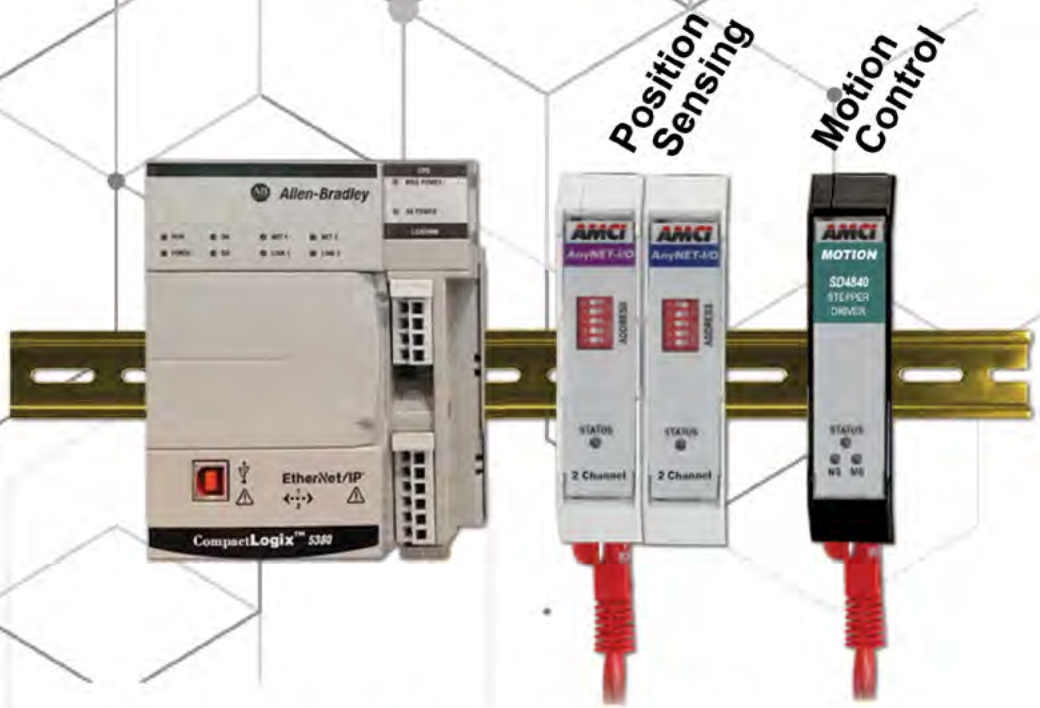
Average downtime of the asset, maintenance history and other factors can help to determine the best path forward for operational efficiency.

With smart, connected devices gathering information, maintenance managers can prioritize maintenance activities, proactively manage the condition and health of their assets and improve mean time between failures.

Using information to help monitor assets and manage operations is critical to balancing between reactive and proactive maintenance. To achieve efficiency, look at the amount of data you're entering into systems and remove the nonvalue-added labor involved. By being proactive, you can help reduce risk and help improve operational effectiveness.

PLC NETWORK PRODUCTS

for CompactLogix™ 5380



Position Sensing Resolver Interface
SSI Interface
PLS Controller

Motion Control Motion Controller
Integrated Stepper Drive/Controller

Specialty I/O Solutions for CompactLogix 5380
AMCI's networked specialty I/O modules provide versatile position sensing and motion control solutions for any PLC-based system; especially where no other solutions exist, such as with the 5380 CompactLogix. No additional software is required, as all programming is done using Studio 5000®. Call us at 860-516-8771 or visit www.amci.com to learn more!

SILVER Technology Partner
A ROCKWELL AUTOMATION PARTNER

PROUDLY MADE IN THE USA

AMCI ADVANCED MICRO CONTROLS INC.

It's important to put an ongoing asset performance management discipline in place.

As a result, the plant operation leads shifted gears to begin working with the financial operations team to first allocate resources to upgrade to managed switches. From there, they planned to embark on the fuller digital transformation journey and outlined the necessary steps to bring it to fruition.

Step #3. Anticipate and Prepare

Whether before or after a company completes an operational overhaul to support a digital transformation, it's important to put an ongoing asset performance management discipline in place. This should include:

- **Regular performance monitoring.**
- **Scheduled preventive maintenance.**
- **Calendared plans for replacing or upgrading software and hardware.**

It also assigns a single "source of truth" for operations and asset management in which all related information is tracked and shared across the organization for easy cross-functional access.

That Skills Gap

Beyond the current or near-term hardware and software needs of a plant, conducting these assessments can help you anticipate and address skills gaps. This includes meeting the needs of newly deployed innovations and moving closer to the ideal asset management future state in which information is collected and contextualized for use across the organization.

This connected, contextualized environment, in turn, can help drive more digital transformation as teams from the shop floor to the top floor gain access to insights, so you can stay proactive.

LISTEN TO THE PODCAST

How Wearable Computers are Changing Maintenance

In *The Journal* magazine's latest Automation Chat podcast, Executive Editor Theresa Houck talks with Andrew Chrostowski, Chairman of the Board and CEO of RealWear. Learn how head-mounted, hands-free, wearable tablet computers are helping with workforce challenges, including efficiency, safety, an increased number of remote workers because of the pandemic, and the retiring workforce.

They also chat about the role of the "connected worker," typical applications such as maintenance and operations, and how your work will change as wearable communications become more common in the next few years. Listen on your favorite podcast app or on the web at **http://bit.ly/tj21realpod**, or watch their chat on YouTube at **https://youtu.be/FsrfGrcXR2E**.

Time to **Step Forward** for Smart Manufacturing

If your machines can GET *SMARTER*, why not?

Machines with **CompactLogix™ 1769-L3x** or **CompactLogix 1768-L4x** control systems can step forward with easy migration to a **CompactLogix 5380** control system.

Besides getting smarter, your system gets more productive and flexible with:

- High-performance 1 Gb network flexibility with Dual-IP mode
- Integrated motion control on EtherNet/IP™ for up to 32 axes
- Increased capacity, enhanced security and expanded diagnostics

What's more? Your migration experience is made even easier with serial communication support. Plus, you can design and configure in the same development environment, Studio 5000 Logix Designer® application.

Step forward to **rok.auto/CompactLogix5380**

Allen-Bradley
by ROCKWELL AUTOMATION

FIIX,
a Rockwell Automation Company

Marc Cousineau

4 Steps to Efficient Condition-Based Maintenance

With the right systems, processes and procedures in place, maintenance teams can use this predictive strategy to build a sustainable operation.

Equipment failure is not a single event — it's a process. This concept means that breakdowns are both a journey and a destination, and it has become firmly established in the realm of maintenance best practices. Condition-based maintenance (CbM) can act as a guide on the road to failure and back.

What is Condition-Based Maintenance?

CbM is a predictive maintenance strategy where the performance of an asset is observed and measured in real time to identify and prevent deterioration and possible failure at the earliest possible moment.

Under CbM, maintenance only occurs when data indicates a decline in performance or the early warning signs of failure. This differentiates CbM from preventive maintenance, where tasks are performed at regular intervals.

Because CbM is based on collecting and analyzing data, it can be used to build a great predictive program, identify trends in asset performance, and assess where an asset is in its life cycle. This makes it easier to make informed decisions on everything from scheduling and labor to budgeting.

4 Steps to Using CbM More Effectively

Using CbM is one thing. Using it effectively is a whole other story. If you don't have the right systems, processes and procedures in place, CbM can cost you more time, money and goodwill than it's worth.

Here are four steps maintenance teams can take to better harness the power of CbM and build a sustainable operation around condition monitoring.

Step 1: Map Out Your Assets, Failure Modes and Baselines

Before implementing CbM, you must understand everything about how your equipment functions so you can properly calibrate sensors, spot problems as soon as possible and prescribe the right cures.

First, map out all your assets and their possible failure modes to understand if each piece of equipment has the key ingredients for CbM. The first ingredient is a condition that can be monitored. Condition monitoring doesn't work for every asset, so knowing which ones don't support sensors or other monitoring tools and techniques can save you time and money later.

For the remaining assets, determine if the failure modes identified by condition monitoring can alert you to a problem with enough time to fix it in a cost-effective way. If the answer is yes, the asset is likely a good candidate for CbM.

Once you have your group of qualified assets, set baselines for normal operation. Baselines are the established thresholds that indicate a healthy and fully functional system. For example, the baseline vibration frequency for a bearing might be 1,000 Hz to 2,000 Hz. Any number between those two frequencies means the bearing is operating at its optimal level. If it reaches above 2,000 Hz or below 1,000 Hz, it could signify a problem.

Baselines can be established in many ways, from manufacturer recommendations to historical trends. Creating baselines for each system takes the guesswork out of CbM and makes your decisions more effective.

Step 2: Understand and Use the Potential Failure (P-F) Curve

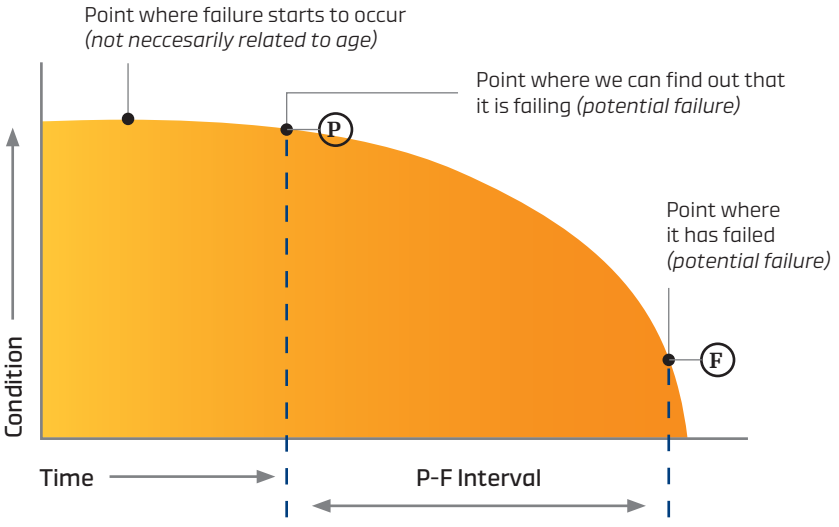
Talking about CbM without the P-F curve is like talking about a car without wheels; it just doesn't work.

The P-F curve (see Illustration) demonstrates the relationship between a breakdown, its cost, and how it can be prevented. It's based on the fact that equipment might be in the early stages of failing even if seems to be working fine.

Along the X-axis of the curve is time. As you move through time, the machine moves from the point of potential failure to the point of actual (functional) failure. There are also instances when faults can be detected before total failure.

Along the Y-axis is the machine's condition. The machine progresses from top working condition to point of failure, and then down from there until actual failure.

The most important part of the P-F curve is the P-F interval. The P-F interval is the time between an asset's potential failure and its functional predicted failure. For successful CbM, you must verify your inspection intervals are smaller than the P-F interval so you can catch a failure after it's detectable, but before it actually occurs. Fine-tuning your maintenance intervals is also crucial to optimizing CbM.



The P-F curve and P-F interval help to determine how often you should complete a condition-based maintenance task.

Understanding the P-F curve and the P-F interval is key to building an efficient CbM strategy. The P-F curve and P-F interval help to determine how often you should complete a CbM task. The frequency of maintenance is reduced, as are the costs and time commitments associated with maintenance.

Step 3: Use Maintenance Technology

CbM combines recommended guidelines with repair and performance data to determine what tasks need to be completed and how often. When these parameters are decided, maintenance software can help you get a head start on everything from logging sensor data to triggering work orders and scheduling maintenance.

Integrating your existing production technology, like your manufacturing execution system (MES), programmable logic controllers (PLCs), SCADA and asset sensors, with maintenance software, such as a computerized maintenance management system (CMMS), helps reliability engineers, maintenance managers and technicians capture, organize and analyze information much easier, quicker and more accurately.

This also allows you to automatically trigger a work order when certain measurements fall outside the established baseline. For example, you can set up a CMMS to schedule maintenance on a filter when the differential pressure exceeds 20 psi. This way, maintenance can be scheduled at the most appropriate time, reducing the likelihood of failure while maximizing resources.

Optimized inventory purchasing is another byproduct of using maintenance software to manage CbM. Because

Understanding the P-F curve and the P-F interval is key to building a CbM strategy.

SMC
Automation·Controls·Process

IO-Link Compatible Products

IO-Link

SMC is providing the point to point digital connections to meet your communications protocol requirements.

High Precision
Digital Pressure &
Vacuum Switches

High Precision Digital
Pressure Switches
for air and fluids

Electro-Pneumatic
Regulator

Digital Flow
Switches for water

Actuator Stroke
Position Sensor

Fieldbus SI Unit for
Control Valves

IO-Link Base for
EX600 SI Unit for
Control Valves

Step motor Controller
for Electric Actuators

Providing Sustainable, Energy Efficient and CO_2 Reducing Components for Industrial Automation

SMC Corporation of America **800-762-7621**

SMC Automation Canada Ltd. **800-762-7621**

Email: sales@smcusa.com

www.smcusa.com

www.smcautomation.ca

Energize Your Efficiency

SILVER
Technology Partner
A ROCKWELL AUTOMATION PARTNER

software can track work order history and create reports on parts usage, it makes it easy to adjust inventory levels so you're only ordering the parts you need, when you need them. Not only will the parts always be on-hand (thus minimizing downtime), but inventory prices can be cut.

Step 4: Create a Solid Training Program for Staff

While CbM relies heavily on technology and automated systems, like sensors and software, a human element always is involved. For your CbM strategy to be as efficient and effective as possible, all members of the maintenance team must be properly trained on the concept of CbM, its benefits and how to use the systems. This will increase buy-in, reduce user error and increase reliability throughout the process.

Training should include a thorough breakdown of the different types of condition monitoring and how they affect each asset at your facility. It should also be clear how every member of the team can confirm sensor data is logged correctly and how resulting maintenance tasks should be treated.

It's a good idea to create an asset management policy at this stage of CbM implementation. This will help not only the maintenance team, but also everyone in your facility understand how CbM impacts the organization as a whole and their place in helping the strategy work to its full potential.

Are You Ready?

Like any tool or strategy, CbM isn't a silver bullet. There will still be random, unpredictable breakdowns. But these failures can be the exception instead of the norm with a well-executed CbM program.

That takes three key ingredients: people, processes and tools. Everyone at your facility needs to think and act proactively. Processes need to be set up to catch failure and act on it quickly. And you need the technology to be able to monitor asset conditions accurately and relay this information from one piece of software to another. When you have all three, you'll be set for success. ●

50 YEARS CENTERLINE® MOTOR CONTROL CENTERS

CENTERLINE®

Motor Control Centers

CONTINUOUS INNOVATION | CONTINUOUS IMPROVEMENT | CONTINUOUS INTEGRATION

Build a wall of CENTERLINE MCCs around
CENTRAL PARK
NEARLY 600 FEET TALL

Create a continuous line of CENTERLINE sections
FROM NEW YORK CITY TO TORONTO
ALMOST 500 MILES LONG

WITH WELL OVER
A MILLION SECTIONS SOLD
YOU COULD

Enclose the
BURJ KHALIFA TOWER
TO A HEIGHT OF ALMOST 2 MILES

Stack CENTERLINE sections vertically to reach the
INTERNATIONAL SPACE STATION
over 8 times or
ALMOST 2000 MILES

1971 •

CENTERLINE **2100**

CENTERLINE **1500**

CENTERLINE **2500**

• 2021

The smart choice for **SMART MANUFACTURING** for over **50 YEARS**

Rockwell Automation

ROK.AUTO/MCC

How Eli Lilly Transformed IT/OT to Get Results

Global pharma company's well-established IT/OT cooperation is key to its cybersecurity, serialization, analytics and other digital transformation efforts.

While many companies are in the midst of breaking down barriers between their IT and operational technology (OT) organizations to create smarter production operations, Eli Lilly and Co. started that process more than a decade ago.

Indianapolis-based Eli Lilly, a global healthcare leader with products marketed in 120 countries, has long fostered a willingness to continually improve and adapt digital technologies. Central to its digital transformation journey is its strong partnership between IT and OT.

Here's a look at how this IT/OT collaboration evolved and is driving the company's serialization, cybersecurity, analytics and other digitization efforts.

Decades-Long Journey

Eli Lilly and Co.'s path to IT/OT convergence began in the 1980s and 1990s, when the boundaries of IT and OT started to expand and overlap.

Leadership later realized what matters isn't who reports to who, but rather how teams interact.

For example, IT solutions expanded from financial and data processing to address transaction-management requirements on the manufacturing floor. And process automation expanded from proprietary, stand-alone digital controllers to integrated networks running on IT hardware.

In the early 2000s, the company's manufacturing operations experienced incidents resulting directly from conflicts, gaps and overlaps between OT and IT domains. These incidents led to issues like production stoppages and cost-overruns for solution deployments.

Initially, process automation was moved from the engineering organization to the IT organization. But leadership later realized what matters isn't who reports to who, but rather how the teams interact.

Actions were taken to better define areas of responsibility and implement shared governance. Engineering leaders joined the IT lead team, while IT senior directors were aligned with engineering senior directors. IT also assumed responsibility for providing manufacturing network services and server support, while engineering assumed responsibility for areas such as process control software and logic.

"In the last 10 to 15 years, we really have started to partner together, whether it is on life-cycle management projects and upgrades that we're doing, or in identifying new technologies and new places where we want to move forward," explains Dave Sternasty, vice president of corporate engineering and global health, safety and environment (HSE) at Eli Lilly. "I would say that the partnership between IT and OT is really strong and is one of the things that we see as a key to our success."

The Power of Collaboration

Eli Lilly has been benefitting from its IT/OT collaboration since the early 2010s. For example, IT and OT collaborated to develop an understanding of industrial cybersecurity risks, a plan to mitigate immediate risks and an ongoing strategy for best-available protection.

The IT/OT partnership also helps drive the company's global serialization program, which stewards a global solution to provide regulatory-mandated traceability for all final product units. The solution converges IT and OT domains by integrating vision systems, high-speed control, event management systems and ERP systems.

"We also now are capturing a tremendous amount of data across our supply chain tied to the serialization solution," notes Karen Harris, vice president and information officer, manufacturing and quality, Eli Lilly and Co. "And we're really looking at ways to take advantage of that data and turn it into information to make better decisions."

The company also is modernizing its data and analytics architecture. This involves incorporating critical capabilities such as cloud, edge storage and computing, and the Industrial Internet of Things (IIoT).

"We're really at the crux of shop-floor data and the integration of IT/OT information at the shop-floor layer, and being able to turn that data into information to make better decisions whether that be on the shop floor or in our labs," Sternasty says.

What's Next?

The pharma company expects it will take at least 10 years to fully realize its digital-transformation vision across its major sites. This includes an aspirational goal of having a predictive plant by 2023.

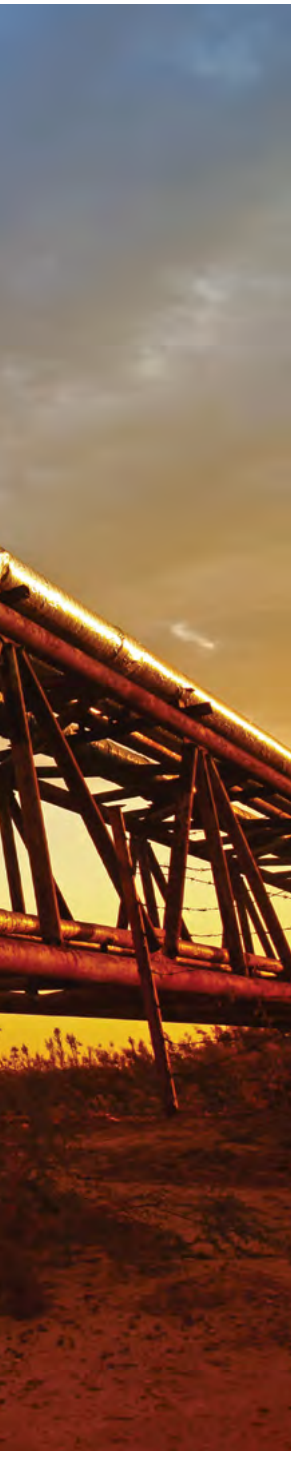
To help with technology implementations both at the strategic and execution levels, the company engages its core collaborators like Rockwell Automation and its Strategic Alliance Partner Microsoft, among others. It also is focusing on hiring and developing workers who are digitally empowered.

And of course, continuing to develop and build on the strong partnership between IT and OT will continue to be central to the company's digital transformation.

"We've had this relationship in place for years," Harris says. "And actually, it aligns with our broader Team Lily approach, where we believe it's the cross-functional teams and cross-functional relationships that really drive success. And it's that teamwork that helps us advance our agenda." ●

Q&A: Lessons from the Colonial Pipeline Cyberattack

Editor Theresa Houck talks with a cybersecurity expert about what manufacturers and infrastructure utilities can learn to help fortify their networks.



THE JOURNAL
From Rockwell Automation and Our PartnerNetwork

Theresa Houck

EXECUTIVE EDITOR

The ransomware attack that shut down the Colonial Pipeline on May 7, 2021, is considered the most impactful cyberattack against U.S. critical infrastructure to date, but it's not the only one. Many infrastructure and manufacturing facility cyberattacks occur that we don't hear about.

To find out what we can learn from this and other incidents, I spoke with Grant Geyer, chief product officer at Claroty, a leading industrial cybersecurity firm and a Rockwell Automation Digital Partner. We examined how the Colonial Pipeline ransomware attack happened, as well as how the February 2021 Oldsmar, Florida water treatment cyberattack occurred, and the far-reaching effects.

This Q&A also reveals lessons our industry can learn about cybersecurity to help the oil and gas industry, critical infrastructure facilities and all manufacturers.

You can listen to our conversation in our "Automation Chat" podcast on your favorite podcast app or on the web at http://bit.ly/tj21claropod, or watch our chat on YouTube at https://youtu.be/rFxa2-wyquw.

Theresa: Describe what happened with the cyberattack that shut down Colonial Pipeline.

Grant: A piece of ransomware found its way into Colonial Pipeline's IT environment. Colonial Pipeline also shut down parts of their OT environment that stopped the transmission of fuel to the U.S. East Coast.

I've seen many attacks on the IT side of the environment. But this is one of the most impactful attacks that happened in the cyber world affecting events in the *physical* world. It led to the pipelines being shut down, which led to gasoline shortages, which led to people trying to horde gasoline, which led to skyrocketing prices.

This is one of the first events that impacts the company itself, other businesses because of the fuel supply chain, consumers in terms of the cost of fuel, and the U.S. government from supply chain and critical infrastructure perspectives.

On the technical side, this is not just a ransomware attack, but a **targeted** ransomware attack. A group known as DarkSide tries to legitimize itself by appearing like a pseudo-legitimate business, but the reality is that this is a criminal gang that allegedly operates outside of the Eastern Bloc countries.

They figure out a target they want to go after, intimidate the target, put ransomware on their machines, and before locking up the systems, they'll steal the data. If a company has a good backup, a recovery program in place, and they can restore the data, the DarkSide group still has that data and can release it bit by bit onto the Internet to continue to raise the stakes around the release of sensitive information.

Theresa: Critical infrastructure is an easy target. For example, another high-profile one occurred in February at the Oldsmar, Florida water treatment facility. Talk about what happened there.

Grant: That's an interesting case. A small water utility that leveraged a third-party tool for remote access called TeamViewer was all of a sudden connected by someone outside of the environment. And an asset operator noticed water levels were changing from 100 parts per million by volume drinking water to over 11,000 parts per million. And that is a lethal amount for consumers.

Initially, the operator thought it was a mistake or that he was being tested, and

KEY LESSONS LEARNED FROM THE COLONIAL PIPELINE CYBERATTACK

1. **Engage asset operators as the first line of defense.** They know what's going on in real time.
2. **There are other entry points for cyberattacks besides coming into the IT network**, including remote access points (remote workers).
3. **With converged OT/IT architectures, it's important to have virtual zones, microsegmented environments, and zero-trust network architectures.** These let users get to the assets they need, but you can prove they're who they claim to be and that they have the rights to access those assets.
4. **Air gap is not the answer.** When done in a secure way, you can benefit from emerging technologies and digital initiatives.
5. **Understand that it's a journey.** Know your inventory of assets and which are vulnerable. It's a long game of reducing the inherent risks of those assets, and then monitoring for threats for the residual risk that remains.
6. **Make sure your remote access is *secure* remote access.**
7. **Conduct tabletop exercises.** Ask, "What if what happened to Colonial Pipeline happened to us?"

he fixed it, but then it happened again. He literally saw the cursor moving across his screen and saw the levels being changed. This demonstrates how important it is to engage the asset operators as the first line of defense.

The second lesson is that often, we think cyberattacks that will come in from the IT side of the network and then go through the IT/OT bridge to try to compromise OT assets. But there are other entry points. This breach was a case where, because of the need for remote connectivity — especially during the pandemic — [remote worker access] provided access for attackers.

Theresa: Does the convergence of IT and OT make it *more* or *less* vulnerable to cyberattacks?

Grant: That's an interesting question because historically, OT environments were air-gapped from IT environments. I once heard that an air gap is a low-latency network, meaning that if business needs to happen, people will figure out a way of connecting the environments.

The advantages to be gained through digital transformation and convergence, whether they're in the public or private sector, are too high to be ignored. The key is how organizations do it safely and securely with safe architectures.

We're going to see a lot of converged OT/IT architectures where it will be important to have virtual zones, microsegmented environments, and what are known as zero-trust network architectures. These let users get to the assets they need, but you can prove they're who they claim to be and have the rights to access those assets.

Theresa: What are other lessons learned not just from these two high-profile incidents, but also from the many cyberattacks we don't hear about in the headlines?

Grant: What is clear for any asset owner or operator is that you're going to have a variety of brownfield equipment that can't be easily replaced due to technology obsolescence periods. It may not be patchable due to maintenance windows.

So, it's clear that air gap is not the answer. You need to benefit from digital transformation efficiencies, but it needs to be done in a secure way.

Another lesson is understanding that it's a journey. Know your inventory of assets and which of those are vulnerable. It's a long game of reducing the inherent risks of those assets, and then monitoring for threats for the residual risk that remains.

A third lesson is how important it is to make sure your remote access is ***secure*** remote access. Make sure a users' credentials to get into the environment can't be stolen by cyberthieves.

And finally, conducting tabletop exercises are important. Ask yourself, "What if what happened to Colonial Pipeline happened to us? How do we respond? Do we have backup and recovery? Do we have a policy about whether we would pay ransomware or not? Who are the officials that we would need to talk to within the U.S. government? Do we require multi-factor authentication?"

Theresa: What else do you want industrial automation professionals to understand about cybersecurity?

Grant: The most important thing that I've seen in successful initiatives in OT security is recognition that it's a team sport. It starts with an understanding of the mutual context between IT and OT. At the fundamental level, the least common denominator for both teams is managing risk.

It's getting to an understanding of what the differences are, what the organizations have in common, and through the different experiences, shared initiatives and shared goals, developing a strategy. That's where the magic happens — working together and asking, "How do we win together to manage and mitigate risks knowing this very lethal threat environment that we're dealing with?" ●

LISTEN TO THE PODCAST

Lessons from the Colonial Pipeline Cyberattack & Steps to Take

The ransomware attack that shut down the Colonial Pipeline on May 7, 2021, is considered the most impactful cyberattack against U.S. critical infrastructure. In this "Automation Chat" podcast episode, Executive Editor Theresa Houck talks with Grant Geyer, Chief Product Officer at Claroty to examine how the Colonial Pipeline breach happened and its impact.

Also learn about an asset operator's role as the first line of defense; how converged IT/OT networks are vital for ICS efficiency, but also increase the attack surface available — and what to do about it; what comprises a well-thought-out cyberdefense; lessons learned that are useful for every industrial firm and critical infrastructure facility. And more.

Listen on your favorite podcast app, on the web at **http://bit.ly/tj21claropod**, or watch our chat on YouTube at **https://youtu.be/rFxa2-wyquw**.

CLAROTY

Guilad Regev

SENIOR VICE PRESIDENT OF CUSTOMER CARE

Tips for Setting Up a Converged IT/OT Security Operations Center

Achieve greater security monitoring and better visibility across the enterprise and threat mitigation by presenting a unified front against cyberthreats.

EDITOR'S NOTE This article is adapted from the white paper, "5 Essential Steps for a Converged IT/OT SOC." Download the full paper at http://bit.ly/tj21wpclaroty to get detailed information about what having a converged IT/OT security operations center (SOC) accomplishes; how to align with your firm's existing cybersecurity abilities; how to improve visibility into assets, the network and processes in the OT environment; traits and duties of a cybersecurity site leader; and how to establish a product security incident response team (PSIRT).

While OT requires specific tools for industrial cybersecurity, one area where enterprises can use their existing resources and personnel is the security operations center (SOC). The best industrial cyberdefense strategy is to present a unified front against threats to IT and OT assets by establishing a converged SOC that protects these once-separate technology environments in a holistic manner.

The SOC already is widely accepted as a hallmark of mature IT security programs. By consolidating OT security with your existing IT-centric SOC, you can achieve greater visibility across the entire enterprise, enhanced security monitoring and comprehensive threat mitigation.

Tip #1. Achieve Optimal Alignment with Existing Capabilities

Since maximizing return on investment (ROI) is one of the key advantages to a consolidated IT/OT SOC, it's important to use your existing cybersecurity infrastructure as much as possible. This requires a thorough assessment of current capabilities to identify areas in which tools already at your disposal can be used, while zeroing in on gaps that will require new solutions in order to be addressed. It's important for these new solutions to be compatible with existing IT security tools as much as possible. When evaluating potential technology integrations for your SOC, assess alternatives based on the value and functionality they deliver.

A strong, centralized ecosystem of integrations can reinforce ease of maintenance and upgrades, while also allowing automatic health checks and monitoring. Integrations also allow incorporating existing standard operating procedures (SOPs) and other playbooks into the converged IT/OT SOC.

Tip #2. Gain Visibility Into IT and OT Security Alerts Within OT

With increased interconnectivity to IT networks, OT environments are exposed to IT-centric cyberthreats from which they were previously isolated. Over the past several years, cyberattacks such as WannaCry and NotPetya wrought havoc upon OT environments globally. They've led to increased awareness of the need to detect the cross-proliferation of IT cyberthreats within OT environments.

Cyberthreats to OT typically enter the enterprise technology environment via the IT network before moving laterally to compromise OT assets. Given this typical infection pattern, it is crucial to have unified visibility across IT and OT environments.

Because SOC personnel already are trained to handle IT security alerts, it's often the case that only minimal changes need to be made to existing playbooks to make them applicable to OT. And because your team likely has existing access to IT security technologies capable of detecting IT cyberthreats, all that's required of this step is to make sure those abilities are applied properly to your OT environment.

Once your SOC has visibility into IT security alerts, the next task is to gain visibility into OT-specific alerts. To effectively monitor and defend against threats to their organization's OT environment, IT security teams need purpose-built technology that delivers detailed, real-time visibility into industrial assets, networks and processes.

Tip #3. Designate a Cybersecurity Leader for Each Site

Likely the most involved step, depending on the number of sites your team is responsible for securing, will be the need to designate an OT cybersecurity site leader (CSL) at each of your organization's physical OT sites. This person will serve as the eyes and ears of your converged IT/OT SOC for that location.

The CSL for each facility will be a critical liaison between OT personnel and the SOC. In contrast with the IT/OT cybersecurity program manager role, which involves a great deal of strategic leadership, the CSL role is an additional responsibility taken on by a designated on-site staff member to serve as a point person in the event of an incident.

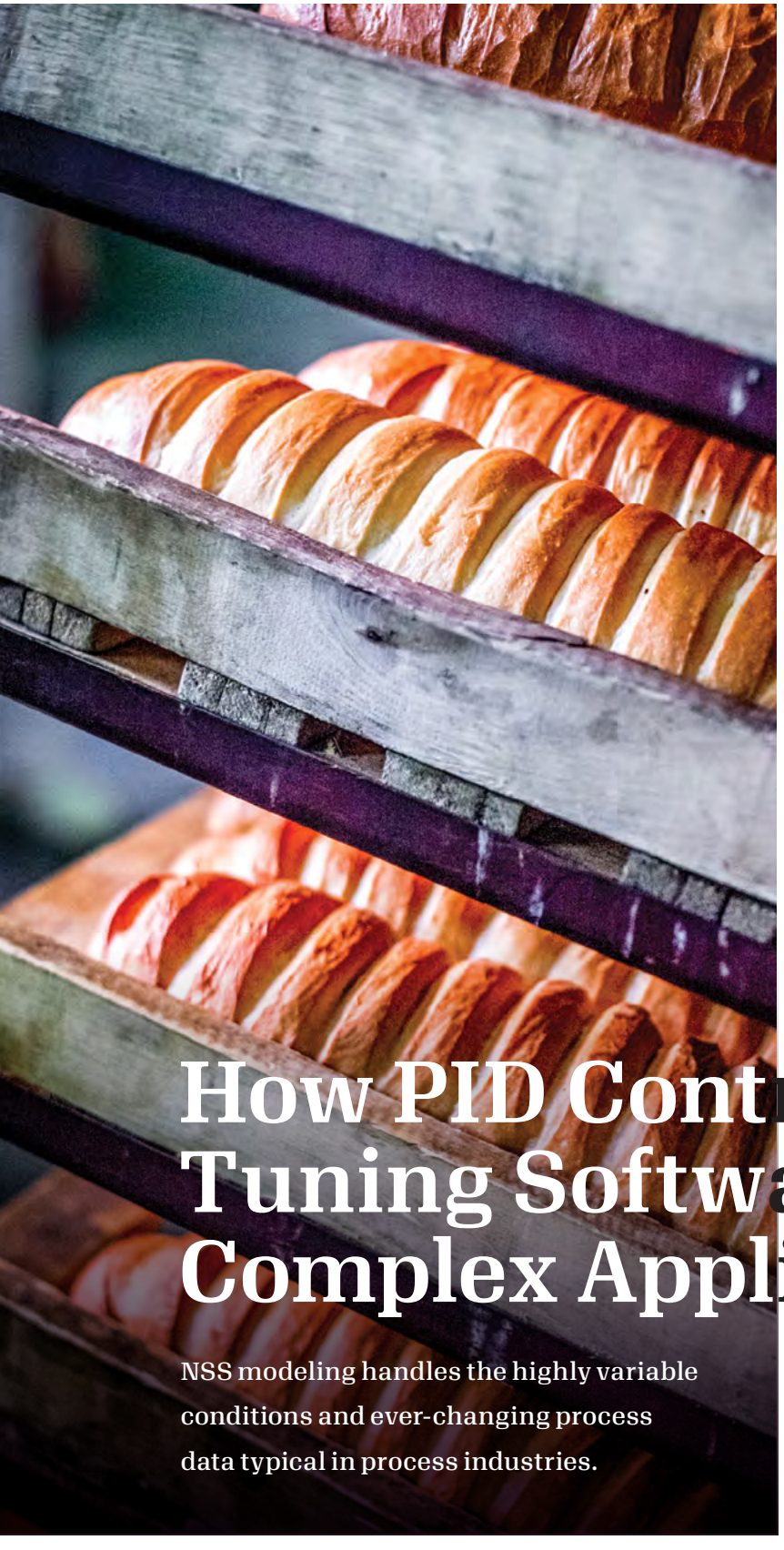
The CSL must be knowledgeable about SOC procedures, requirements and objectives — or alternatively, undergo thorough education and training on these subjects. The CSL also must be able to speak the language of plant stakeholders and understand their roles well enough to work with them effectively to resolve critical issues.

This responsibility typically can be assumed by an existing staff member and handled with their existing work responsibilities. The CSL must be prepared to lead rapid response, coordinating with SOC and site-specific OT personnel.

Manage That Risk

A converged IT/OT SOC is necessary for managing risk effectively within industrial environments. The ease, effectiveness, cost efficiency, and speed at which they can be implemented depends on having a well-thought-out plan.

CLAROTY Based in New York City, Claroty is a Rockwell Automation Digital Partner. The company provides comprehensive cybersecurity solutions for industrial control systems (ICSs) to help users reveal, protect and manage their OT, IoT and IIoT assets.



CONTRIBUTED BY

Control Station, Inc.

Today's proportional integral derivative (PID) controller tuning software helps process manufacturers by modeling the noisy, oscillatory process data so manufacturers improve throughput and efficiency. Typical process data is highly dynamic, so it has caused tuning products, from integrated auto-tuners to aftermarket products, to fail. It has also caused some users to subsequently swear off tuning software altogether. But here's what users should know who still believe manual tuning is the best option.

EDITOR'S NOTE This article is adapted from the white paper, "Aggregated PID Data Provides Process Manufacturers with New Insights into Control Loop Performance." Download the full paper at http://bit.ly/tj21stationwp to get information about new opportunities for process optimization by using control loop performance monitoring and data analytics. The paper includes references to studies about PID controller tuning software and information about the future of analytics.

How PID Controller Tuning Software Handles Complex Applications

NSS modeling handles the highly variable conditions and ever-changing process data typical in process industries.

Purpose of Tuning Software

Tuning PIDs controllers typically begins with calculating a process model using step test data. A good model should accurately describe three key characteristics of a process' behavior: how far, how fast and how much delay.

- The **how far** variable, also known as Process Gain, describes how far the Process Variable travels in response to a change in Controller Output.
- The **how fast** variable is also known as the Process Time Constant, and it describes how quickly the Process Variable moves in response to a change in the Controller Output.
- Process Dead-Time is the variable that represents **how much delay** exists in a process. More specifically, Dead-Time is the delay that occurs after a change in Controller Output is first initiated until the time that the measured Process Variable begins to respond.

Users look to software to tune PID loops that exhibit challenging, highly variable characteristics. But software has historically required users to steady a loop's behavior before the software can function properly.

Nearly all automation software vendors agree on the need for a steady or "quiet" process before their prescribed tuning procedure is initiated. What isn't stated clearly is that those same products can only produce positive results after the prework of steadying that very same process is completed by the software licensee.

When it comes to tuning PID loops, most with experience would argue that steadying a process is the hard part. If achieving a steady-state was easy — let alone feasible — then manual tuning methods would suffice. By requiring users to do the hard part of tuning, then the value of software is justifiably called into question.

The objective of tuning software should be to make optimization possible for most loops that are inherently variable. From a practical viewpoint, that means that software should simplify the procedure by which loop dynamics are modeled and new parameters are calculated.

Further, software should be able to accommodate the complexities that the average user can't with the use of pen and paper alone. Indeed, those challenging loops provide the justification for an investment in software.

Non-Steady State Modeling

Non-steady state (NSS) modeling was first coined in 2008 with the introduction of the NSS Modeling Innovation™. This involves a proprietary method for modeling a PID control loop's dynamics. While dynamic tests such as the step, bump and doublet are still required, the innovation eliminates the steady-state condition that had been universally required prior to the start of testing.

Regardless of the process type, software equipped with NSS modeling can accurately model loops that demonstrate oscillatory behavior. Similarly, noise and long Dead-Time are no longer limiting factors.

Industry Implications

What does NSS modeling mean for food and beverage manufacturers and other process manufacturers?

First, it eliminates the burden of steadying a process. Software equipped with NSS simply requires bump test data that includes Controller Output and Process Variable signals distinct from any apparent noise in the process. That factor alone dramatically reduces the time and effort involved with tuning a plant's PIDs.

Now consider critical loops such as fermentation and batch temperature where steadying the process is viewed as a nonstarter. Those usually are the loops deemed too financially important or too technically challenging to be subjected to a software program's steady-state criteria. With a similarly distinct bump test, the performance of these loops can finally be improved efficiently with NSS modeling.

Lastly, consider processes characterized by exceptionally large Dead-Time or Time Constant values, such as pasteurization temperature and pH control loops. It might be understandable that a requirement for steady-state to steady-state testing would exceed the patience of most operational staff members, but that shouldn't be the case with software. Exceptionally slow systems consistently foil the modeling capabilities of traditional tuning software products. ●

CONTROL STATION, INC. Control Station, a Rockwell Automation Technology Partner, offers the LOOP-PRO Tuner software that simplifies tuning of PID controllers, and PlantESP for monitoring plant-wide performance of control loops.

SOFTING INC.

No-Config Networking Communications Modules for OT

Do you have legacy PLCs? Do you need to extend the life of your Rockwell Automation legacy networks? Softing has networking, in-chassis, communications modules for ControlLogix®, CompactLogix™, and even SLC 500™ and PLC-5®. When you need to keep legacy protocols alive, such as Remote I/O, ControlNet®, Genius, Modbus™ and Data Highway, Softing has no-config communications modules designed for OT, not IT.

https://bit.ly/32ofK6u

ADVANCED MICRO CONTROLS INC.

Integrated Servo Motor Offers Safety Features

AMCI's SV160E2 integrated servo motor includes Safe Torque Off, enabling increased safety across applications, and preventing unintentional starting or motion. It reduces system costs by eliminating the need for separate components. Move commands are programmed through Studio 5000®. EDS files and sample programs help streamline initial setup and programming. It features dual port EtherNet/IP™ networking with DLR, built-in web server, absolute encoder and virtual axis follower.

http://bit.ly/2mvdulf

HARDY PROCESS SOLUTIONS

New Hardy Caseweigher for QA with Rockwell Automation PLC

Hardy's all new Caseweigher machine is designed for simplicity using off-the shelf components and a CompactLogix® PLC control platform with Studio 5000® to use data across The Connected Enterprise. Hardy's 4050CW Checkweight controller samples at 4,800 times per second to provide extremely accurate and fast weight data with a full statistics package.

https://bit.ly/3znJMXc

HMS NETWORKS

Unlock New Services with Your Machine Data

The Ewon Flexy 205 is an advanced internet data gateway from HMS Networks that allows monitoring and collection of data for analysis and predictive maintenance. With data logging, alarming, built-in web interface, scripting and enhanced Internet connectivity, it is a versatile internet gateway for your IoT deployment.

www.ewon.biz/products/ewon-flexy/flexy-205

SYTECH INC.

XLReporter from SyTech

XLReporter gets the information you need, in the report you want with no programming. Built with Microsoft Open Office standard, it is the first reporting platform in industry to deliver workbook technology to an automated environment. Within minutes, reports are ready to view/email as workbooks, PDF and web pages. It interfaces to FactoryTalk® Linx Gateway, FactoryTalk Historian SE, PanelView™ Plus, OPC and databases. For FactoryTalk View SE, access to the ODBC data logs and File Data Sets is included.

www.SyTech.com

Six-Axis Robot

The VMB series robots from Technology Partner **Denso Robotics** offer a longer arm reach and higher load capacity than traditional models. The six-axis robots suit palletizing, packaging and material handling applications.

New features include greater air piping, valve and signal line options, and programming options using WINCAPS Plus software. Dust- and splash-proof IP67 protection and ISO Class 5 cleanliness suit electric parts handling, food manufacturing, pharmaceutical and medical device applications that require strict sanitation conditions.

Various sensors and other devices on the robot arm can be attached with internal piping, valves, and newly added EtherCAT® wiring. The design also reduces wiring and piping around the robot arm.

Thermoelectric Cooled CMOS Cameras

Technology Partner **Imperx, Inc.** introduces six new CMOS digital cameras with optional image sensor-cooling technology. The cameras are designed with thermal optimization for low noise performance and a full set for scientific imaging. The thermoelectric cooling option reduces dark current and warm/hot pixels while stabilizing the image sensor temperature to improve measurement precision over a range of ambient temperatures.

Available in resolutions of 17, 20 and 31 MP, the line uses the Sony Pregius IMX367, IMX387 and IMX342 CMOS image sensors with frame rates up to 32 fps.

PRODUCT SPOTLIGHT

LASER SCANNER WITH EMBEDDED CIP SAFETY

Rockwell Automation introduces the **Allen-Bradley® SafeZone™ 3 laser scanner with CIP Safety™ over EtherNet/IP™**. The smart safety device provides critical data needed for a comprehensive picture of machine or production line status.

The diagnostic information can help deliver insights, such as where safety-related failures are occurring or if workers are following standard operating procedures. The laser scanner provides area detection inside a work cell.

CIP Safety allows users to simultaneously operate multiple safety zones and provides diagnostic data over a single EtherNet/IP connection. This can improve productivity, such as alerting workers nearing a hazard to help prevent a machine from slowing down or stopping.

PA Link Module

The PA Link module from Technology Partner **Aparian** simplifies implementation of PROFIBUS® PA. The module combines an EtherNet/IP™ and Modbus™ TCP Linking device with an internal isolated power conditioner and bus terminator.

The module can either operate as a PROFIBUS DPV0/DPV1 master allowing EtherNet/IP devices, such as Rockwell Automation Logix platforms, or Modbus devices to exchange process, alarming and diagnostic data with PROFIBUS PA devices. It also provides parameterization and asset management of slave devices using device type managers (DTMs).

The module can exchange up to 2 kb of PROFIBUS data with either a Logix controller or any Modbus TCP master or slave device.

Expanded IEC Contactor Options

The expanded **Allen-Bradley® Bulletin 100-E™ energy-saving IEC contactor line** from Rockwell Automation is designed to help industrial companies save energy and reduce engineering time. With new sizes from 9 to 96A, these contactors save energy by reducing inrush apparent power (VA) by up to 68% and sealed VA by over 75% compared to standard, non-electronic coils.

The electronic coils also cover 20V to 500V AC/DC coil voltages with only four coil options, simplifying selection. The contactors allow coil input terminals to be moved from the line to load side of the contactors without disassembly.

PRODUCT SPOTLIGHT

HMI AND ALL-WEATHER WORKSTATIONS

Technology Partner **Pepperl+Fuchs, Inc.** offers two HMI systems: VisuNet Edge all-weather workstation and the VisuNet GXP modular, field-maintainable HMI.

VisuNet Edge's adaptable indoor/outdoor, watershed housing, and intrinsically safe touchscreen works without restrictions in Division 1 areas. An antimicrobial and chemically resistant keyboard with various mouse options completes the workstations.

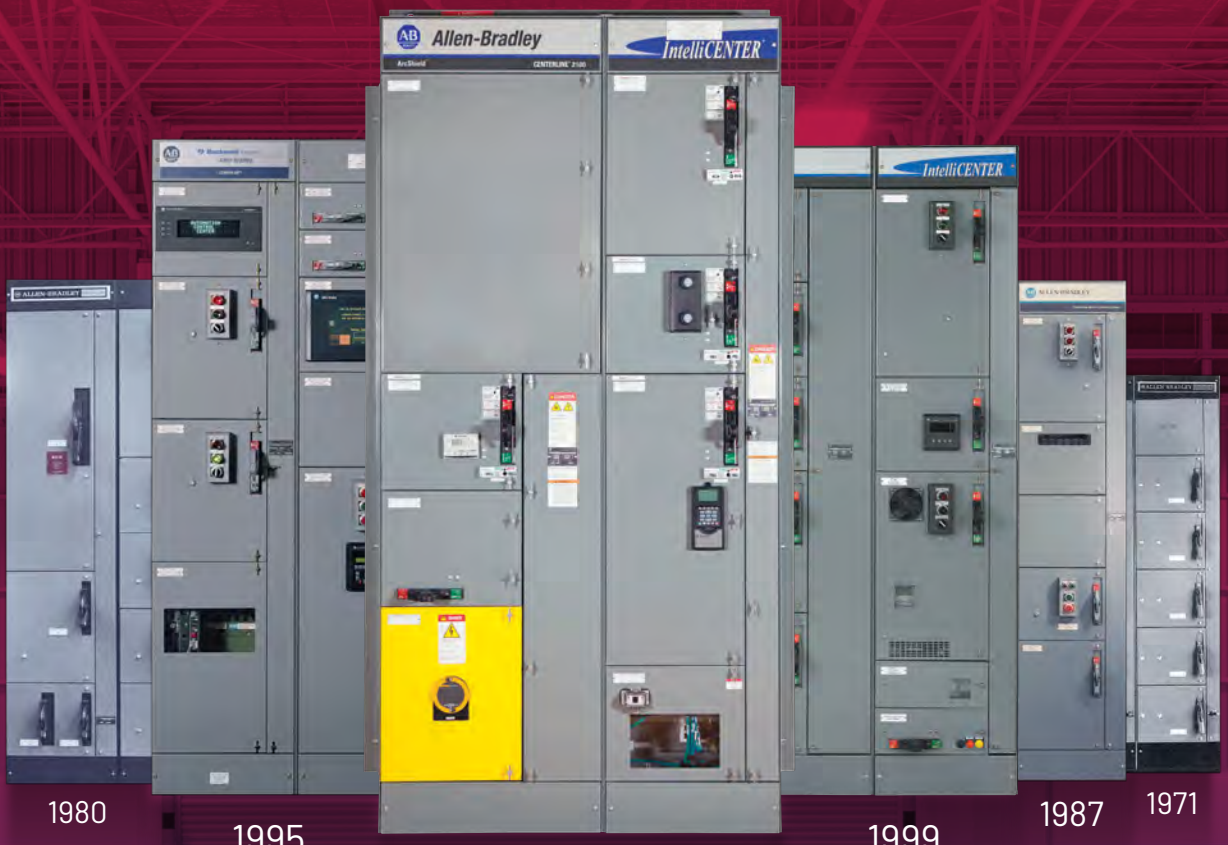
For life science applications, VisuNet GXP's modular, compact design simplifies setup and maintenance. The systems' three main components can be replaced in the field: display unit, power supply, and computing unit (PC or ThinManager Compatible Thin Client). Its stainless-steel housing resists chemicals and detergents.

ADVERTISER INDEX

Rockwell Automation

CENTERLINE®

Motor Control Centers



50 YEARS CENTERLINE®
MOTOR CONTROL CENTERS

The smart choice for **SMART MANUFACTURING** for over **50 YEARS**

CONTINUOUS INNOVATION | CONTINUOUS IMPROVEMENT | CONTINUOUS INTEGRATION

ROK.AUTO/MCC

Get Connected

aws Azure ptc SAP Microsoft SQL Server ORACLE

tManager™

PLC direct to cloud
No PC. No OPC. In-chassis.
Plant floor data
to your dashboards
in about 10 minutes

SILVER
Technology Partner
A ROCKWELL AUTOMATION PARTNER

Phoenix Digital

Redundant. Fiber. High availability.
No configuration. Plug and play.
Industrial networking modules.

Stay Connected

NetXpert XG

Industrial Ethernet cable testing
Active network testing
POE testing
Reporting

Softing Inc.
865-251-5252
sales@softing.us
industrial.softing.com/us

optimize! softing

Contact us for a quote or demo

Get Connected
Stay Connected

https://industrial.softing.com/us/solutions/rockwell-automation-solutions.html