May/June 2019

InTech®

A PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

ISA™

Data-driven decision making

Digitalization value

Machine vision systems

Preventive maintenance

Thin clients

Open Process Automation Standard Takes Flight

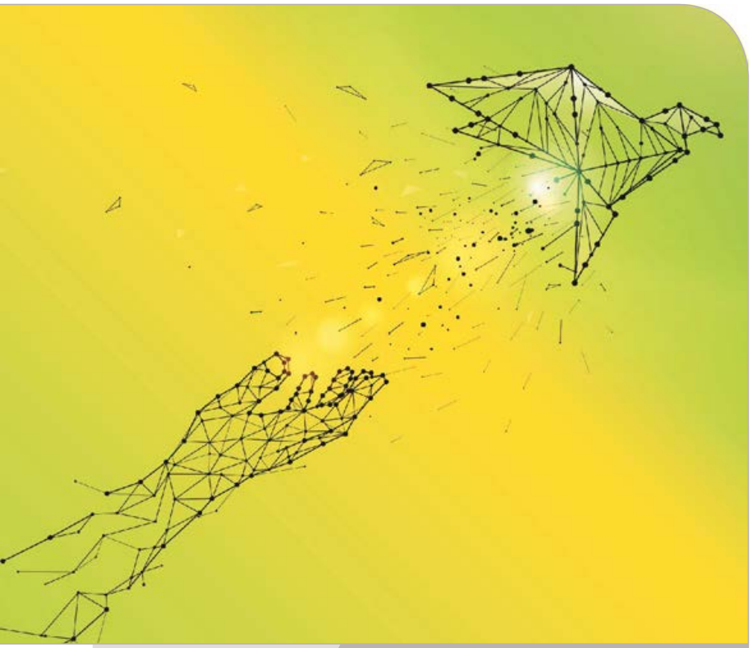
A detailed look at O-PAS™ Standard, Version 1.0

Setting the Standard for Automation™

www.isa.org/intech

May/June 2019 | Vol. 66, Issue 3 www.isa.org

InTech



COVER STORY

10 The Open Process Automation Standard takes flight

By Dave Emerson

The first release of O-PAS Standard, Version 1.0, addresses interoperability topics, while forthcoming releases will tackle configuration and application portability.

SPECIAL SECTION: MOISTURE MEASUREMENT

34 Digitize and optimize preventive maintenance for process instrumentation

By Fawaz AlSahan

Conventional time-based preventive maintenance is widely used throughout industry but has shortcomings that can be overcome with smart sensors and analytics, increasing the effectiveness and profitability of process facilities.

PROCESS AUTOMATION

16 Industrial Process Operation 4.0

By Martin Hollender, PhD

Industry can now provide the same level of digital support to the industrial worker and the office worker whether they are in the control room, in the plant, or working remotely. Digitalization, Internet of Things, big data, artificial intelligence, and virtual reality are rapidly developing technologies that will change how industrial processes will be operated in the future.

FACTORY AUTOMATION

22 Digitalization delivers value

By Duncan Micklem

Every software initiative in the energy and chemical industry is now tagged with the name "digitalization," which has risen to the top of the C-suite agenda due to the rapid penetration of disruptive technologies. Those who embrace digitalization will prosper, while those who do not respond will indeed be left behind.

SYSTEM INTEGRATION

26 A relook at machine vision system design

By Gineesh Sukumaran

Machine vision systems must be designed so they can be reused for multiple applications and easily modified for changing product designs, manufacturing processes, varying components, and business needs. Reconfigurable vision systems' programmable logic is meeting this challenge.

AUTOMATION IT

30 Building reliable visualization and control for industrial edge applications

By Jason Andersen

The best industrial edge deployment strategies for visualization and control include flexible hardware and software delivering the best advantages of thin clients.

DEPARTMENTS

8 Automation Update
Industry 4.0, digitalization dominate 2019 Hannover Messe, Risks of connected OT networks, By the Numbers

40 Association News
Bassett new *InTech* chief editor, ISA supports Cyber Shield, ISA director of strategic initiatives awarded SANS ICS Lifetime Achievement Award; certification review

42 Automation Basics
Single-loop control – Still the mainstay of advanced process control

45 Channel Chat
The changing role of the control system engineer

46 Standards
New standards work on IIoT cybersecurity, controller algorithms

47 Products and Resources
Spotlight on vision systems

COLUMNS

7 Talk to Me
If disruption is the "problem," innovation is the solution

44 Executive Corner
Building a cybersecure manufacturing strategy

50 The Final Say
Beware of the hype

RESOURCES

48 Index of Advertisers

49 Datafiles

49 Classified Advertising

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**

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 3.**

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

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.

PRINTED WITH SOY INK

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.


HART & Functional Safety
Go Together Like
Wheels & Brakes
MOORE INDUSTRIES
WORLDWIDE
Demand Moore Reliability
STZ
SST
SSX
HES
READY
CHANNEL 1
CHANNEL 2
CHANNEL 3
CHANNEL 4
SPAN
ZERO
SPEED
ETHERNET
LINK/ACT
Keep your plant safe and intelligent by getting all the data you can from your smart HART instruments. Moore Industries products are designed to wheel that critical process and diagnostic data to your monitoring, control and safety systems so they can put on the brakes when problems arise in your process.
To learn more
Go to miinet.com/Wheel-and-Brake
Call 800-999-2900

If disruption is the "problem," innovation is the solution

By Bill Lydon, *InTech* Contributing Editor

Futurist Nicholas J. Webb (www.nick-webb.com) spoke at the 2019 Manufacturing in America conference in Detroit in March and discussed a number of thought-provoking trends. On the topic of disruption, he made a statement that to me seemed fundamental, "If disruption is the problem, innovation is the solution."

He suggested when change is occurring, people may have a tendency to deny, hide, or be victimized by disruption. Alternatively, people can realize change is happening, embrace it, and benefit from new opportunities.

Another key point in his presentation noted that "legacy" is very comfortable and creates a resistance to change. My observation is that holding on to legacy practices and systems too long can hold back an organization from progress, and in manufacturing creates an environment for competitors to overtake your business. Once it becomes obvious that competitors are "beating" your company with sales and profits declining, the time, effort, and resources to become competitive are expensive. At this point you are chasing rather than leading in your industry.

Destruction

Thinking about innovation, the famous painter Pablo Picasso said, "Every act of creation is first an act of destruction." Creating something new usually requires letting go of something old—which can be very difficult. Transitions are painful, because they destroy the status quo, pushing us beyond our comfort zones.

It is important to remember that we often do not see disruptive innovation coming. Disruption takes us by surprise if we are not the ones disrupting. This makes it important to explore new ideas and technologies that can lead to innovative disruption within your manufacturing operations.

The task for automation professionals is to analyze the confusing multidimensional chaos of new technologies, expectations, requirements, and processes to develop new superior solutions. Innovations may be internally complex but simplify life for users, reducing complexity and increasing efficiency.

Challenge

Automation professionals shine at using their experience, know-how, and creativity to solve problems to improve manufacturing and production efficiencies and quality by designing applications. Working within the limitations of existing legacy systems in a plant inherently limits the ability to create applications to improve operations, productivity, and profits. Newer automation systems with superior technology give automation professionals the tools to achieve greater results. In the environment of changing technology, it is important to look beyond and understand the options for improving productivity and competitiveness that may take new investments. Setting goals beyond today's status quo and then finding ways to achieve those goals will yield new results.

It's hard to achieve the goal of disruptive innovation if you aren't certain what you are trying to accomplish. ■

ISA *INTECH* STAFF

CHIEF EDITOR
Renee Bassett
rbassett@isa.org

CONTRIBUTING EDITOR
Bill Lydon
blydon@isa.org

CONTRIBUTING EDITOR
Charley Robinson
crobinson@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

Industry 4.0, digitalization dominate 2019 Hannover Messe

Surrounded by a bustling fair illuminating the theme of "Integrated Industry – Industrial Intelligence," the excitement and energy overflowed at the 2019 Hannover Messe. With 6,500 exhibitors from 75 countries and 215,000 attendees from 95 nations, the event featured Sweden as the partner country and hosted over 80 forums and conferences highlighting a host of new digitalization trends and technologies. This year's event revealed a number of organizations focused on providing standards and information to assist the modernization and digital transformation of manufacturers.

Open Industry 4.0 Alliance: Some of the biggest news was the announcement of The Open Industry 4.0 Alliance, a collaboration with the goal of overcoming proprietary solutions. The charter of the organization is to create customer value through holistic interoperable Industry 4.0 solutions and services in a common framework powered by an alliance of industry partners for the digitization of the factory, plant, and warehouse. Founders and members endorse an open ecosystem and commit to using an Open Industry 4.0 Alliance Framework to achieve interoperability that provides attractive opportunities for companies of all sizes. A major end goal is to have machines in a given smart factory speak the same language.

5G Alliance for Connected Industries and Automation (5G-ACIA): This global forum, prominently seen throughout Hannover Messe 2019 halls, was formed to address, discuss, and evaluate the technical, regulatory, and business aspects of fifth-generation (5G) cellular network technology for industrial applications. The dominant objective of 5G-ACIA is the best possible applicability of this wireless communications technology for connected industries. 5G-ACIA works to ensure that the interests and specific aspects of the industrial domain are adequately considered in 5G standardization and regulation. It encompasses stakeholder groups including operational technology, information and communication technology, and academic groups or associations.

New wave suppliers: Since the Industry 4.0 topic was first explored at Hannover Messe 2011, there has been an influx of new wave exhibitors and presenters reflecting the transition to digitalization. Hannover Messe 2019 continued to see the traditional industrial suppliers exhibit and show off new products, but there has been a change. The booths of high-technology companies—including Amazon, Microsoft, Oracle, SAP, IBM, Dell, Hewlett Packard Enterprise, Huawei, Dassault Systèmes, CISCO, and PTC—have gotten bigger and more prominent. New high-tech companies, either upstarts or those crossing over from computer/IoT applications, are also increasingly bringing value to manufacturing. ■

– By Bill Lydon, InTech

Transportation sector reveals risks of connected OT networks

Time to market is an essential competitive edge in a digital marketplace that has placed growing pressure on the rapid delivery of goods. In addition to developing new products and services, success today depends upon new functions like DevSecOps teams and agile software development, more speed and bandwidth, on-demand infrastructures spanning multicloud environments to manage big data, and hyperconnectivity across data and resources.

Few places are experiencing more of the cyberimpact of this new business model than the operational technology (OT) transportation sector. Organized cybercriminals have actively exploited container shipping companies and container port operators. By hacking Internet-connected OT systems, cybercriminals have accessed ICS-based cargo systems to redirect containers or make them disappear off the grid entirely. They access aircraft systems by breaking into Internet-connected OT subsystems such as communication, maintenance, catering, and baggage handling.

Although OT systems do not present the sort of personal data value that many traditional cybercriminals seek, targeting critical infrastructure still has huge appeal. Cybercriminal agendas include holding a critical system hostage, manipulating a stock price, or even operating as a cyber "hit man" as a competitive strategy. The following examples show vulnerabilities in today's transportation systems.

Satellite/Internet communications: Navigation and cargo systems are increasingly connected to satellite and Internet communication, escalating cyberrisk. In 2013, a University of Austin student participating in a sanctioned experiment aboard an $80M yacht spoofed the navigation system, steering the ship off course.

Advanced persistent threats: APTs are a clear and present danger to the transportation industry. Compromised ticketing and scheduling systems, for example, can shut down transportation hubs. Airlines security experts agree that more intelligence across the cyber kill-chain must be shared between carriers, but this requires public-private cooperation that does not currently exist.

Phishing attacks: The impact can be severe when cybercriminals execute a masquerade attack and gain network privilege, but the attacks are difficult to execute. Once a cyberattacker has access, the threat can extend to IT resources.

Espionage: According to one report, 47 percent of malware aimed at manufacturers was intended to steal intellectual property. According to the National Center for Manufacturing Sciences, 21 percent of manufacturers lost intellectual property as a result. ■

– By Rick Peters, Fortinet

Automation by the Numbers

630 After a two-year design and construction phase, as part of its "Mission to Zero," ABB has opened its first CO_2-neutral production site in Luedenscheid, Germany. As a visible sign of intent, the company is commissioning a solar power plant at its Busch-Jaeger subsidiary. The installed ABB technology will generate enough power on sunny days to cover 100 percent of the factory's power requirements. The site is projected to save about **630 tons of CO_2 a year**.

The photovoltaic system, which measures 3,500 square meters and is installed over the car parks on the company premises, will deliver about 1,100 MWh of climate-neutral solar power a year—approximately the annual requirement of 3,360 private households. In combination with a cogeneration plant that operates with double the energy efficiency of a coal-fired power plant, about 14 percent more energy can be generated than is needed at the site. The surplus power is fed into the public grid, contributing to the region's power supply with sustainably produced energy.

To cover peaks in demand, additional green energy is sourced from MVV Energie AG, which guarantees 100 percent CO_2-neutral production. MVV and ABB signed a partnership agreement in April that focused on shared solutions for the sustainable improvement of energy efficiency in industry, medium-sized companies, and "smart city" municipalities.

Over half of ABB's worldwide revenues are generated by technologies that help industry combat the causes of climate change, and many of those technologies have been used on this flagship production site. The technological centerpiece of the entire system in Luedenscheid is the scalable energy management system OPTIMAX from the ABB Ability Energy Management Suite.

OPTIMAX provides for the constant surveillance and optimal control of energy production, consumption, and storage, and operates largely autonomously. This learning system calculates the optimal energy flow on the basis of predictive data and compensates for deviations in real time.

Aside from the energy management system and the photovoltaic system with inverters, the entire system brings together other ABB technologies that are digitally interconnected. These include smart switchgear for energy distribution, a battery energy storage system, and ABB charging points where staff and visitors can charge their electric vehicles free of charge. ■

537 At its annual Innovators' Meeting held this year in France, the Endress+Hauser Group claimed a company record of **537 patents granted in 2018**. The company said it submitted 287 initial patents in 2018—another record. Endress+Hauser owns nearly 7,800 active intellectual property rights worldwide and cites its 309 invention disclosures in 2018 as a sign of the company's ongoing innovation. Roughly one-third of the 2018 patent filings are related to the Industrial Internet of Things, digital communications, and instrument diagnostics, released under the motto #empowerthefield.

Each invention undergoes a multistage internal evaluation process before submission to the patent office, usually within four months. To handle the stream, in 2016 an internal patent department was created in the U.S. Four specialists in Greenwood, Ind., are responsible for protecting the technical innovations, handling all patent filings from the group companies located in the U.S., and handling up to 80 percent of the overseas filings. ■

The Open Process Automation Standard takes flight

A detailed look at O-PAS™ Standard, Version 1.0

By Dave Emerson

FAST FORWARD

- OPAF, under the guidance of The Open Group, has developed the O-PAS Standard, Version 1.0.
- The standard defines minimum requirements for components that can be used to create federated process automation systems with an open and interoperable reference architecture.
- O-PAS Version 1.0 was released in January 2019 as a preliminary standard of The Open Group; OPAF will incorporate industry feedback after an interoperability workshop this June.

Process automation end users and suppliers have expressed interest in a standard that will make the industry much more open and modular. In response, the Open Process Automation™ Forum (OPAF) has worked diligently at this task since November 2016 to develop process automation standards. The scope of the initiative is wide-reaching, as it aims to address the issues associated with the process automation systems found in most industrial automation plants and facilities today (figure 1).

It is easy to see why a variety of end users and suppliers are involved in the project, because the following systems are affected:
- manufacturing execution system (MES)
- distributed control system (DCS)
- human-machine interface (HMI)
- programmable logic controller (PLC)
- input/output (I/O)

In June 2018, OPAF released a technical reference model (TRM) snapshot as industry guidance of the technical direction being taken for the development of this new standard. The organization followed the TRM snapshot with the release of the OPAS™ Version 1.0 in January 2019. Version 1.0 addresses the interoperability of components in federated process automation systems. This is a first stop along a three-year road map with annual releases targeting the themes listed in table 1.

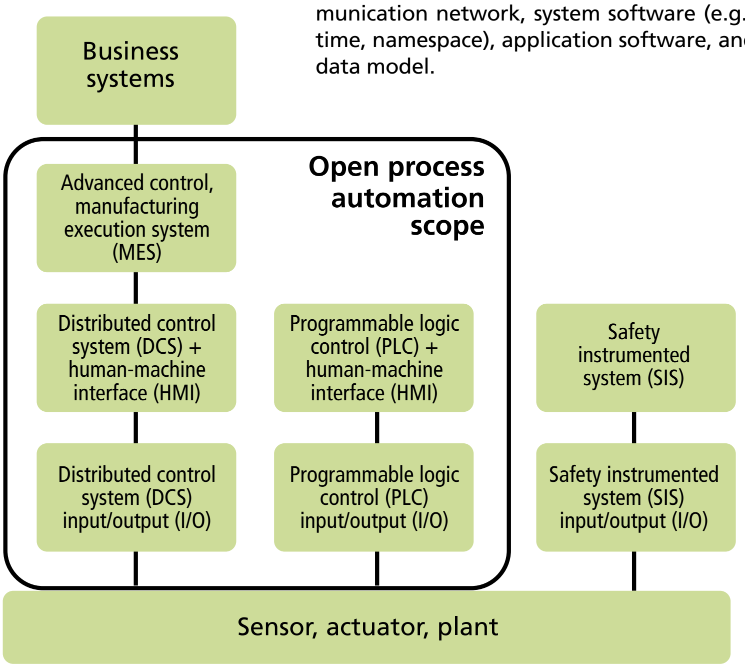
Table 1. The O-PAS Standard three-year release road map addresses progressively more detailed themes.

Version	Target date	Theme
1.0	2019	Interoperability
2.0	2020	Configuration portability
3.0	2021	Application portability

By publishing versions of the standard annually, OPAF intends to make its work available to industry expeditiously. This will allow suppliers to start building products and returning feedback on technical issues, and this feedback—along with end user input—will steer OPAS development. O-PAS Version 1.0 was released as a preliminary standard of The Open Group to allow time for industry feedback.

The OPAF interoperability workshop in May 2019 is expected to produce feedback to help finalize the standard. The workshop allows member organizations to bring hardware and software that support O-PAS Version 1.0, testing it to verify the correctness and clarity of this preliminary standard. The results will not be published but will be used to update and finalize the standard.

Figure 1. A broad sampling of suppliers and end users are highly interested in the scope of the OPAS under development by OPAF, because it touches on all the key components of industrial automation systems: hardware (I/O), the communication network, system software (e.g., run time, namespace), application software, and the data model.



Some terminology

For clarity, a summary of the terminology associated with the OPAF initiative is:
- The Open Group: The Open Group is a global consortium that helps organizations achieve business objectives through technology standards. The membership of more than 625 organizations includes customers, systems and solutions suppliers, tool vendors, integrators, academics, and consultants across multiple industries.
- Open Process Automation Forum: OPAF is an international forum of end users, system integrators, suppliers, academia, and other standards organizations working together to develop a standards-based, open, secure, and interoperable process control architecture. Open Process Automation is a trademark of The Open Group.
- O-PAS Standard, Version 1.0 (O-PAS): OPAF is producing the OPAS Standard under the guidance of The Open Group to define a vendor-neutral reference architecture for construction of scalable, reliable, interoperable, and secure process automation systems.

Standard of standards

Creating a "standard of standards" for open, interoperable, and secure automation is a complex undertaking. OPAF intends to speed up the process by leveraging the valuable work of various groups in a confederated manner.

The OPAS Standard will reference existing and applicable standards where possible. Where gaps are identified, OPAF will work with associated organizations to update the underlying standard or add OPAS requirements to achieve proper definition. Therefore, OPAF has already established liaison agreements with the following organizations:

- Control System Integrators Association (CSIA)
- Distributed Management Task Force (DMTF), specifically for the Redfish API
- FieldComm Group
- Industrial Internet Consortium (IIC)
- International Society of Automation (ISA)
- NAMUR
- OPC Foundation
- PLCopen
- ZVEI

Additionally, OPAF is in discussions with AutomationML and the ISA Security Compliance Institute (ISCI) as an ISA 62443 validation authority. In addition to these groups, the OPC Foundation has joined OPAF as a member, so no liaison agreement is required.

As an example of this cooperation in practice, OPAS Version 1.0 was created with significant input from three existing standards, including:

- ANSI/ISA 62443 (adopted by IEC as IEC 62443) for security
- OPC UA adopted by IEC as IEC 62541 for connectivity
- DMTF Redfish for systems management (see www.dmtf.org/standards/redfish)

Next step: Configuration portability

Configuration portability, now under development for OPAS Version 2.0, will address the requirement to move control strategies among different automation components and systems. This has been identified by end users as a requirement to allow their intellectual property (IP), in the form of control strategies, to be portable. Existing standards under evaluation for use in Version 2.0 include:

- IEC 61131-3 for control functions
- IEC 16499 for execution coordination
- IEC 61804 for function blocks

O-PAS Version 3.0 will address application portability, which is the ability to take applications purchased from software suppliers and move them among systems within a company in accordance with applicable licenses. This release will also include the first specifications for hardware interfaces.

Under the OPAS hood

The five parts that make up O-PAS Version 1.0 are listed below with a brief summary of how compliance will be verified (if applicable):

- Part 1 – Technical Architecture Overview (informative)
- Part 2 – Security (informative)
- Part 3 – Profiles
- Part 4 – Connectivity Framework (OCF)
- Part 5 – System Management

Part 1 – Technical Architecture Overview (informative) describes an OPAS-conformant system through a set of interfaces to the components. Read this section to understand the technical approach OPAF is following to create the O-PAS.

Part 2 – Security (informative) addresses the necessary cybersecurity functionality of components that are conformant to OPAS. It is important to point out that security is built into the standard and permeates it, as opposed to being bolted on as an afterthought. This part of the standard is an explanation of the security principles and guidelines that are built into the interfaces. More specific security requirements are detailed in normative parts of the standards. The detailed normative interface specifications are defined in Parts 3, 4, and 5. These parts also contain the associated conformance criteria.

Part 3 – Profiles defines sets of hardware and software interfaces for which OPAF will develop conformance tests to make sure products interoperate properly. The O-PAS Version 1 profiles are:

- Level 1 Interoperability Hardware Profile: A certified product claiming conformance to this profile shall implement OSM-Redfish.
- Level 2 Interoperability Hardware Profile: A certified product claiming conformance to this profile shall implement OSM-Redfish BMC.
- Level 1 Interoperability Software Profile: Software claiming conformance to this profile shall implement OCF-001: OPC UA Client/Server Profile.
- Level 2 Interoperability Software Profile: Software claiming conformance to this profile shall implement OCF-002: OPC UA Client/Server and Pub/Sub Profile.

The term "Level" in the profile names refers to profile levels.

Part 4 – Connectivity Framework (OCF) forms the interoperable core of the system. The OCF is more than just a network, it is the underlying structure allowing disparate components to interoperate as a system. The OCF will use OPC UA for OPAS Versions 1.0, 2.0, and 3.0.

Part 5 – System Management covers foundational functionality and interface standards to allow the management and monitoring of components using a common interface. This part will address hardware, operating systems and platform software, applications, and networks—although at this point Version 1.0 only addresses hardware management.

Conformance criteria are identified by the verb "shall" within the O-PAS text. An OPAF committee is working on a conformance guide document that will be published later this year, which explains the conformance program and requirements for suppliers to obtain a certification of conformance.

Technical architecture

The OPAS Standard supports communication interactions that are required within a service-oriented architecture (SOA) for automation systems by out-

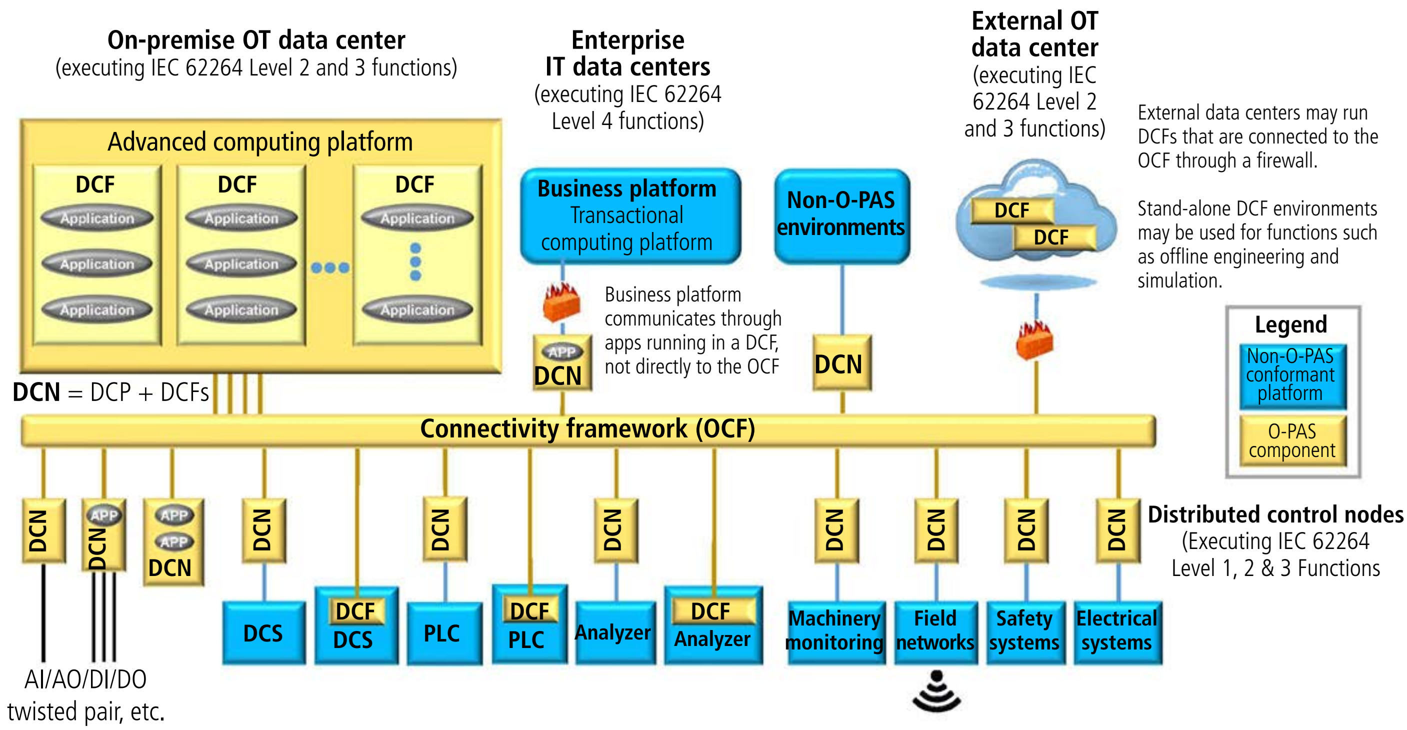


Figure 2. OPAS establishes a system architecture organizing process automation elements into interoperable groupings.

lining the specific interfaces the hardware and software components will use. These components will be used to architect, build, and start up automation systems for end users.

The vision for the OPAS Standard is to allow the interfaces to be used in an unlimited number of architectures, thereby enabling each process automation system to be "fit for purpose" to meet specific objectives. The standard will not define a system architecture, but it will use examples to illustrate how the component-level interfaces are intended to be used. System architectures (figure 2) contain the following elements:

Distributed control node (DCN): A DCN is expected to be a microprocessor-based controller, I/O, or gateway device that can handle inputs and outputs and computing functions. A key feature of O-PAS is that hardware and control software are decoupled. So, the exact function of any single DCN is up to the system architect. A DCN consists of hardware and some system software that enables the DCN to communicate on the O-PAS network, called the OCF, and also allows it to run control software.

Distributed control platform (DCP): A DCP is the hardware and standard software interfaces required in all DCNs. The standard software interfaces are a common platform on top of which control software programs run. This provides the physical infrastructure and interchangeability capability so end users can control software and hardware from multiple suppliers.

Distributed control framework (DCF): A DCF is the standard set of software interfaces that provides an environment for executing applications, such as control software. The DCF is a layer on top of the DCP that provides applications with a consistent set of O-PAS related functions no matter which DCN they run in. This is important for creating an efficient marketplace for O-PAS applications.

OPAS connectivity framework (OCF): The OCF is a royalty-free, secure, and interoperable communication framework specification. In O-PAS Version 1, the OCF uses OPC UA.

Advanced computing platform (ACP): An ACP is a computing platform that implements DCN functionality but has scalable computing resources (memory, disk, CPU cores) to handle applications or services that require more resources than are typically available on a small profile DCP. ACPs may also be used for applications that cannot be easily or efficiently distributed. ACPs are envisioned to be installed within on-premise servers or clouds.

Within the OPAS Standard, DCNs represent a fundamental computing building block (figure 3). They may be hardware or virtual (when virtual they are shown as a DCF as in figure 2), big or small, with no I/O or various amounts. At the moment, allowable I/O density per DCN is not settled, so some standardization in conjunction with the market may drive the final configuration.

DCNs also act as a gateway to other networks or systems, such as legacy systems, wireless gateways, digital field networks, I/O, and controllers like DCS or PLC systems. Industrial Internet of Things (IIoT) devices can also be accessed via any of these systems.

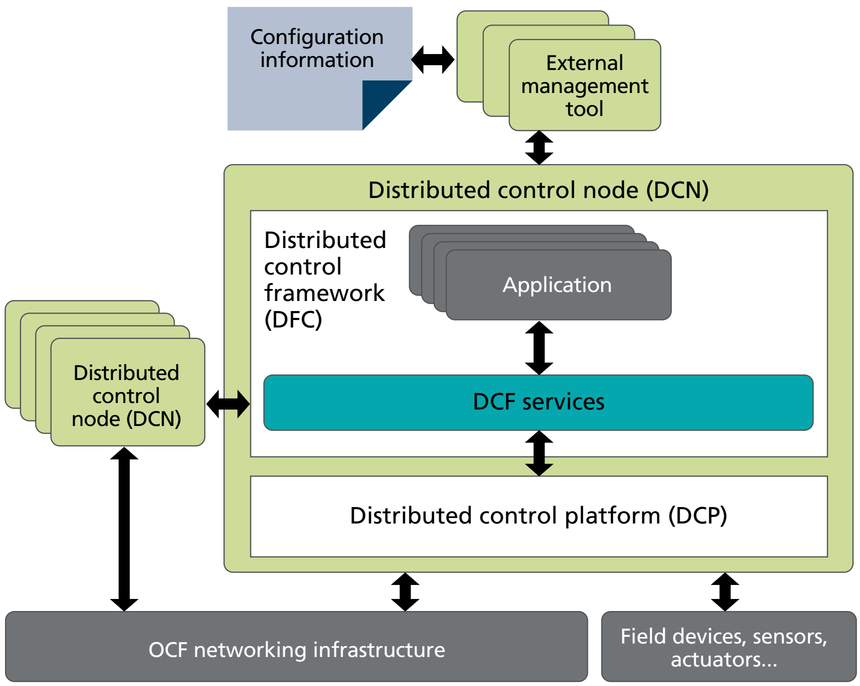


Figure 3. DCNs are conceived as modular elements containing DCP (hardware) and DCF (software), both of which are used to interface field devices to the OCF.

Building a system

End users today must work with and integrate multiple systems in most every process plant or facility. Therefore, the OPAS Standard was designed so users can construct systems from components and subsystems supplied by multiple vendors, without requiring custom integration. With the OPAS Standard it becomes feasible to assimilate multiple systems, enabling them to work together as one OPAS-compliant whole. This reduces work on capital projects and during the lifetime of the facility or plant, leading to a lower total cost of ownership.

By decoupling hardware and software and employing an SOA, the necessary software functions can be situated in many different locations or processors. Not only can software applications run in all hardware, but they can also access any I/O to increase flexibility when designing a system.

One set of components can be used to create many different systems using centralized architectures, distributed architectures, or a hybrid of the two. System sizes may range from small to large and can include best-in-class elements of DCS, PLC, SCADA, and IIoT systems and devices as needed.

Information technology (IT) can also be incorporated deeper into industrial automation operational technology (OT). For example, DMTF Redfish is an IT technology for securely managing data center platforms. OPAF is adopting this technology to meet OPAS system management requirements.

Comprehensive and open

Each industrial automation supplier offers a variety of devices and systems, most of which are proprietary and incompatible with similar products from other vendors and sometimes with earlier versions of their own products. End users and system integrators trying to integrate automation systems of varying vintages from different suppliers therefore have a challenging job.

To address these issues, OPAF is making great strides toward assembling a comprehensive, open process automation standard. Partially built on other established industry standards, and extending to incorporate most aspects of industrial automation, the O-PAS Standard will greatly improve interoperability among industrial automation systems and components. This will lower implementation and support costs for end users, while allowing vendors to innovate around an open standard.

For more information on OPAS Version 1.0, please download the standard at https://publications.opengroup.org/p190. Submit feedback by emailing ogspecs@opengroup.org. ■

ABOUT THE AUTHOR

Dave Emerson is vice president of Yokogawa's U.S. Technology Center in Dallas, Texas. He is experienced in applying and developing automation systems used in the process industries. Emerson is an ISA Fellow and a member of *Control* magazine's Process Automation Hall of Fame. He has more than 30 years of experience participating on U.S. and international consensus standards committees, such as ISA-88, ISA-95, IEC TC65, and ISO TC184. He also represents Yokogawa in several industry groups, including leadership roles with MESA, MIMOSA, and the OPC Foundation. Emerson is Yokogawa's primary representative with OPAF and is currently co-chair of OPAF's Enterprise Architecture Working Group.

View the online version at www.isa.org/intech/20190601.

RESOURCES

"New software for next-gen automation"
www.isa.org/intech/201806final

"Breaking closed architecture bonds"
www.isa.org/intech/20180201

"End users want COTS, and they want it now"
www.isa.org/intech/20160604

Industrial Process Operation 4.0

Digitalization is impacting industrial processes as the technical infrastructure that allows data-driven decision making—Internet of Things, big data, artificial intelligence, virtual reality—becomes available

By Martin Hollender, PhD

Digitalization, Internet of Things (IoT), big data, artificial intelligence, and virtual reality are some examples of rapidly developing areas of technology that will have a big impact on how industrial processes will operate in the future. Normal operations that are already highly automated will be even more automated in the future. Tasks like fault detection, diagnosis, and process optimization are becoming more complex.

Many of those tasks are best handled by interdisciplinary teams with broad expertise and knowledge about process, plant, operations, maintenance, networks, sensors, and actuators. Collaborative process operations make it possible to efficiently bring disciplines together to focus on the problem at hand. Big data and artificial intelligence tools support teams and make them as efficient as possible. Previously isolated control rooms become networked control centers for the Industry 4.0 high-performance work force. Work environments must support collaboration at all levels and support high-performance work around the clock.

Like the situation in the transport sector with the advent of self-driving cars, the way industrial processes operate is dramatically changing. Today's sophisticated digital automation programs can handle most situations. Cheap sensors connected to powerful artificial intelligence algorithms, like image recognition or vibration monitoring, can increasingly replace human sensing. A single operator can take responsibility for larger and larger plant sections.

Integrated industrial information systems gather operational data to enable collaboration across locations, disciplines, and organizations. They make real-time data easily available to the appropriate individuals.

However, the reality is often far from ideal. In a

FAST FORWARD

- Digitalization, IoT, big data, artificial intelligence, and virtual reality will improve industrial process operation.
- Work environments must support collaboration at all levels and support high-performance work around the clock.
- Knowledge workers in process operation still spend too much time searching for data in information silos or proprietary tools.

case example about offshore platforms, McKinsey has shown that although huge amounts of data are already being collected, only a small portion is actually being used as a basis of operational decisions (figure 1). This is currently changing, as the technical infrastructure that allows data-driven decision making becomes available.

Other important trends include flexible modular plants for producing small quantities of frequently changing products. Such processes are more difficult to operate because of the frequent product changeovers, and it is more difficult to gather experience.

New big data and artificial intelligence methods can predict upcoming problems long before they affect production. They also enable prescriptive maintenance strategies. Remote operation is becoming more widely used. Often it makes sense to bring in highly specialized remote expertise. Sometimes even the whole plant is operated remotely, as is the case for many offshore platforms.

Modern control rooms have turned into networked information and communication centers where collaboration workflows come together. The remaining operators need a supportive work environment that helps them stay vigilant and carry out their jobs as effectively as possible.

Breaking down information silos

Modern process plants are complex and highly coupled systems. As a result, a problem in one part of the process will tend to propagate across different subsystem and plant components. The advanced automation systems in use also add complex dynamic interactions between the different plant components, making it difficult to obtain a clear assessment of a potential problem. Collaborative efforts from a multidisciplinary team are needed to effectively troubleshoot, diagnose, or optimize process dynamics. In addition, the

From a base of 30,000 data tags, close to zero tags are used to inform operational decisions.

		Comment	Source
People and processes	0%	Schedule predominately based on OEM-recommended maintenance intervals	Interviews with operational staff
Deployment	<1%	No interface in place to enable real-time analytics to "reach" offshore	
Analytics	<1%	Reporting limited to a few KPIs that are monitored in retrospect	BI and KPI walkthrough
Data management	~1%	Data cannot be accessed in real time, enabling only ad hoc analysis	Walkthrough of infrastructure and bandwidth between off- and onshore
Infrastructure	60%	Only about 1% can be streamed onshore for day-to-day use	
Data capture	100%	About 40% of all data is never stored—the remainder is stored locally offshore	Assessment of storage capacity (on the highest-capacity asset)

~30,000 tags measured

Figure 1. Case example about data-driven decisions

Source: McKinsey

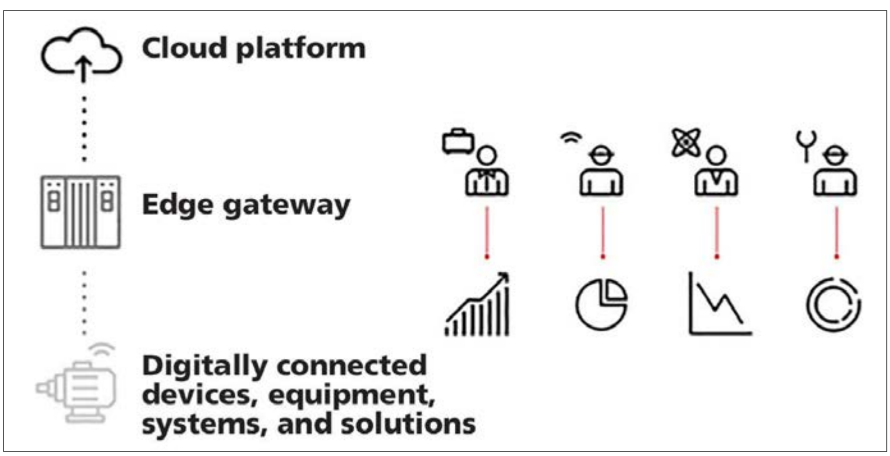


Figure 2. Although industrial applications have been lagging behind consumer and enterprise solutions, industry is now catching up to provide the same level of digital support to the industrial worker and the office worker.

highly advanced systems used to support plant operations may also require the involvement of specialized expertise, often represented by an external supplier.

Unfortunately, collaboration between personnel from different disciplines, locations, and organizational boundaries is often hindered by the fact that the information needed to solve the problem at hand is hidden within numerous information silos. Knowledge workers in process operation still spend too much time searching for data in information silos or proprietary tools. Many companies also lack the organization and work processes to support multidisciplinary collaboration, and therefore tend to execute work based on a relay race approach instead of as a collaborative effort.

However, industrial companies are realizing that they need to improve the way they work to stay competitive in an increasingly volatile market. The digitalization trend is sweeping across the industries. Companies are taking actions to improve workforce effectiveness through the introduction of digital technologies. Many companies are introducing "bring-your-own-device" policies and deploying solutions so their employees can work effectively wherever they are: at the office, on trips, or from home.

Although industrial applications have been lagging behind consumer and enterprise solutions, industry is now catching up to provide the same level of digital support to the industrial worker and the office worker, whether they are in the control room, in the plant, or in a remote location (figure 2).

Information previously hidden within the control systems or proprietary tools is now increasingly made available through improved connectivity and integration across different systems and network layers. Web-based applications are available to support the consolidation of data from different systems and tools, making these easily accessible from one place. Easy data access and a common work environment is the first step for effective collaboration to support process operation. Improvements in analytics and visualization techniques also help workers make sense of the increasing amount of data available.

Other technology trends are also supporting a new collaborative approach to working. After many years of teething troubles, video conferencing technology has matured and is moving from a nice-to-have technology to a necessity. Several companies now have remote operation centers that support the local control rooms with continuously open video links between locations. High-quality video conferencing technology is also available from mobile devices or personal workstations, so operators can get instant access to remote expertise via video conferencing whenever they need it. In combination, the introduction of digital technology for easy access to information, independent of location, and the proliferation of video conferencing to support remote collaboration, are blurring the boundaries between local and remote operation.

Modern automation systems cover most aspects of normal operation but also handle many abnormal situations. Advanced control techniques, such as model-predictive control (MPC) and state-based control, allow the automation of very complex tasks, such as the startup of a plant. Automatic control performs better than typical human operators. The operator is less and less involved in the inner control loops with direct contact to the process. The tasks shift more and more to supervisory control, where the operator manages and supervises a large number of control modules.

Bridging the knowledge gap

But being less involved in direct process control also means fewer opportunities to develop a feeling for the process by training on the job. (This problem was dramatically illustrated with the accident of flight AF447. The autopilot discovered inconsistent speed measurements from all three redundant speed measurements and switched into manual mode. The pilot did not have enough experience flying at great heights and was overburdened with this sudden and unexpected transfer of responsibility. He went into climb mode, which reduced the speed of the plane and finally led to the crash.)

To be able to take over when automation fails, operators need higher qualifications and a profound understanding of the technical process, the automation system, and the control modules. Simulator training is necessary to develop a feeling for the process. Modern operators should also be deeply involved in the optimization of process operations, because such an activity keeps them involved and helps to build up the required knowledge that allows them to take over in case of automation failure.

Another area where Industry 4.0 will have a huge impact is industrial quality control. Big data techniques make it possible to distill historical process data into algorithms that can predict the quality of the currently production. Upcoming problems can be detected early, and countermeasures can be taken before the effect of the problem becomes significant. Previously, it took an operator many years to accumulate comparable experience.

Remote expertise should be brought in for all complex and difficult decisions (figure 3). For example, in the case of the Deepwater Horizon oil spill, the investigation report clearly states that one major factor contributing to the accident was the incorrect interpretation of available measurements. Quite likely, with advice from highly qualified remote experts, the company would have avoided this accident.

The high complexity of modern plants requires expertise from many different domains (e.g., MPC, chemistry, electrical drives, distributed control systems). It is impossible for most plants to hire personnel with sufficient knowledge in all these areas. Modern collaborative environments make it possible to bring in remote expertise as needed.

Managing key performance indicators for process operations in areas such as control loop performance, alarm management, energy efficiency, and overall equipment efficiency is not a classic operator task but is becoming more and more important to ensure good production performance. Disciplines such as operations, maintenance, and analytics need to go hand in hand to achieve best results. Many of the tasks either can be performed by centralized internal service centers or can be outsourced to specialized external service providers.

Typical goals are increased throughput, efficiency, and uptime for the production plant. These goals are accomplished by a structured approach to revealing the sources of process variations and upsets and how they are currently handled. By reducing process variations, organizations will increase the operational flexibility, plant regularity, safety, and integrity, while reducing off-spec production, energy costs, environmental impacts, operator stress, and equipment wear.

For example, Dow Chemical introduced a global analytics layer that turns vast amounts of data into information and metrics anyone could see. Experts from a centralized Analytical Technology Center can now support plants globally

To be able to take over when automation fails, operators need higher qualifications and a profound understanding of the technical process, the automation system, and the control modules.

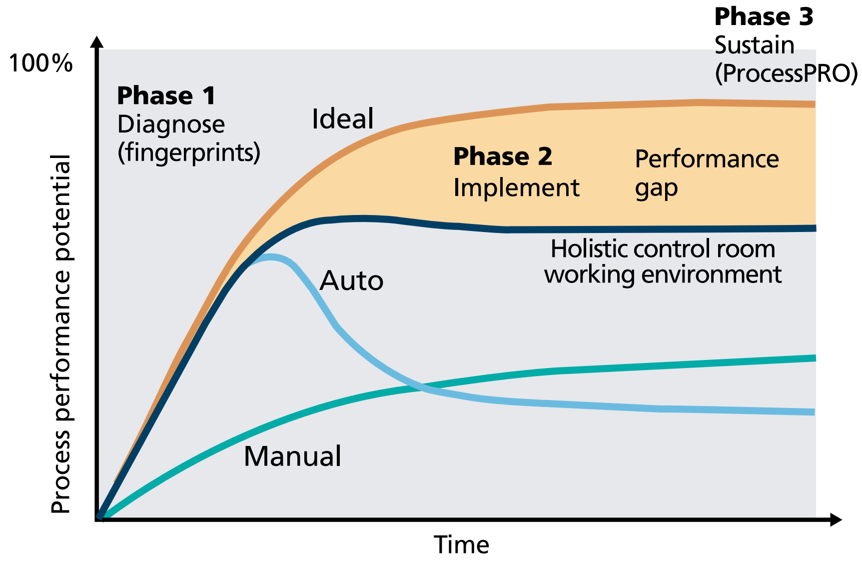


Figure 3. Modern operators should be deeply involved in the optimization of process operations, because such an activity helps to build up the required knowledge that allows them to take over in case of automation failure. Remote expertise should be brought in for all complex and difficult decisions.

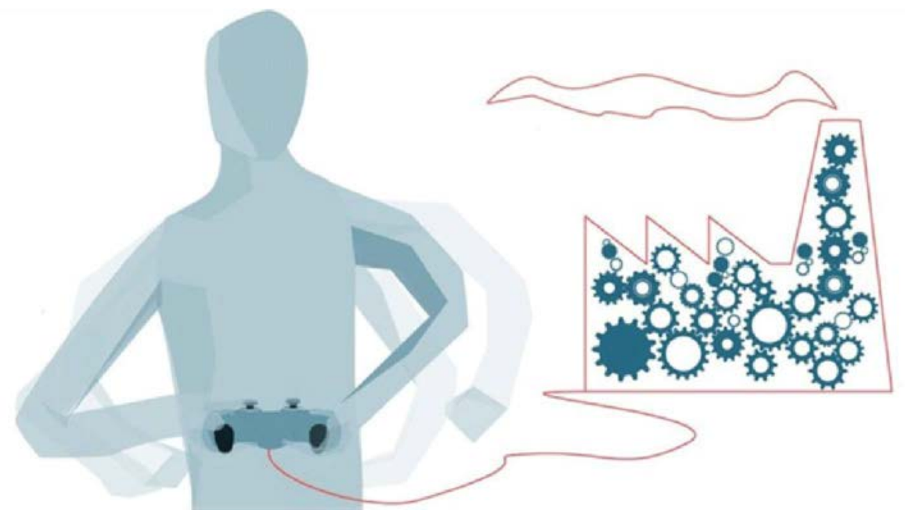


Figure 4. The only way to encourage the next generation of operators to work in control rooms is with a holistic approach to the control room working environment. Introducing gamification can be a motivation for learning, education, and passing knowledge from baby boomers to the gaming and multitasking generation.

to determine manufacturing obstacles, improve efficiencies, and develop best practices. World-class expertise, methods, and tools are now available.

Improving the working environment

As shown in previous sections, most simple parts of traditional operator work have been taken over by automation. Modern operators now have a very different profile. They supervise large numbers of control modules and must be able to quickly diagnose complex situations, collaborate with various support units, and coordinate field operators and maintenance personnel. They decide when it is time to bring in external expertise and manage the temporal integration of remote experts. To make use of their full potential, they need a work environment that really supports their work.

A challenge will be how to design the more collaborative environments that will replace traditional control rooms. Often those centers will no longer be physically close to the process, but they need to be much better integrated with remote service communities in their own company and with service providers and suppliers. New collaboration centers can also be implemented to work through different steps in modernization before the entire technology and organization is ready for all benefits.

The involvement of experienced control room designers from an early stage is even more important in the design of next-generation, collaborative operations centers. They require a totally new approach and "future integration" thinking. As the traditional way of building control rooms becomes obsolete, new best practices will have to be defined.

The new control centers will have fewer operators, and the operator role will evolve from reactive to predictive problem solving and analytic operating. It will become more important to have motivated, stimulated, and more alert operators with better education to deal with increasingly bigger parts of the production process.

The space around the operator will be more connected to many other functions, such as IT/OT support, multifunctional support, technical and remote support, asset risk management, alarms, safety, cybersecurity, and maintenance management, that previously were often separated from the control room operations. More frequent interactive communication with different remote service people to jointly solve troubleshooting and optimization tasks will require a work environment that supports this kind of work as well as if they were in the same room.

These new workflows, still rare today, but which will be the norm tomorrow, have completely new requirements concerning room layout, working zones, screens, cameras, analytical tools, and remote collaboration workspaces. An example of the new design is five traditional control rooms with 12 operators will be replaced by a collaborative center hosting two operators, who will call in remote expertise on demand. The space around the operators will be more connected to many different functions that were previously separated.

There is ongoing research to understand how we can establish an individual health improvement microenvironment that can be adapted to each operator. A typical integrated platform will be much more than an advanced motorized operator desk. This platform is a complete health improvement microenvironment that can be adapted and even automated to change for each individual operator depending on individual needs. For example, the distance between eyes and screens can automatically be adjusted with imperceptible slow speed to release muscle tension in the eyes, and the lighting can shift from warmer to colder light during the day. These are just two examples of how technology can support the health and well-being of the operator.

New technology and big data analytics make it possible to create a data-driven "day by day" improvement program for operators. The new collaborative operations center will turn big analyzed data into actions and, thanks to Industry 4.0, yield benefits by becoming faster, safer, more competitive, and of course more profitable.

New generation of operators

Generational shift will affect business markets and the industry sectors as the older generation (i.e., baby boomers) retires. One challenge will be to attract the next generation of operators, often referred to as Generation Y, the gaming generation, or the multitasking generation, into the control room working environment. An average, a gamer executes up to 300 actions per minute, while a nongamer can perform a maximum 100 actions per minute (figure 4).

Personal ergonomics is becoming more and more important to improve the health and well-being in the control room working environment. Human factor involvement in the early stage of design layout is even more important in future control rooms or control centers with the entry of the next generation into the industrial field. We must seriously consider the needs, requirements, behaviors, and values of the next generation of operators that we need to attract to the industrial world.

The only way to encourage the next generation of operators to work in control rooms is a holistic approach to the control room working environment. Acoustic disturbances will play a key role if operators must share a common working space, communication devices, navigation keyboards, etc.

Improved illumination is another area of concern, because we know that interrupting individual circadian rhythms can have devastating consequences for shift operators. Air quality, heating, air conditioning, and ventilation also matter when enhancing human performance in the control room working environment. Dedicated operator fatigue management minimizes the influence of fatigue.

The knowledge gap is another problem that we will face as baby boomers retire. One way of transferring knowledge from baby boomers to the gaming and multitasking generation is by introducing gamification as a motivation for learning, education, and passing on knowledge. Human-centered design that creates intelligent and individual working places is the way forward to meet these demands for the next generation of operators.

Integrated control centers

With the shift away from traditional control rooms toward integrated collaborative control centers, tomorrow's operators will require a very different skill set, with much more emphasis on cooperation, coordination, analytics, and management. To be able to attract the best operators and offer them an environment where they can consistently bring high performance in 24/7 work settings, the integrated control centers should be designed by experts from the beginning.

New digitalized infrastructures tear down information silos and make world-class remote expertise available. Optimizations previously not possible are coming into reach. ■

ABOUT THE AUTHOR

Martin Hollender, PhD (martin.hollender@de.abb.com), is a principal scientist and project leader at ABB's Corporate Research Center in Germany.

View the online version at www.isa.org/intech/20190602.

Note: This article was adapted from Hollender, M.; Graven, T.-G.; Partini, J.; Schäring, P. Process Operation 4.0. atp edition, 2017, 59, pp. 52–58.

Digitalization delivers value

Creating a sustained competitive advantage

By Duncan Micklem

It seems that every software initiative in the energy and chemical industry is now tagged with the name "digitalization." Yet similar initiatives a few years ago were called Six Sigma or lean manufacturing projects. In essence, they are all focused on operational excellence, but digitalization has risen to the top of the C-suite agenda due to the rapid penetration of new technologies disrupting the way consumers are buying and using everyday products and services.

Music and movies are provided as services that learn about your preferences and those of your peers; they used to be sold as a hardware product that you bought and owned. More and more, people are buying products of all kinds from unknown vendors in far-off locations through trusted online marketplaces. They are delivered to your doorstep, so you no longer have to find and visit a local vendor and hope it has stock on hand. Newspapers and magazines are failing as we consume news and entertainment in real-time through our phones, and often for free. Our cars are mobile information centers with the intelligence to save us from our own bad driving habits. And we can control our homes and maintain their security remotely. The process industries saw this and feared they would be left behind.

In the consumer world, entrepreneurship caused the digital revolution. Consumers benefited from improved efficiency and convenience, greater social connectivity and personal security, and even elevated status. Minor improvements in a consumer's experiences have changed suppliers' business models massively and forever—newcomers have entered from nowhere, and some household names that failed to respond are gone forever (think Blockbuster, Sears, and Toys"R"Us). Some of our kids are growing up knowing nothing different.

The response of the energy and chemical industry is digitalization. In this world, the gains to be had are much more valuable—greater profitability, improved asset performance, and better competitiveness. We can expect much more drastic consequences—hundreds of millions of dollars are at stake, and those who embrace digitalization will prosper. Those who do not respond will indeed be left behind: either consumed by those who do or fatally destroyed in the marketplace.

So digitalization is more than just another Six Sigma or lean manufacturing project. It is an

imperative that is not going away. Digitalization is the scalable application of the *digital technologies* and alignment of the *organizational capabilities* that we believe an energy or chemical process operation should *have and master* with *digital information at the core* in order to *achieve excellence*. All the emphasized words matter.

Applied correctly, digitalization allows a process plant operator to not just manage day-to-day performance of the plant safely and reliably, but also to anticipate and respond to swings in market dynamics. Plant personnel become implementors and supervisors of strategy, rather than number-crunchers or tacticians. Digitalization ensures that the plant will operate at its true optimum, squeezing down on the gap between potential and realized margin. Better and faster decisions will be made, outmaneuvering competition.

For many beginning their digitalization journey, there is a strong pressure to deliver something big using one of the latest buzzwords—Industrial Internet of Things, Industry 4.0, cloud, edge, big data, or analytics. Proponents of this input-oriented approach risk applying technology for the sake of technology, without realizing its true value. Here, we look at outcomes; we explore how digitalization can deliver and sustain true value to the energy and chemical industry.

FAST FORWARD

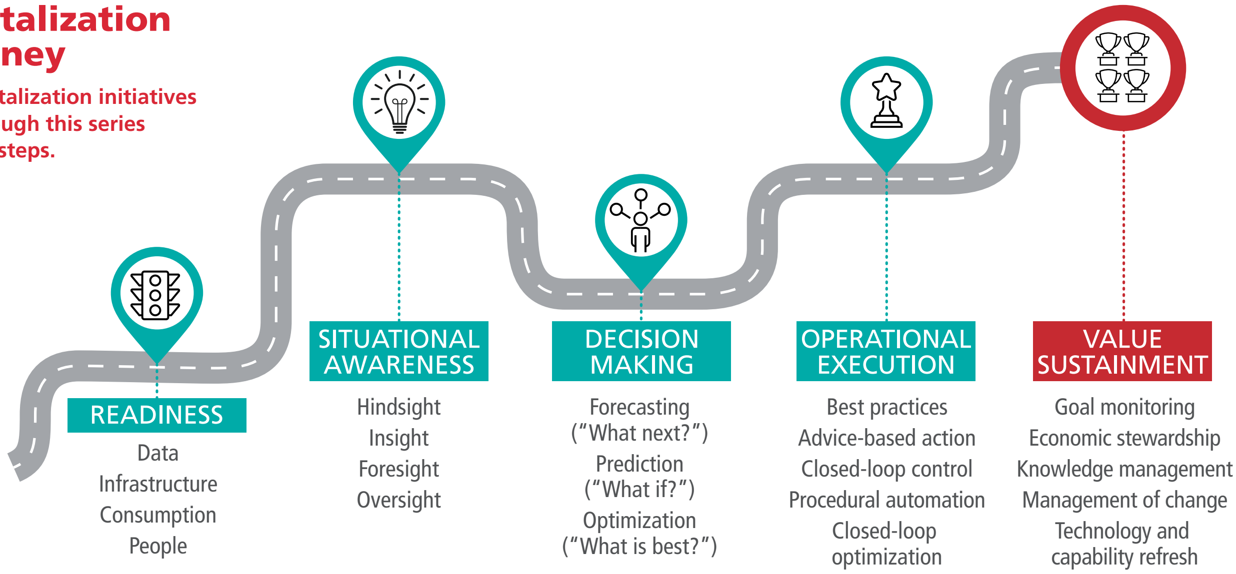
- **Every software initiative in the energy and chemical industry is now tagged with the name "digitalization."**
- **The goal is operational excellence, leveraging new technology.**
- **Digitalization gives process plant operators the opportunity to anticipate and respond to swings in market dynamics to outmaneuver competition.**

Sticking to the map

All digitalization initiatives lie somewhere on the journey shown in the map image on the next page. For any initiative to be successful, no matter where it lies on the journey, the earlier stages must already have been accomplished. For example, most analytics projects ("situational awareness" ambition) fail due to poor data quality (lack of "readiness"); most advanced controls ("operational execution" ambition) are turned off (a sure sign of failure) because their strategy or constraints are not up to date (poor "situational awareness"), so the operator can do better. Let's explore each part of the journey.

Digitalization journey

All digitalization initiatives go through this series of five steps.



READINESS

Frost & Sullivan estimated that process industries use less than 5 percent of the data that is collected—95 percent of the data is either siloed (used selectively), dark (unused), or not consistently in use. Problems of assigning context to data and poor quality have also been identified.

To be ready for digitalization, the impediments to data utilization must be addressed: (a) data readiness (data sufficiency, data trust, data propagation, and data governance), (b) infrastructure readiness (physical infrastructure; security, privacy, and confidentiality; software infrastructure and cloud infrastructure), (c) consumption readiness, and (d) people readiness. A wise approach is to perform a readiness assessment and to tackle any readiness issues before starting (or perhaps in parallel with) a digitalization initiative.

SITUATIONAL AWARENESS

To take the right actions to improve a plant's operation, it is important to understand the potential for improvement. Situational awareness is therefore a crucial step—knowing how the plant is and has been performing in absolute terms ("hindsight"), understanding where it has capacity for improvement versus its constraints and optimal capability ("insight"), predicting responses to changes ("foresight"), and assessing the success and value of such changes ("oversight").

Tools associated with hindsight and insight are largely visual—dashboards, BI tools, spreadsheets. These gain significant value when they align with goals, targets, and constraints. Therefore, to present decision makers with valid information in dashboards, for example, the right tools must be applied to each situation being analyzed.

Analytics are necessary for foresight and oversight, and we also consider them beneficial for hindsight and insight. We are strong believers in using first principles-based analytics tools in conjunction with emerging correlation-based analytics (also known as statistical or stochastic analytics) for situational awareness—a so-called "ensemble approach." First principles tools bring rigor due to their built-in understanding of physics, chemistry, and dynamics, but at the cost of complexity and relatively high computation time. Correlation-based analytics suffer from lower fidelity without any guarantee of feasibility, but with the advantage of simplicity and speed of solution.

DECISION MAKING

In the same way that we recommend an ensemble approach to situational awareness, we also believe that decision making should be grounded on first principles in conjunction with correlation-based tools as necessary. Decision making is about looking for answers. In an operating plant seeking to improve performance, there are three main kinds of answer that can be sought: (a) forecasting ("what next?")—a judgment of what is likely to happen in the future based on knowledge of the past; (b) prediction ("what if?")—an estimate of what will happen in the future based on changes that could be made in the present; and (c) optimization ("what is best?")—an approach that answers the question, "Of all possible changes that can be made, which has the best economic outcome?"

In the energy and chemical industry, there are many complex decisions to be made due to the vast number of variables that can be controlled and the large quantity of disturbances and constraints. Correlation-based decision tools are useful when accuracy is not as important as feasibility and when the answer lies within an already-experienced operating window. However, sloppiness in accuracy comes at a cost—the actual optimal solution is likely worth a lot more than a simply feasible solution. Rigorous models will always find the best answer. Always.

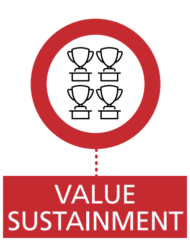
Being ready, situationally aware, and making the right decisions only guarantee success with efficient and effective operational execution. Digitalization compresses time horizons, which means not only doing the same thing faster, but becoming liberated to do completely new things.

The more encompassing the decision, the longer it takes to make and the more economically and organizationally impactful it is, and for a longer time. A wise business decision may reap rewards for years, whereas a poor business decision may have long-term costly consequences.

Automation, on the other hand, by its inherent nature, makes decisions very quickly based on very recent limited data. The scope is typically much more contained, and the automation actions can be suspended or terminated quickly. So, the more informed and timelier the decision process becomes, the more likely the decision will be good, the quicker it will be to execute, and the easier it will be to course correct.

Digitalization accelerates information flow, increases the power of analytics, and automates much of the execution, which greatly condenses the decision/execution time horizons, allowing strategic business decisions to be made in real time, and the results to be visible and available almost immediately.

The tools of operational execution (advice-based open-loop actions, closed-loop control, procedural automation, and closed-loop optimization) start with best practices. Replicating poor or average business processes in a digital environment does not ensure delivery of superior results. The focus should be on acquiring best practices to execute the organization's work, and thereafter on finding the digital means to institutionalize automation of as much of each of these processes as possible.



Digitalization is typically not a one-time hit, where the benefits are achieved and stay forever. Unless proactive steps are taken, benefits will almost always decline over time, and the opportunity to capture incremental benefits will diminish too. This happens for a number of reasons:

- the economic basis for the solution changes
- goals change
- plant performance changes
- business priorities change
- focus by people (management, engineers, operators) changes
- technology changes.

Our approach to sustaining digitalization value entails going above and beyond compliance with how new digital applications are implemented. It is an approach where there is a clear sense of ownership by the organization, especially the front-line operators, through recognition of the added value of the applications.

Achieving this involves goal monitoring and economic stewardship, knowledge management, management of change, and a value-versus-cost mindset around technology and capability refresh.

No doubt this will have a significant cost. However, the value that it unlocks will be orders of magnitude greater, enabling sustainment actions to pay for themselves many times over.

Our organization recently worked with a major multinational oil company that was looking for a flexible, lightweight, and cloud-based solution to manage operating goals and constraints at its western Canada plants. It wanted to ensure its assets were always operated according to best practice, something it had struggled with due to a retiring skilled workforce being replaced by younger, less experienced staff.

Embracing the digitalization concept, the oil company worked with our organization to adopt Operating Goals Manager™ (OGM) as a standard application delivered through a software-as-a-service model. The application allowed users to define measured variables and tasks as indicators. Each of these indicators contained company knowledge, such as reasons for the specific operating envelope; consequences for not addressing an excursion in a timely fashion; recommended actions to address an excursion; and stored company procedures and documents.

As a result, OGM is being used in four gas plants in western Canada as a cloud service, tracking thousands of live indicators in real time and supporting hundreds of users. This is just one example of many where a digitalization strategy has helped improve overall operational excellence.

Do not get left behind

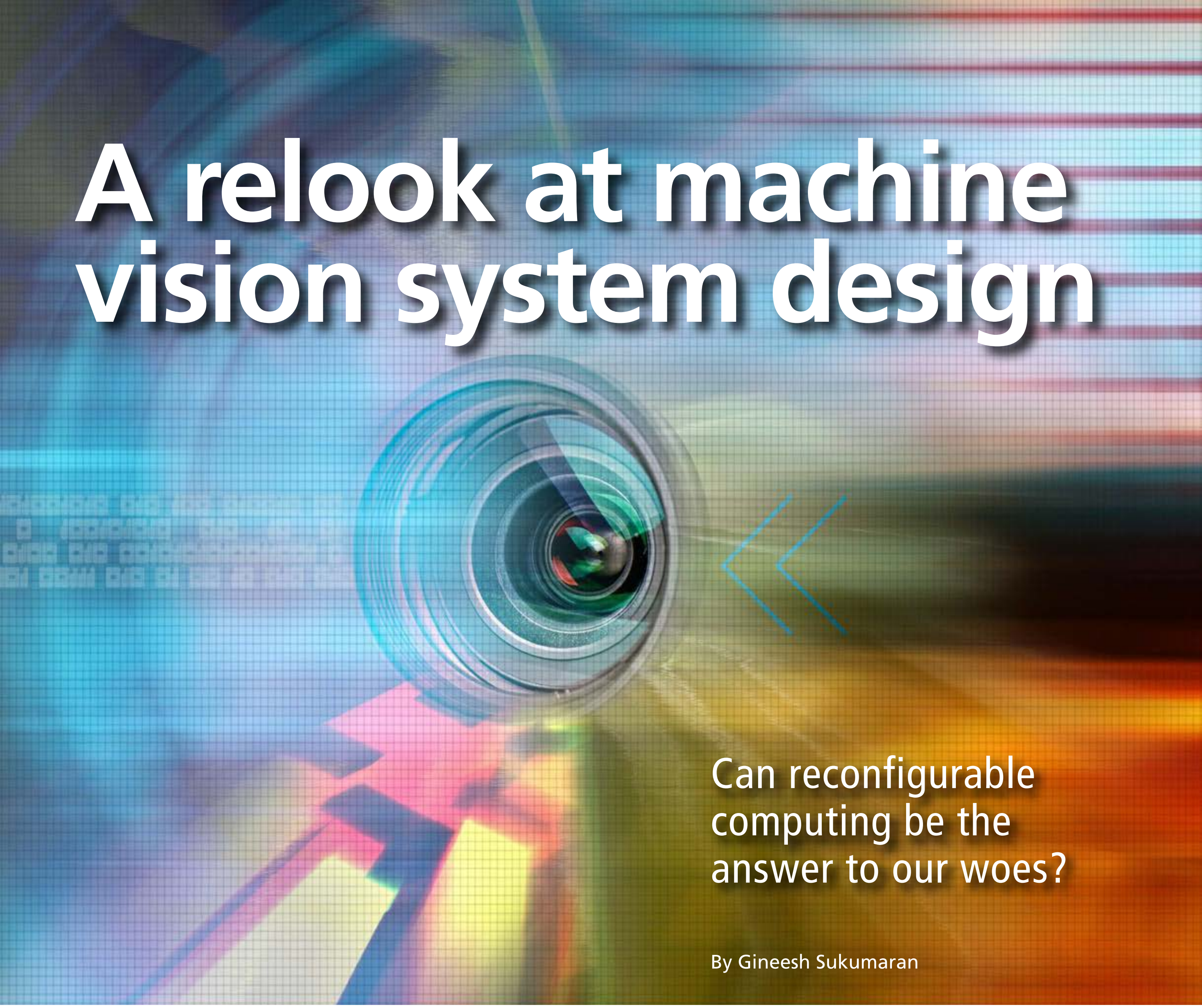
Digitalization creates and sustains competitive advantage and is one of the key strategies a plant can adopt in pursuit of operational excellence. Despite this, many in the industry still remain confused or irritated by digitalization. Some feel it is merely an information technology issue and do not understand its relevance for operations; some are frustrated by the plethora of buzzwords; some see it as hype and fail to see the value proposition.

Digitalization leaders, however, see it as a holistic business issue and are already making huge strides forward in productivity, efficiency, flexibility, and agility. Those who do not realize the value digitalization has to offer risk being left behind. Failure to adapt and transform means that the magnitude of value being lost will continue to increase—the digitally wise will consume the laggards in the market. ■

ABOUT THE AUTHOR

Duncan Micklem (KBC@berkeleypr.com) is the executive vice president, strategy and marketing at KBC, a Yokogawa company. Based in Houston, Texas, Micklem's responsibilities include business planning, M&A/alliances, investment prioritization/capital allocation, and marketing. Micklem has a degree in biology and geography from the University of Exeter, U.K., and an MBA from Cass Business School, U.K.

View the online version at www.isa.org/intech/20190603.



A relook at machine vision system design

Can reconfigurable computing be the answer to our woes?

By Gineesh Sukumaran

Although machine vision may seem like a new concept, we can trace its origins to the 1960s. Back then, machine vision existed as raw image files. A paradigm shift happened with the advent of digital photography. Slowly, companies began developing a software ecosystem that could import these digital photographs and process them in multiple ways.

Alongside superior cameras and greater image processing capability came automation that enabled machines to independently capture images without human intervention. Today, advanced artificial intelligence (AI) and deep learning tools have taken this one step further by augmenting machines with the intelligence to make right decisions based on the images captured.

As machine hardware on the shop floor goes through transformational upgrades, manufacturers want the ancillary things around the hardware to keep pace. Hence, machine vision systems that once took several minutes to compute images are now expected to do the same computation in seconds (real-time computing). A prime example of this is bottle inspections in a soda manufacturing facility. Soda companies use an advanced four-camera system that can inspect a whopping 72,000 bottles per hour.

Why does real-time machine vision need more flexibility?

Engineering real-time machine vision is an extremely expensive process. Several companies have accomplished it by either building dedicated field-programmable gate array (FPGA) systems or installing custom camera systems that have prefed, application-specific integrated circuits (ASICs). The limiting factor here is the need for a dedicated design architecture for every single application. This is expensive and not scalable.

Going back to the soda bottle inspection system, every camera comes fitted with a dedicated ASIC chip. These high-end cameras cannot be repurposed for any other application. To make matters worse, inspection processes and packaging in manufacturing facilities are modified from time to time. Tweaking the vision inspection system to work with the new processes or packaging requires extensive and expensive modifications.

Given these limitations, machine vision systems must be designed so they can be reused for multiple applications and easily modified to meet changing product designs, manufacturing processes, varying components, and business needs.

Reconfigurable computing is the best bet

Selection of computing platforms for automation tasks is often governed by the trade-off between two important parameters: *efficiency* and *flexibility*. The search for a balance between the approaches brings us to reconfigurable computing. Reconfigurable systems are implemented with programmable logic. The best part is that hardware circuits can be easily upgraded to meet the demands of fresh or modified vision applications.

Processors with a fixed architecture allow the user to *temporarily compose* the operations provided by the arithmetic logic unit (ALU). ASIC processors are implemented by *spatially composing* dedicated functional units. Reconfigurable computing uses both *temporal* and *spatial composition*—that is, these systems typically have a programmable hardware logic and a group of programmable interconnection networks. There are several approaches available to accomplish a reconfigurable computing system:

- fine-grained systems: FPGAs and logic gates as programmable elements, connected by switches and wires
- coarse-grained systems: software-configurable processors and a programmable network on chips
- heterogeneous reconfigurable systems: a combination of fine-grained and coarse-grained elements

The ramifications are awesome. Take a traditional packaging vision system that comes with a prefed ASIC in a dedicated camera setup. If the product packaging were changed, new patterns and components were added, or the text on the package was modified, we would need a new ASIC chip for every production line in every manufacturing plant of this company. The costs and time involved in design, fabrication, testing, and rollout are massive.

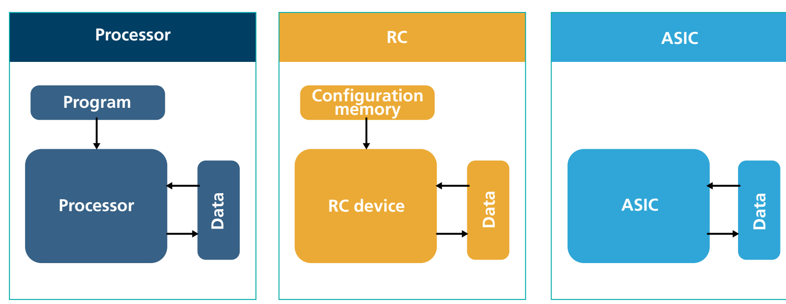
On the other hand, with reconfigurable computing, the camera system can be trained to accommodate modifications to the packaging or the inspection process.

Ideal reconfigurable computing platform

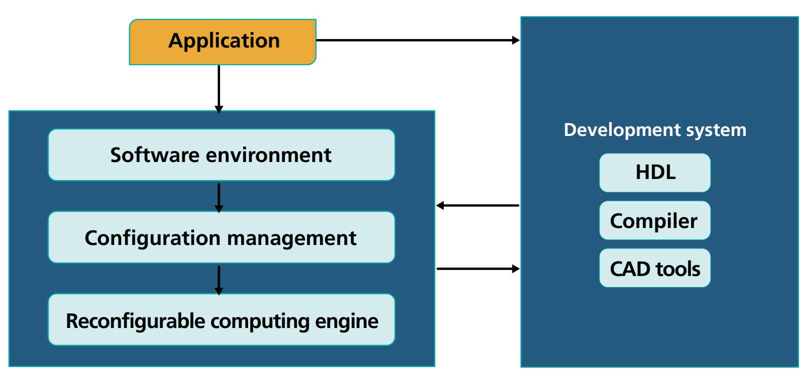
Whatever the approach may be, configuration management and development systems are integral parts of a reconfigurable computing platform.

There are a variety of choices when considering the development of a reconfigurable system. Some of the critical elements to bear in mind when implementing a task on reconfigurable systems are:

- Overhead for run-time reconfiguration: How much additional work needs to be done to use the flexibility offered by the reconfigurable systems?
- Configuration granularity: To what level can an algorithm be decomposed during the imple-



Concept of reconfigurable computing



Composition of a reconfigurable system

FAST FORWARD

- Legacy vision systems are limited by the need for a dedicated design architecture for every application. This is expensive and not scalable.
- We can now deploy reconfigurable machine vision systems that are reusable for multiple applications and can be easily modified for changing product designs, manufacturing processes, varying components, and business needs.
- Advanced AI and deep learning tools have taken this one step further by augmenting machines with the intelligence to make right decisions based on the images captured.

mentation—the number of partitions and their size—which mainly depends on the resources available on the reconfigurable processor.

- Ease of use of SW and development system: This largely depends on how the manufacturer packages different hardware and software elements and provides them to the developer.

Based on the specific requirements at hand, the most appropriate elements can be put together to design an application.

Optimization of vision algorithms

The most important aspect when working on a reconfigurable system has to do with programming the logic to the reconfigurable processor. This requires an understanding of both the platform and industry domain.

Every machine vision system can be considered a pipeline that uses three kinds of algorithms, low, mid, and high, which are classified per the computational characteristics.

- *Low-level vision algorithms*: These are simple algorithms that typically operate on a small neighborhood. Low-level vision algorithms are easy to implement and provide great computational efficiency when operating on a large amount of data. Some typical examples include filtering operations, image enhancement, denoising, and image compression. When processing low-level algorithms, reconfigurable systems are extremely efficient—up to 100 times faster and more efficient than CPU-based vision systems.
- *Midlevel vision algorithms*: Though they operate on a small neighborhood, midlevel vision algorithms are more complex and often require random memory access. Some examples of midlevel vision algorithms include connected component labeling and segmentation and feature extraction techniques. The components that can be in parallel in these algorithms are relatively fewer and are hence not ideal candidates for reconfigurable architectures. It takes a great deal of effort to make reconfigurable processors work with midlevel vision algorithms.
- *High-level vision algorithms*: These algorithms are computationally intensive, nonlocal, nondeterministic, and extremely complex to process. A large majority of the matching, object recognition, classification algorithms, decision making, inferences, and retrieve queries from database algorithms fall under this category. As the number of parallel operations are high, one can implement extremely efficient and flexible systems using reconfigurable processors.

Reconfigurable computing pros/cons

The advantages

- *Increased efficiency*: One of the greatest advantages of reconfigurable systems is the enhanced execution speed with lower power consumption. For manufacturing organizations that deploy hundreds of machine vision systems in their shop floors across the world, the savings are massive.

- *Faster time to market*: As reconfigurable systems can be easily upgraded, a product with reduced functionalities can be quickly designed and released to the market. Unlike ASIC systems, most reconfigurable platforms have simulators that developers can use to swiftly build prototypes and facilitate faster time to market.
- *Lower system cost*: For ASIC and general-purpose hardware, the design costs are high, and the life of the vision product is short. Because reconfigurable systems have flexibility and upgrades, the upfront design costs are substantially lower, and the shelf life of the vision product can be significantly enhanced.

The drawbacks

- *Difficulty in programming reconfigurable chips*: The programming issues in reconfigurable computing involve the placement of the new hardware and routing. Once a new hardware is introduced, the time synchronization between the older hardware system and newly introduced hardware should be factored in. Otherwise, the system can behave inconsistently.
- *Development tools*: The existing development tools in reconfigurable computing require a great deal of manual intervention. Most of these tools are in the development stage and not very mature. Developers need commercial off-the-shelf tools to be able to handle the development and implementation of reconfigurable systems.

Weighing the pros and cons, reconfigurable computing has immense promise in the field of machine vision. As more developers get onboard the reconfigurable wagon, the development and implementation of these systems will significantly ease. ■

ABOUT THE AUTHOR

Gineesh Sukumaran (Gineesh.Sukumaran@Ltts.com) is an image processing and computer vision specialist. He is technical head at L&T Technology Services' Digital Image Processing division and has more than 14 years of experience in the design and development of computer vision algorithms. Sukumaran's research interests include biomedical image analysis, multiple view geometry, and deep learning. He has six patents in this field.

View the online version at www.isa.org/intech/20190604.

RESOURCES

The Current Status of Reconfigurable Computing
https://doi.org/10.3929/ethz-a-004704215

Reconfigurable computing: architectures and design methods
http://www.doc.ic.ac.uk/~wl/papers/05/iee05tjt.pdf

Building reliable visualization and control for industrial edge applications

Increase manageability, flexibility, and reliability using thin-client and virtualization architectures

By Jason Andersen

Industrial manufacturers understand that holding steady is rarely an option. This is because ongoing productivity improvements are a near-universal requirement. Manufacturers can achieve such improvements in many ways, with the most valuable upgrades enhancing several things simultaneously, perhaps across multiple levels of an organization. Today's automation experts are discovering that moving visualization and control functionality toward the industrial "edge" is helping them achieve better operations and improved maintainability, among other benefits.

Production and manufacturing industries have long employed supervisory control and data acquisition (SCADA) applications, human-machine interface (HMI) software, and other automation platforms, such as programmable logic controllers (PLCs) and process automation controllers (PACs). Progressive use of these systems reduces waste, increases uptime, and improves overall equipment effectiveness (OEE).

These systems require some level of "core" server and PC computing power to function, combined with local "edge" computing elements in the field to support visualization and control. With the right pieces in place, organizations attain maximum value. Data from smart field systems has a reliable path to flow to the core, while operators can access the key information required to run the factory in the best way (figure 1).

Standard commercial solutions have often been used to achieve these industrial computing goals. However, a better way is to use redundant hardware and thin-client software optimized for industrial applications. These products help users scale and locate their automation elements anywhere they want with flexibility and high reliability. This article examines why it is compelling to use thin clients at the industrial edge for improving visualization and control.

FAST FORWARD

- SCADA and HMI visualization that are installed closer to the plant floor get information where it is needed, improving monitoring and control.
- Converging IT and OT business units is not the end game, but industrial edge deployments must successfully coordinate both groups.
- Thin-client technology is the preferred way to reliably deploy and manage distributed HMIs and virtual machines throughout a facility.

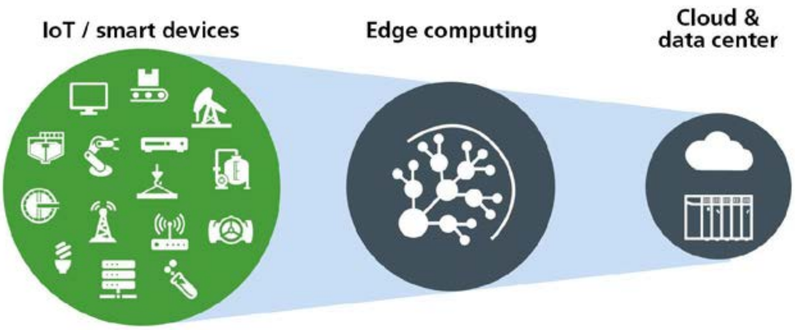


Figure 1. Computing power located at the "industrial edge" occupies a critical region for improving operations by efficiently gathering data and providing visualization when and where it is needed, often by using thin clients.

Industrial edge not an isolated case

Visualization and control computing at the industrial edge is applicable and beneficial to almost all operations. Most edge-located systems, devices, and Industrial Internet of Things (IIoT) sensors have become "smarter" and able to provide extensive data. Improved SCADA and HMI connectivity at the field enables access to this data.

Plants and processes can operate more efficiently when more HMI functions are deployed on the production floor, at field locations, or wherever operators need them. This includes basic process monitoring and control, where operators need an immediate real-time picture of production that is accurate and comprehensive, along with the ability to make adjustments and changes. But it also involves providing visibility into more detailed analytics performed on the big data obtained from field devices. Analytics reveal longer-term trends that may not be addressed by directly observing real-time data, but which informed operators can act upon to improve efficiency.

In addition to operational improvements, other stages of the project life cycle can take advantage of the industrial edge. During design and development, proven edge computing architectures are a structure that can be reused from project to project, leading to design efficiency. The modular nature of edge computing means original equipment manufacturers (OEMs) and system integrators (SIs) can do programming and testing development work on an in-house development platform, and then quickly deploy the results to new and existing field production systems. Fast HMI deployments and mobile capabilities make it far easier to commission new systems and to update existing ones.

Ongoing maintenance is simplified by reliable thin-client devices, which are rapidly replaced and redeployed if necessary. As with commissioning, being able to deploy mobile visualization and computing clients on laptops or tablets gives maintenance crews more options for troubleshooting problems.

Who owns industrial edge computing?

At this point, it is relevant to examine who owns the industrial automation computing structure and how that definition concerns industrial edge and thin-client rollouts. Traditional industrial computing solutions have been heavily based on commercial information technology (IT) infrastructure, and rightly so. Many computing technologies used in industrial applications have trickled down from the commercial world, including PCs, servers, Ethernet wired and Wi-Fi networking, virtual machines (VMs), thin clients, and certain redundancy schemes.

However, manufacturing and process industries are built around the always-on world of operational technology (OT). OT requires much of the computing infrastructure described above, but adds mission-specific hardware, software, and communications methods. This includes PLCs, HMIs, smart instrumentation, and industrial Ethernet protocols.

Figure 2. Purpose-built edge computing platforms, like this Stratus ztC Edge system that operates as a redundant pair of nodes, can withstand challenging environments and are easily deployed and maintained by OT personnel.

Converging IT and OT business units is not the end game, but industrial edge deployments must successfully coordinate both groups. Generally speaking, IT personnel are not trained to work with industrial-specific products. In fact, the industrial network usually must be carefully firewalled from the business network. OT depends on VMs and thin-client technologies, but personnel are often not equipped to manage extensive IT-centric systems.

A workable middle ground is to package IT-centric hardware and software deployment capabilities into OT-focused platforms. In this way, OT personnel can readily operate and maintain IT technologies.

Thin clients aid the edge and core

Traditional automation computing architectures have included both distributed and centralized elements. Purely OT devices, such as PLCs and PACs, have been installed at the industrial edge to interact with field devices like motors, valves, and sensors for gathering information and performing detailed control. These OT assets continue to become more capable. They still play an important role.

Crossing over into the IT realm, industrial automation SCADA and HMI servers formed a "core" above the OT devices, networked to desktop PCs situated throughout the facility as needed. Although this IT-centric server and PC arrangement is functional, this configuration can be cumbersome to manage, because it is relatively expensive to deploy and maintain numerous remote PCs. And now, the growing trend to install control and visualization computing assets out on the factory floor, or even on skids and machines, makes this an even more complex proposition.

A better solution is to maintain centralized redundant server hardware at the core, but use it to host automation-related VMs, while serving up HMI applications to remote thin clients as needed. The servers can be located in a secure computer room or another protected yet remote location like a control room or electrical room. Redundant servers can be traditional IT-centric style or OT-optimized versions tailored for operating in an industrial role (figure 2).

Thin-client technology is the preferred way to reliably deploy and manage distributed HMIs and virtual machines throughout a facility, especially those systems supporting mobile device clients. This means any industrial automation VM or application can be viewed and operated at any PC, panel-mounted terminal, or mobile device connected to the company intranet.

This thin-client architecture brings a better experience at the edge and is far more maintainable by OT personnel responsible for the industrial automation core. Some benefits are:

- *Inexpensive edge:* Edge-located thin clients are lightweight in terms of hardware resource requirements and relatively inexpensive. They can be quickly replaced and reconfigured.
- *App-serving flexibility:* HMI applications can be served to any sort of remote device, such as a PC, panel-mounted terminal, or even mobile devices.
- *Easier development:* Factory development and testing activities can be carried out on a VM environment hosted anywhere; actual field-deployed hardware is not required. This ability is very significant for OEMs and SIs.
- *Rapid integration:* Transferring development configurations to production system thin clients is convenient and quick, especially compared to configuring multiple standalone physical servers and PCs.
- *Simplified maintenance:* Centralized control of VMs is easier than maintaining widely distributed assets that would otherwise require in-person attention for updates and security patches.
- *Scalable:* Thin-client architectures are readily scalable and benefit from centralized standardization and reuse.
- *Verified:* Best practices can be established and maintained across deployed devices, for consistency, reliability, and repeatability.

The preceding benefits are only the basics that standard thin-client configurations provide. Just as the industrial hardware experience can be improved by using OT-optimized servers, so too can the thin-client software experience. Thin-client manager software optimized for industrial users is available (figure 3) and adds the following to enhanced thin-client management:

- *Redundancy:* VM sessions are redundant and can fail on the server side to keep the thin clients running.
- *Shadowing:* Administrators or terminals can view and operate another terminal.
- *Session control:* Multiple sessions can be combined and arranged on a single display.
- *Role-based control:* Organizations can control and manage the content delivered based on login. Certain users can view and control only what they are authorized to see and change.
- *Locational control:* Content can be tailored to the location of the thin client.

Next, let's look at the architectural shift that enables thin-client deployment.

Built for operations

Traditional automation computing architectures commonly employ servers and PCs, while the improved configuration advocated here uses servers and thin clients. On the surface this does not seem like such a drastic difference. However, the distinction is where the computing is performed and how redundancy is carried out.

Classic architectures use servers to perform core supervisory computing services (e.g., VMs for SCADA I/O servers, historians), while remote PCs execute HMI functions and access the servers for I/O points. Reliability is based on dependable servers, redundant networks, and multiple parallel PCs. Careful IT configuration could enable high availability and failover between server VMs, but these would be custom configurations.

On the other hand, thin-client architectures centralize almost all computing on the servers, even the HMI functionality. VM sessions and HMI applications are delivered out to thin clients, with each acting as a window into functionality hosted on server VMs. But because the critical computing core is more centralized, it becomes more important to improve network and server redundancy.

As with classic architectures, the server VMs could be hosted on traditional hardware with customized high-availability configurations, but a better option is to use industrial-specific servers with paired redundant nodes. These systems can load share individual VMs between two nodes, or even assign a VM to one node or the other. In the rare event of any single hardware failure, this type of redundancy has zero downtime.

Furthermore, using industrial-grade thin-client manager software installed on these servers provides even greater reliability. OT-optimized servers and thin-client software are complementary products for visualization and control computing services at the industrial edge.

Closer to the edge

The nature of the production and manufacturing industries, with their emphasis on reliability, means they do not usually employ cutting-edge technologies for automation. However,

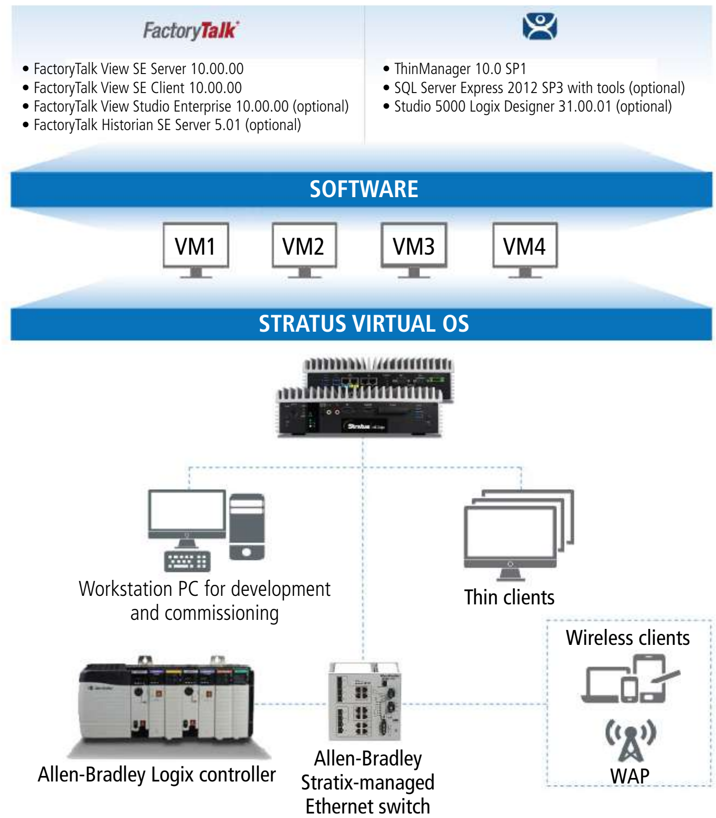


Figure 3. Thin-client deployment is eased by mission-specific visualization and mobility software like Rockwell ThinManager, which delivers content to many forms of computing and mobile devices.

each time industry personnel move ahead on a new project, they are well positioned to survey the technological landscape and make good use of proven technologies. To improve productivity and OEE, end users have recognized a need to enable visualization and control closer to the industrial edge.

SCADA and HMI visualization have been fundamental elements of automation strategies for a long time, but now there are better ways to deploy these systems. Establishing an architecture of redundant servers supporting remote thin clients provides the familiar benefits of SCADA and HMI systems, while allowing them to be easily extended to any location. Content can be delivered to any fixed or mobile device. Thin-client architectures are a modular way for OEMs and SIs to perform development, a rapid way to deploy the work to the field, and a flexible means for operations and maintenance to own and operate these systems for the long haul.

This improved method for visualization and control can be achieved by using customized commercial solutions and carefully coordinating the activities of IT and OT personnel. However, a better approach is to use mission-specific server hardware and thin-client software products optimized for industrial applications—which can be more readily deployed, operated, and maintained by OT personnel. ■

ABOUT THE AUTHOR

Jason Andersen (Jason.Andersen@stratus.com) is vice president of business line management, where he is responsible for setting product road maps and go-to-market strategies for Stratus products and services. Andersen understands both on-premise and cloud-based infrastructure for IIoT and has been responsible for the market delivery of products and services for almost 20 years.

View the online version at www.isa.org/intech/20190605.

Digitize and optimize preventive maintenance for process instrumentation

Defining scope, optimizing tasks, and using digitalization

By Fawaz AlSahan, CAP, SCE

Maintenance can be made more efficient, helping make operations more efficient and profitable, by leveraging new digital technologies. Conventional time-based preventive maintenance (PM) is widely used throughout industry but has shortcomings that can be overcome with smart sensors and analytics (digital transformation). This enables process facilities to move into performance-based and shutdown-based preventive maintenance.

The common categories for preventive maintenance are:

- Time-based preventive maintenance: Conducted as a defined procedure during a preset interval.
- Performance-based preventive maintenance: Conducted when the instrument performance goes below a certain limit. Performance monitoring is done either online (via an online instrument) or off-line (via a portable instrument).
- Shutdown-based preventive maintenance: Conducted during plant shutdown.

The diagram shows the ISO categorization for maintenance in general and preventive maintenance in particular.

It is worth highlighting that conventional time-based preventive maintenance is widely used and has the following shortcomings:

- Forty to 60 percent of PM tasks add no value to operations.
- Some PM tasks are similar.
- Many tasks require removing the instruments or valve to the shop, while condition monitoring is enough to determine reliability.
- New technologies and digital instrument features are not used to optimize tasks.
- Some PM tasks have a high probability of causing unnecessary shutdowns and operation interruptions.

Using smart sensors and analytics (digital transformation) resolves these shortcomings and enables process facilities to move into performance-based and shutdown-based preventive maintenance.

Defining PM scope, tools, and frequency

To have the right preventive maintenance for instrumentation, first clearly define the type and scope of PM. Proper tools need to be selected, and the right frequency defined. The scope of PM can include a certain task to be performed. This can be a time-based visual check, time-based functionality check, removal and overhauling, or a condition-based task.

Second, address who will perform the PM task, such as a field operator or maintenance technician. Determining this point requires agreement between the parties, with clear tasks and a system to collect and communicate the findings.

The tools used for PM tasks are either instrument asset management systems (IAMSs), handheld tools, an instrument built-in keypad, hand tools, or shop activities. The frequency of a PM task is based on prior knowledge from similar equipment, manufacturer or supplier data, reliability data, and performance prediction, and defines the task as online or shutdown activity.

Strategies to optimize PM

Optimizing the preventive maintenance for instrumentation is needed to eliminate unnecessary activities and unnecessary cost. Excessive preventive maintenance may also cause nuisance trips or operation upset. This is another motive to optimize the PM tasks.

Implement optimization with the following strategies: improve the design and apply technologies, capitalize on instrumentation self-diagnostics and online condition monitoring, and use the redundancy approach, once justifiable.

Design and technology

Nowadays, available technologies, like smart sensors, bring a new dimension of reliability and minimize maintenance requirements. Capitalizing on the following technologies and design approach will highly reduce the PM scope and time:

- single-rod, guided-wave radar (GWR) for level measurement
- pressure transmitters instead of process-actuated switches
- smart pressure and vibration fork switches (with display and/or diagnostics) instead of conventional blind switches
- diaphragm/remote seal pressure transmitters instead of tubing-based transmitters
- digital vibration transmitter/switch instead of mechanical switches
- smart valve positioner
- single-rod GWR and two-wire noncontact radar for inventory tanks application
- electrochemical gas detector for H_2S gas detection
- infrared gas detector for combustible gas detection
- configuring a discrepancy alarm between adjacent control and safety transmitters
- avoiding soft-seated control valves and instead installing a metal-seated control valve next to a tight shutoff rotary isolation valve

FAST FORWARD

- Preventive maintenance for instrumentation shall be redefined as periodical, online, or shutdown tasks.
- Achieve PM optimization by enhancing the design, effectively using instruments' built-in diagnostics, and utilizing new or alternative technologies.
- Digital transformation can eliminate or greatly reduce conventional preventive maintenance for instrumentation.

Diagnostics and online condition monitoring

Available instruments are now smart and have internal diagnostics (analytics) and digital communication. These features are effectively used to improve the preventive maintenance program and eliminate or highly reduce traditional practices. Diagnostic data is obtained and collected using:

- smart sensors (like smart transmitters, smart positioners, and smart pressure switches)
- an analytics data platform (IAMS, which receives the data from the smart instruments via a wired or wireless connection and generates a status message with a recommendation)
- digital connectivity, like Foundation fieldbus (FF) with physical layer diagnostics

Redundancy

Redundancy is having a permanent or temporary reference to compare the installed instrument performance and reading to. Below are some examples:

- having dual circuits (or more) for axial and radial vibration, bearing temperature, and fired equipment flame monitoring
- applying two-out-of-two voting, if safe and practical, to avoid nuisance trips and reduce excessive maintenance
- installing control and shutdown transmitters

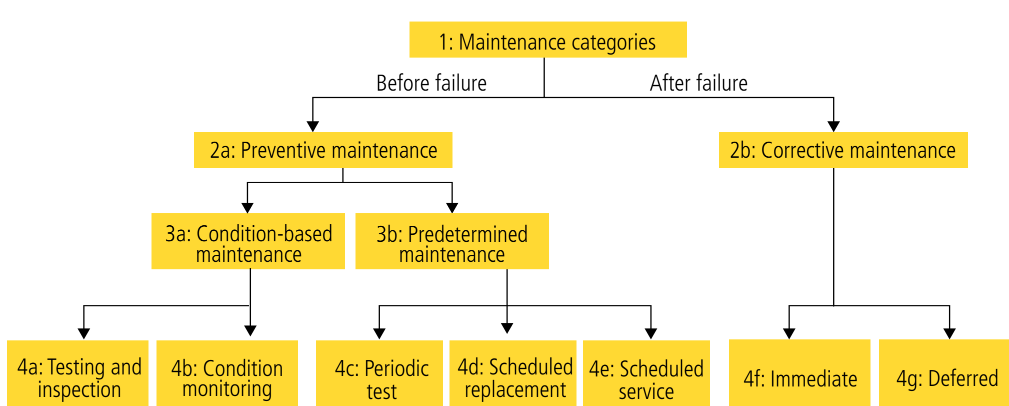


Figure 1. Maintenance categorization
Source: ISO 14224:2016

Recommended preventive maintenance for process instrumentation Part 1

Instrument description	PM task performer	Online/ turnaround	PM interval	Task description
SIS input devices	Maintenance	Online	Per SIL study	• Conduct visual check (leaks, grounding, insulation, cables, terminations and electrical fittings, heat tracing, corrosion, enclosure/cabinet doors). • Zero check and functional check (use IAMS, if available for GWR, noncontact radar, and similar devices)
SIS valve	Operation	Online	Per SIL study	• Conduct visual check and conduct partial/full stroke testing.
	Maintenance	Turnaround		• Conduct full stroke test. • Conduct leak test without removing the valve if possible. • Replace the valve soft parts, per manufacturer recommendations.
Interposing relay	Maintenance	Turnaround		• Conduct functional check for the relay. • Confirm relay mounting and wiring are well tightened. • Inspect relay for any sign of corrosion, color change.
Skid (instrument air/nitrogen/ hydrogen)	Maintenance	Online	Per manufacturer	• Secure a complete set of identical valves for one skid. During PM, remove the complete valve set, replace with the spare set, and return the skid back to operation. • For the removed valves, inspect and replace the valve's soft parts.
Control valve	Operation	Online	Six months	• Visual inspection: Check for leak, vibration, heat tracing and insulation, corrosion, loose wiring, air regulator and filter, pressure gauges, auxiliary devices, hunting. Compare DCS signal versus valve opening, noise, and enclosure tightness. • Stroking if valve at fixed position for long time.
	Maintenance	Online	Two years	• Check diagnostics via IAMS or a laptop. • Apply lubrication per manufacturer recommendations. • Stroke check and leak test prior to T&I.
	Maintenance	Turnaround (based on findings from above task)		• Overhaul and check. • Replace soft parts as recommended by manufacturer. • Conduct functional test. • Perform leak test.

with the same calibration range and configuring discrepancy alarms for them

- having permanently or temporarily installed pressure gauges to compare to the nearby pressure transmitters' readings
- local level gauges (sight glass, magnetic level indicator) or infrared cameras to cross check the level instruments' (displacer, differential pressure, radar, etc.) readings
- checking the online temperature sensor reading with a temperature gauge, a test temperature element, a portable temperature detector, or with an infrared detector/camera.

SIS preventive maintenance

Diagnostics provided by the logic solver, input devices (like transmitters), and output devices (like emergency isolation valves) should support the overall preventive maintenance program for the safety instrumented system (SIS) by reducing the required physical preventive maintenance. The safety requirement specification (SRS) document should be developed after the safety integrity level (SIL) study/verification is conducted. The SRS specifies the required testing intervals for the SIS equipment (logic solver, input and output devices).

To define and further optimize the

$$\frac{PFD_{avg}}{\left[\lambda^{DU} \times \frac{TI}{2}\right]}$$

$$PFD_{avg,\,SIF} = PFD_{Sensors} + PFD_{Logic\ Solver} + PFD_{FE} + PFD_{Power\ Supplies}$$

Safety integrity levels and performance requirements (for the entire system)			
ISA S84 safety integrity levels (SIL)	Safety availability	Probability of failure on demand (pfd) (1 – safety availability)	Risk reduction factor (RRF) or (1/pfd)
3	99.9% – 99.99%	0.001 – 0.0001	1,000 – 10,000
2	99% – 99.9%	0.01 – 0.001	100 – 1,000
1	90% – 99%	0.1 – 0.01	10 – 100
0	Process control – not applicable		

Figure 2. Probability of failure on demand calculation and safety integrity level

required preventive maintenance for SIS devices, do the following for each safety instrumented function (SIF):

- Review the SIL study and SIL verification report or conduct a study.
- Check the test interval (TI) for input and output devices recommended in the study report.
- Increase the TI to the maximum number (such as matching the plant total shutdown interval) and confirm if the SIL requirement is still achieved. The preventive maintenance interval is based on the maximum possible TI.
- For emergency isolation valves, if the TI for these valves (i.e., full stroke test) cannot meet the plant shutdown window, introduce partial stroke testing (PST) with a weight of 60 percent of the total stoke test. TI for the total and partial valve stroke shall then be clearly defined.

Operator tasks versus technician tasks

There should be two different PM tasks. One is conducted by the maintenance crew, and one is conducted by the operation crew. Operation tasks are visual checks, visual inspections, or simple test and observation tasks. The maintenance crew PM tasks include detailed test procedures, calibration, and physical testing that requires hand tools and communication devices.

The objective of segregating the operation and maintenance tasks is to optimize the testing intervals and duration. Some tasks are simple, requiring a long time to prepare the work permit and the system that needs PM. Also, due to the internal mandatory requirements, the operations team must be involved in these PM tasks. Simple examples are stroke testing for control valves and emergency isolation valves and testing gas detectors.

Analysis of PM findings

There is great value in reviewing and analyzing PM findings in terms of preventing failures and maintaining equipment reliability and availability. This requirement is clearly addressed

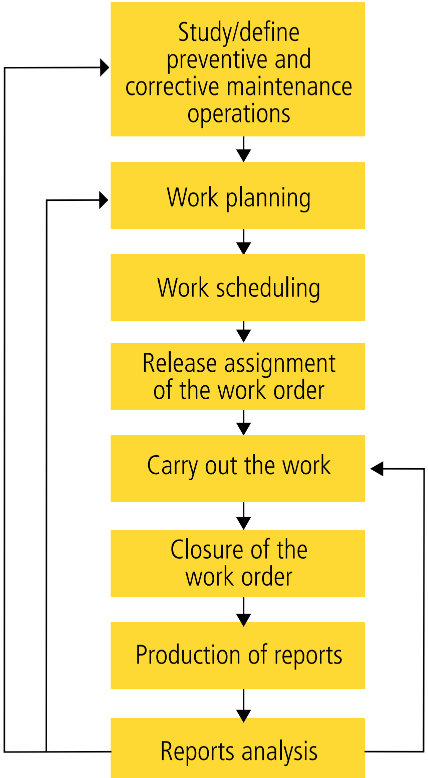


Figure 3. Maintenance work order
Source: EN 13460

Recommended preventive maintenance for process instrumentation Part 2

Instrument description	PM task performer	Online/ turnaround	PM interval	Task description
MOV	Operation		Six months	• Visual inspection, leak, damage, corrosion, enclosure and conduits tightness, integrity of fire-proofing. • Check handwheel, control panel, and remote-control modes. • Check alarm messages. • Conduct partial stroke, if MOV is SIS output device.
	Maintenance		Two years	• Grease per manufacturer recommendation (might be turnaround scope). • Change memory battery.
	Maintenance	Turnaround		• Full stroke • Do leak test. • Check cables/terminations connections and sealing.
Process actuated Switches	Operation	Online	Six months	• Test functionality.
Monitoring/ control transmitters	Operation	Online	Yearly	• Verify level transmitters' readings in comparison with local level gauges, infrared camera, or by dip measurement. • Verify pressure transmitters' readings in comparison with permanently installed or temporary pressure gauges. • Verify temperature transmitters' readings in comparison with infrared portable device or camera or by inserting a temperature element inside a test thermowell.
Flame detectors	Maintenance	Online	Yearly	• Visually inspect flame, leak, damage, corrosion, cables and connection, enclosure tightness. • Visually inspect cooling air and purging air.
Gas detectors	Operation	Online	Per manufacturer	• Test the detector by a test gas and confirm correct alarm settings.
	Maintenance	Online	Per manufacturer	• Conduct detector calibration.

in industry references (figure 3). Doing analysis requires the PM executer to write accurate PM findings. The analysis of the compiled findings helps identify the PM tasks that add value and eliminate the "value-wasting" PM tasks. Also, it helps to identify repeated failures and to recommend revisiting some system designs. Moreover, analyzing PM findings helps improve PM tasks by better managing spare parts, highlighting optimization opportunities and life-cycle costs, and capturing and applying lessons learned across the plant or company.

Impact on instrumentation preventive maintenance

Digital transformation will change the world of preventive maintenance for instrumentation and equipment to more "predictive analytics," where data is used to predict performance and failures. The "big data" collected from the instruments can be used for making decisions about when maintenance is actually needed. Hence, 70 percent or more of conventional PM tasks for both process instrumentation and equipment could be deleted. Digital transformation will address the major maintenance challenges of aging equipment and the aging workforce, and can highly cut cost, time, and manpower.

Recommended preventive maintenance for process instrumentation Part 3

Instrument description	PM task performer	Online/ turnaround	PM interval	Task description
Vibration measuring devices/switches	Maintenance	Online		• Visually inspect damage, corrosion, cables and connection, enclosure tightness. • For switches, portable vibration measurement tool can be used to verify the installed switch reading. • For vibration circuits with dual voting (2 out of 2), PM shall be conducted during turnaround. • For vibration circuits with no-voting (1 out of 1), the following needs to be performed every year: - Check grounding. - Check extension cable and connector for scratches or damage. • Confirm DC voltage at proximate without probe. • Check vibration probe and extension cable resistance. • Clean dirt and grease from the connector by spraying it with an electrical contact cleaner. • Check diagnostics via online asset condition monitoring system/station).
Level gauges	Operation	Online	As needed	• Sight glass: - Retorque overhauled sight glass after plant startup. - Drain and flush. - Check for any leakage and examine for glass cracks. • Magnetic level indicator: - Drain to confirm float is not stuck.
	Maintenance	Turnaround		• Ensure all isolation and vent/drain valves are functional and not clogged. Replace as needed.
Thermowells	Maintenance	Turnaround		• Remove and inspect thermowells for corrosion or cracks.
Pressure gauges	Operation	Online	As needed	• Check the zero-reading of pressure gauges by isolating and draining/venting. Also, compare the pressure gauge reading to a pressure transmitter or pressure gauge next to it. Pressure gauges can be calibrated during plant shutdown.
Process flowmeters	Maintenance	Online	Yearly	• PM task for differential pressure flowmeters: - Inspect orifice in question during turnaround. - Check for leaks and check zero. - Check reading using clamp-on flowmeter. • PM task for inline flowmeters (like ultrasonic, Coriolis, vortex, and magnetic flowmeters): - Conduct zero, if possible, by isolating the flowmeter while it is full of liquid. - Conduct electronic verification or check diagnostics to verify performance and reading accuracy. Obtain details from the manufacturer. - Use clamp-on flowmeter to cross-check the reading.
Flare flowmeter	Operation/ maintenance	Online	Yearly	• Use smart sensor analytics (online diagnostics) or compare to a reference (insertion flowmeter, tracer). • Or collect a gas sample and identify the composition and then calculate sound velocity using the manufacturer software and compare to the flowmeter reading. (This option is for ultrasonic flowmeters only.)

Solutions like wireless instruments, automatic work permits, risk-based maintenance, remote maintenance, robotics, and self-calibrating instruments will be used more and more. Printed PM sheets for equipment and instruments will be replaced by additional smart sensors, like acoustic detectors, video, and infrared cameras. Digital transformation can also extend monitoring into the instrumentation utilities (i.e., the quality of instrument air and power supply).

Digital transformation will also provide more efficient and safer PM by remote condition monitoring and built-in analytics and can provide faster resolutions to problems by having more data and more efficient spare parts management.

Control valves are another beneficiary of digitalization, where the cloud can be used to obtain data from the field, predict the life and performance, and also estimate the time for overhaul. Video and augmented reality, used to monitor and train the maintenance crew on valve maintenance, will be part of this digital transformation.

PM procedures for process instrumentation

This section highlights recommended PM tasks for common instruments. It covers SIS input and output devices, control valves, motor operated valves (MOV), transmitters, gas and flame detectors, thermowells, process flowmeters, flare flowmeters, process actuated switches, level gauges, vibration circuits, and skids instruments.

An analytical approach

This article gave guidelines for digitizing and optimizing the instrumentation PM program, an important task that every company needs to perform to avoid an unnecessary maintenance work load, eliminate operational losses, cut unnecessary costs, and digitally transform conventional PM into analytical maintenance. The scope of this exercise included revisiting the instrument type, PM scope, PM frequency, the PM task performer, and the task sheet.

Using smart sensors and analytics (digital transformation) lets process facilities move into performance-based and shutdown-based preventive maintenance. They eliminate or greatly reduce the conventional preventive maintenance for instrumentation, and replace it with an analytical approach, which uses data to monitor the instrument performance and predict failures. ■

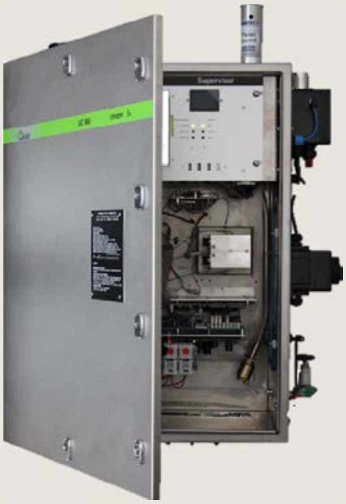
ABOUT THE AUTHOR

Fawaz AlSahan, CAP, SCE (Fawaz.sahan@aramco.com), is the chairman of Saudi Aramco instrumentation standards, a member of the Saudi Arabia Standards Committee of Electrical Metrology, and a voting member of ISO technical committees. AlSahan has more than 20 years of experience in design, technical support, and maintenance of instrumentation and automation systems. He has several published papers, teaches several courses, and holds several patents.

View the online version at www.isa.org/intech/20190606.

New instrumentation products

Gas analyzer for hazardous area zones I and II



To use and valorize natural gas, it is necessary to control its composition. Even if it is composed mainly of methane, natural gas contains some traces of sulfur compounds that can affect its quality and lead to pipe corrosion during transport. Therefore, companies that work with natural gas want to control the level of sulfur compound impurities as well as add specific Mercaptans to odorize the gas and make it easily detectable.

The energyMEDOR measures with speciation the following sulfur compounds generally present in the natural gas: H_2S, DMS, DMDS, and Mercaptans. This instrument works in hazardous areas, such as ATEX zone 1 without any purge gas requested for operation.

The MEDOR Ex d uses MEDOR wet cell detector technology to analyze these sulfur compounds in hazardous areas without purge gas. The instrument needs only a very small amount of zero air or nitrogen to operate (down to 4 mL/min), and the wet cell Sulfur Specific Detector detects sulfurs as low as 1 ppb. This certified analyzer can operate in zone I and II and can be used with 230V, 115V, and 24V DC power supplies.

Chromatotec, www.chromatotec.com

Point level switch

The Nivector FTI26 point level switch detects all types of powdered and fine-grained solids, such as plastic granules, detergent, grain, sugar, and other dry materials. The switch can be installed at the top of a tank to indicate high level, or at the bottom of a tank to indicate low level. The switch is a capacitance device that fulfills all hygienic requirements, such as 3A, EHEDG, and FDA. It is cleanable up to protection class IP69. No additional or individual adjustments to different media are necessary. The function of the switch can be checked via LED signalization without dismounting the device.

Endress+Hauser, www.us.endress.com

Two-wire loop-powered Coriolis transmitter

The Micro Motion 4200 two-wire loop-powered Coriolis transmitter can replace existing two-wire flow devices. The device can accommodate a line size of 4 inches and has an onboard real-time clock for diagnostics. The unit is available in a remote-mount option for applications that require the transmitter to be located separately from the sensor. The 4200 transmitter provides a viable migration path where Coriolis meters were previously not practical as a two-wire solution.

Emerson, www.emerson.com

Bassett named chief editor of *InTech*

Renee Bassett has been named chief editor of ISA's *InTech* magazine and Automation.com digital content-delivery site for automation professionals. Bassett replaces Bill Lydon, who will continue with the publications as contributing editor.

Bassett joins ISA's team of publishing professionals that includes Lydon, ISA's group publisher Rick Zabel, and content editor Cory Fogg. In her role, Bassett will work with Zabel to determine publication and content strategy, develop content, and manage the publications' contributors, staff, and production processes. Bassett will be based in Nashville, Tenn.

Bassett is an expert content creator, media manager, and marketing communications specialist in the areas of industrial manufacturing, technology, and automation. She possesses more than 20 years of experience in content generation for technical and nontechnical audiences. Over the course of her career, Bassett has provided her services to leading automation publications—including *Automation World* and *Control Engineering*—and developed and implemented media and communications programs for many industrial automation companies. ■

ISA director of strategic initiatives awarded SANS ICS Lifetime Achievement Award

At the SANS ICS Security Summit in March, ISA director of strategic initiatives Marty Edwards was honored by his peers with the SANS ICS Lifetime Achievement Award.

This award recognizes individuals who have contributed exceptional efforts to enhance the security of industrial control systems on an international scale, and who actively strive to bridge the gap between information technology (IT) and operations technology. Through educational contributions to the community, honorees have significantly increased the awareness of risks to industrial control systems (ICSs) and fostered the idea that cybersecure ICS implementations and defense in ICS are achievable.

"Marty's unwavering commitment to his mission to help industries mature and better defend ICS from evolving cybersecurity threats continues to have an unmistakably positive effect on society," said Mike Assante, director of critical infrastructure and lead for the ICS curriculum at SANS Institute. "His active involvement in the community has made industrial cybersecurity a mainstream topic worthy of attention at the highest levels of government and with public and private companies alike."

As director of strategic initiatives at ISA, Edwards works with government and industry leaders throughout the world to broaden understanding and implementation of the ISA/IEC 62443 cybersecurity standards. These internationally recognized standards are key components of *The Framework for Improving Critical Infrastructure Cybersecurity* (updated April 2018), a how-to guide developed through the U.S. National Institute of Standards and Technology to help strengthen the cyberdefenses of critical infrastructure.

Before joining ISA in mid-2017, the 25-year industry veteran was the longest-serving director of the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Under his leadership, the ICS-CERT was awarded the 2013 *SC Magazine* Security Team of the Year Award and was named as a finalist in the community awareness category in the 2015 Government Information Security Leadership awards.

Edwards also served as a program manager focused on control systems security at the Idaho National Laboratory and has held a variety of roles in the instrumentation and automation fields. He holds a diploma of technology in process control and industrial automation (magna cum laude) from the British Columbia Institute of Technology and in 2015 received the institute's distinguished alumni award. In 2016, Edwards was recognized by FCW in its "Federal 100 Awards" as being one of the top IT professionals in the U.S. federal government.

Edwards is currently the managing director of the Automation Federation, founded by ISA in 2006. This association of nonprofit member organizations is dedicated to fostering economic growth and manufacturing innovation by helping industry harness the immense capabilities and potential of automation technologies and applications. ■

ISA supports Cyber Shield

In April, ISA provided operational technology (OT) training in support of the U.S. Army National Guard's national cyberoperations exercise, Cyber Shield. Cyber Shield 19, held at Camp Atterbury, Ind., brought together approximately 800 Army and Air National Guard network defenders and world-class cybersecurity professionals, industry network owners, and others to train the next generation of cyberwarriors.

"The training that soldiers and airmen obtained through Cyber Shield 19 and the National Guard adds to their ability to conduct their civilian jobs, and, vice versa, the training and experience they receive in their civilian positions strengthen the military's cyber capabilities. They become very valuable assets in protecting critical infrastructure," said George Battistelli, the Army National Guard Cybersecurity program manager, information technology strategy division chief, and the Cyber Shield 19 exercise director.

Cyber Shield includes a critical training component with courses and seminars organized into tracks based on the roles of the participating cyberteam members.

"We focus on getting people prepared for cyberdefense," said Col. Teri Williams, commander, Cyber Shield 19. "There are a lot of people we bring to the table for that first week of training. Microsoft, CISCO, and SANS are on hand for some of the cyberdefensive training. The International Society of Automation provides ICS/SCADA network training. We also focus on the offensive side. Our belief is that the better that you are trained on the offensive side the stronger a defender you will be."

ISA was selected by the National Guard because of its leadership and experience in developing the world's only consensus-based series of industrial cybersecurity standards, ISA/IEC 62443. These standards, which also serve as the basis for ISA cybersecurity training, protect the industrial automation and control systems and networks that operate OT machinery and associated devices within critical infrastructure. ■

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

In the first order process with dead time model (FOPDT), the process gain *Kp* is defined as:

A. $Kp = \dfrac{\text{change in controller output (in eng.units)}}{\text{change in process variable (in eng.units)}}$

B. $Kp = \dfrac{\text{change in controller output (in \% of range)}}{\text{change in process variable (in \% of range)}}$

C. $Kp = \dfrac{\text{change in process variable (in eng.units)}}{\text{change in controller output (in eng.units}}$

D. $Kp = \dfrac{\text{change in process variable (in \% of range)}}{\text{change in controller output in (in \% of range)}}$

CAP answer

The correct answer is D, Kp = change in process variable (in percent of range)/ change in controller output in (in percent of range).

The process gain indicates the relative change in process variable (PV) that results from the response to a change in the controller output (CO). Both PV and CO are expressed in percent of range to ensure the calculation is not dependent on the engineering units chosen. ■

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.

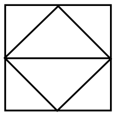
CCST question

As outlined in ANSI/ISA 5.1-2009, *Instrumentation Symbols and Identification*, an instrument that is monitored on the control system HMI and is part of a safety instrumented system (SIS) loop would be represented by which type of symbol on a process and instrumentation diagram?

A. A circle contained in a box with a horizontal dashed line through the circle.
B. A hexagon with a double-dashed line through it, not contained in a box.
C. A diamond contained in a box with a horizontal solid line through the diamond.
D. There is no representation for a SIS instrument given in ANSI/ISA 5.1-2009.

CCST answer

The correct answer is C, "A diamond contained in a box with a horizontal solid line through the diamond."



The diamond symbol was first defined for safety instrumented systems with the release of ANSI/ISA 5.1-2009. Per previous releases, a box around the instrument "bubble" with a solid horizontal line through it indicates that the measurement or control element is normally accessible to the operator from the main operator console, typically a human-machine interface (HMI) screen in modern control systems. ■

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

Single-loop control—Still the mainstay of advanced process control

By Jim Ford, PhD

Just over a decade ago, an article titled, "Advanced Control Strategies Move into the Field" (*Control*, October 2008), highlighted three evolving trends in the process control world that would "make our dependence on single-loop control part of history." The three trends cited were the:

- movement of APC controllers to the field control devices
- increased availability of inexpensive sensors
- increased use of fieldbus and wireless in the control network.

Ten years later, how much of this prediction has come true? Predictably, not much. And, why?

Single-loop control (i.e., a control loop with one input and one output) as implemented in various versions of the proportional, integral, derivative control algorithm in modern distributed control systems has two primary functions:

- servo-control—reacting to changes in the set point (SP) to move the process variable (PV) to its new target
- feedback control—reacting to changes in the PV to return the PV to SP

Servo-control is easy. Choose the right amount of integral action (in combination with the gain action, and with or without gain action on SP changes), and the control algorithm will adjust its output (OP) to move the PV to its new target at the chosen rate with or without overshoot, as desired.

Feedback control is much more important and more complex. It is the *only* mechanism in the entire process control world that can react satisfactorily to changes in unmeasured disturbance variables, such as changes in ambient temperature, rainfall, stream composition, pump load, exchanger fouling, field operator moves, board operator moves, and many others.

APC technological advances

Advanced process control (APC) got its start and made its mark in the 1960s primarily by reacting to *measured* disturbance variables. This "reaction" was coined *feedforward control*. If a disturbance variable to a unit operation can be measured, then the key control variable (CV) for that operation can be kept close to its SP by adjusting the associated manipulated variable (MV) using a simple "model."

For example, consider a catalytic reactor where the key CV is the reactor inlet temperature, which is controlled at the basic level on feedback by adjusting the fuel flow to a fired heater. If the reactor feed rate changes, then a feedforward controller can adjust the fuel flow (the MV) using a dynamic model between the feed rate and the fuel flow. The intended result is little or no change in the reactor inlet temperature (the CV)—the primary benefit of *all* APC—a reduction in process variance.

Initially, feedforward control was implemented using one input – one output relationships. As the technology developed in the 1970s and 1980s, more complex approaches and strategies developed, involving multiple inputs and outputs with more complex models. Eventually, multivariable, model-predictive control replaced simpler APC approaches and algorithms for both feedforward and feedback control of complex process control applications.

But, throughout the past 50 years of APC technology advances, those *unmeasured* disturbances have not gone away. The APC controllers can now be implemented in field control devices (trend number 1); there are cheaper sensors (trend number 2); and fieldbus and wireless (trend number 3) are now realities. But none of these technological achievements have been able to mitigate the process instabilities created by unmeasured disturbances. Their presence still confounds the most experienced control system engineers. That is why single-loop control is still the mainstay of process control, and why those trends discussed earlier (or any others) will never result in APC being implemented successfully in its absence.

If APC needs single-loop control to reject unmeasured disturbances, then how best to utilize it?

APC control objectives

The most important APC control objectives are related to production rate and product quality, because these variables are directly related to operating profitability. Production rate is limited by constraints (e.g., maximum temperature and control valve position). Product quality is normally controlled by temperature, analyzers, lab analyses, or indirectly by "soft sensors" (inferred properties). Vessel levels are integrating, inventory-related variables and are almost never included as CVs in an APC controller. The same can be said for vessel pressure, unless it is a constraint variable related to pushing the production rate. (There are some exceptions—fired heater controls often use burner pressure as a substitute for fuel gas flow to control heater temperature.)

The lone outlier is flow, which is a true "extensive" variable, independent of product quality or operating profitability. In all but truly exceptional cases, flow is *always* adjusted to achieve some other process control objective. It is almost always the secondary, or *slave*, in a one-on-one basic cascade. If the flow controller is standalone, then its SP is adjusted by the operator (or an APC controller) to achieve a higher-level control objective.

At the same time, the flow controller is a true mitigator of unmeasured disturbances. It is typically characterized as a high-frequency loop, meaning that a change in OP is followed almost immediately by a change in PV. When tuned properly, and when challenged by unmeasured disturbances, it returns the PV to its SP very quickly and with little overshoot or oscillation. As such, it is normally the variable of first choice as an MV for any higher-level control strategy, especially for an APC controller.

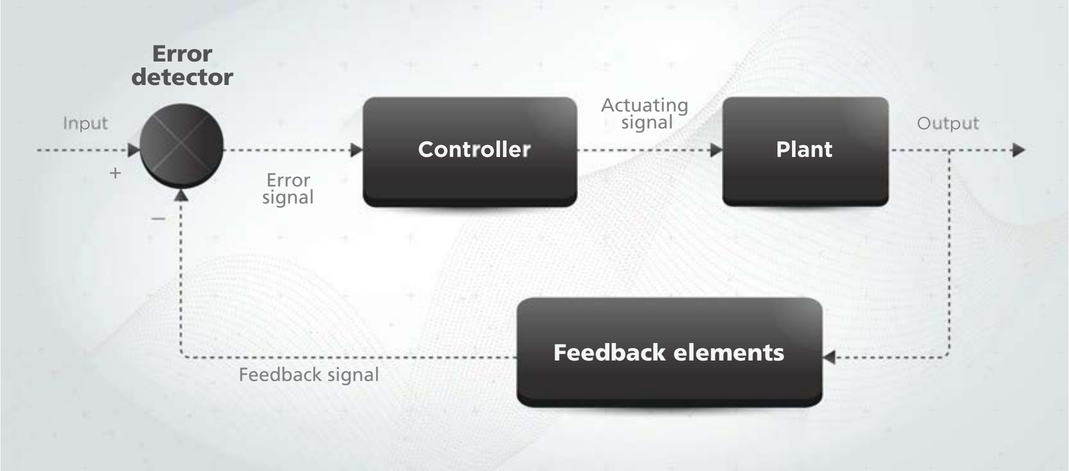
There are some exceptions. Although flow is a true extensive variable, there are instances where it can be used to "create" an intensive variable. Ratio variables are used quite often in process control. For example, reboiler duty on a distillation column can be calculated from flow and temperatures and then ratioed to the column charge rate. The column reboiler duty/charge ratio can then be used as an MV in an APC application. Same for treat ratios in absorbers, product yields in fractionators, and so on. The single-loop flow controller rejects unmeasured disturbances and thereby stabilizes the created intensive variable.

Status quo: Do not disturb

Today, even after 50 years, APC continues to rely on the lowly flow control loop, the most basic single-loop control, as the best rejector of unmeasured disturbances and the most stable platform for the APC/optimization control hierarchy. So, the next time somebody suggests getting rid of single-loop control in an APC application, just ask, "What about unmeasured disturbance variables?" Do not expect a righteous reply. ■

ABOUT THE AUTHOR

Jim Ford, PhD (jim.ford@mavtechglobal.com), is a senior consultant at MAVERICK Technologies, a platform-independent automation solutions provider offering industrial automation, strategic manufacturing solutions, and enterprise integration services for the process industries. Ford specializes in advanced process control, control system engineering, and execution of detailed control system modernization and migration front-end loading evaluations.



Single-loop control (shown) is the mainstay of process control, and APC can never be successfully implemented in its absence.

Building a cybersecure manufacturing strategy

By Bill Lydon

ABOUT THE AUTHOR

Bill Lydon (blydon@isa.org) is an *InTech* contributing editor with more than 25 years of industry experience.

I was fortunate to have the opportunity to talk with Dawn Cappelli, an experienced and accomplished cybersecurity expert, who shared her advice on building cybersecure manufacturing organizations. Cappelli is vice president, global security, and chief information security officer at Rockwell Automation.

Before coming to Rockwell, she was founder and director of Carnegie Mellon's CERT Insider Threat Center. Cappelli is recognized as one of the world's leaders in insider threat mitigation and has worked with government and industry leaders on national strategy issues. Cappelli is a certified information systems security professional (CISSP), and she has a BS in computer science and mathematics from the University of Pittsburgh. Cappelli came to Rockwell Automation in 2013 as director, insider risk, and built the company's insider risk program. Her team is responsible for protecting Rockwell Automation and its ecosystem of customers, suppliers, distributors, and partners from the ever-changing global cyber-threat landscape.

I asked Cappelli what first steps a manufacturing company should take on the journey to achieve cybersecurity protection. She shared her experience, insights, and recommendations for creating a comprehensive industrial cybersecure manufacturing organization.

The first step a manufacturer should take is to determine the leader of the cybersecurity effort. Cappelli noted that many manufacturing companies already have a chief information security officer (CISO) responsible for information technology (IT) security, but traditionally operational technology (OT) security has been the responsibility of the OT engineers. "People are realizing now, due to the convergence of IT and OT, that it's important to have one security leader responsible for all cybersecurity for the company." This is someone who can work with both IT and OT to build and execute a holistic cybersecurity strategy that encompasses the entire ecosystem of not only IT and OT, but also of all external connections, including third parties and the supply chain.

Cappelli described the industry trend of CISOs being given responsibility and/or accountability for all cybersecurity for the company. One reason why is that cybersecurity in IT is significantly more mature than in OT, and someone with IT security experience understands how to methodically build the cybersecurity program across the organization using a risk-based approach.

One of the challenges is building a cross-functional team including both IT and OT, since traditionally they have not worked closely together. Cappelli recommends using the NIST Cybersecurity Framework (NIST CSF) (www.nist.gov/cyberframework) as a tool to deploy a focused process and involve all parties. The framework helps to identify gaps in cybersecurity strategy and becomes the blueprint for risk assessment. Bringing together cross-functional personnel consisting of IT and OT experts, plant experts, and plant engineers using the NIST CSF focuses the activity and fosters team building based on shared goals. This process for building the strategy creates a shared vision and understanding of all stakeholders' challenges and ongoing positive working relationships.

"People are realizing now, due to the convergence of IT and OT, that it's important to have one security leader responsible for all cybersecurity for the company."

—Dawn Cappelli

An important part of this process is prioritizing cybersecurity efforts based on risk. This helps companies prioritize investments, because it is typically impractical to do everything at once.

I asked Cappelli for any tips based on her experience building the Rockwell Automation program over the past few years. She suggests starting first in the IT group to "get your feet wet" if you have not yet used the NIST CSF, then use the NIST CSF Manufacturing Profile to create your manufacturing security strategy. Also, the NIST CSF helps to identify some quick wins for the manufacturing environment, like ongoing communications to maintain security awareness among plant personnel. Rockwell Automation has done this with a monthly cybersecurity awareness bulletin to reinforce topics like the importance of physical security, social engineering, not sharing passwords, and safely using USBs. ■

RESOURCES

NIST Cybersecurity Framework
www.nist.gov/cyberframework

ISA Cybersecurity Resources
www.isa.org/technical-topics/cybersecurity/cybersecurity-resources

The changing role of the control system engineer – Advanced technology and control system basics

By Michael McEnery

The rate of change for new technology in the world of control system engineering is staggering and can be overwhelming if you do not step back to see the forest for the trees. The role of a control system engineer (CSE) is changing with this technology and the cost of its implementation. Hardware and software vendors continue to develop products that are more cost effective—from both product cost and implementation cost perspectives.

Do not forget that a significant cost of a product is the time required by a CSE to implement it. And let's face it, we are well paid, particularly in North America and Europe. As cool as you might think the latest tool from your software vendor is, part of the reason it exists is to reduce your cost. Overall hours required for the development phases of automation projects (programmable logic controller programming, human-machine interface [HMI] programming, device configuration) have decreased drastically over the past 15 years.

Technology also brings opportunities for offshore system development, which further decreases the time CSEs are spending with program development. At the same time, new tools provide opportunities for CSEs to deliver even more value. Data historians; Industrial Internet of Things; data analytics; advanced process control; proportional, integral, derivative (PID) autotuning; and PID loop performance monitoring are all available to help CSEs save energy, increase plant uptime, reduce material costs, etc. But these tools have no value until they are put to work by someone who understands the processes being controlled. This places a stronger emphasis on understanding process control basics. It requires getting away from the keyboard and out onto the plant floor.

These tools have no value until they are put to work by someone who understands the processes being controlled. This places a stronger emphasis on understanding process control basics. It requires getting away from the keyboard and out onto the plant floor.

Control system integrators also have new opportunities for project management, design, and documentation. End users have fewer resources available for projects, and the people who are assigned have less and less time. But a successful project still requires someone to understand the process requirements in detail and to communicate effectively to the project team regarding design. Again, this goes back to the CSE having a strong understanding of process design and process control.

So, the next time you start to stress about a new version of an HMI or a just-released series of I/O modules, take a step back and make sure you are also acquiring knowledge about how the equipment you are controlling actually operates. And how it can operate better. ■

ABOUT THE AUTHOR

Michael McEnery (MikeM@McEneryAutomation.com) is the president of McEnery Automation, a CSIA certified system integrator. Founded in 1994, the Control System Integrators Association (CSIA) is a not-for-profit professional association of more than 500-member companies in 40 countries advancing the industry of control system integration (www.controlsys.org).

ISA99 to develop report on IIoT cybersecurity

ISA99, *Industrial Automation and Control Systems (IACS) Security*, has begun work on an ISA technical report to be titled, Applying ISA-62443 to the Industrial Internet of Things (IIoT). Coverage will include general categories of IIoT devices within IACS, cybersecurity challenges, and rates of adoption in industry. The report will then serve as a guide in determining if any new and related ISA99 work products are required.

The technical report will be the first work product of Working Group 9, *IIoT and Security*, which was established by ISA99 to analyze the specific characteristics of the IIoT in terms of threats, attack surface, and vulnerabilities, and to examine whether the approach developed by ISA99 for securing a conventional IACS is appropriate and sufficient for IIoT. This assessment is vital, as the IIoT is a specific case of IACS with a very wide range of objects, an extended surface area, and a high scalability, resulting in a very large attack surface and new vulnerabilities. The working group will first examine the specific risks and new forms of attack to which the IIoT may be subject.

This project is one of numerous current development activities within ISA99 to support and advance the widely used ISA/IEC 62443 series of standards on IACS security. The standards are developed primarily by ISA99 as American National Standards, with simultaneous review and adoption by the Geneva-based International Electrotechnical Commission (IEC) through IEC partner committee TC65, *Industrial-Process Measurement, Control and Automation*. With more than 900 members, ISA99 draws on the input of cybersecurity experts across the globe in developing the standards, which are applicable to all industry sectors and critical infrastructure in providing a flexible and comprehensive framework to address and mitigate current and future security vulnerabilities in IACS.

ISA99 Working Group 9 is cochaired by Suzanne Lightman of the U.S. National Institute of Standards and Technology, and Eric Braun of Emerson Automation Solutions. For information on ISA99, contact Eliana Brazda, ISA Standards, ebrazda@isa.org. For information on viewing or obtaining the ISA-62443 standards and technical reports, visit www.isa.org/findstandards. ■

New ISA5.9 project to focus on controller algorithms and performance

The time-honored proportional, integral, derivative (PID) algorithm is used in a vast majority of applications for basic control and in many for advanced control. However, there appears to be a widespread lack of understanding of the different forms, structures, and features, and of how performance objectives determine appropriate choices. Consequently, most of the capability of the PID is underutilized, reducing process safety, efficiency, and capacity, points out ISA Fellow, author, and mentor Greg McMillan, a widely recognized expert on process control who received the ISA Lifetime Achievement Award in 2010.

This concern prompted McMillan to propose a new ISA standards project on controller algorithms and performance, which has led to the recent formation of ISA5.9, *Controller Algorithms and Performance*. The new working group will function under the ISA5 committee, *Documentation of Measurement and Control Instruments and Systems*.

ISA5.9 will seek to clarify the algorithms used in industrial control systems to aid in their selection and application to improve manufacturing processes. The working group will develop technical reports, recommended practices, and standards documenting the algorithms used in industrial control systems and the measures of performance for those algorithms. The documents may include guidance on algorithm selection.

ISA5, the oversight committee for ISA5.9, is also responsible for the widely used standard ISA-5.1, *Instrumentation Symbols and Identification*. The committee is chaired by former ISA Standards & Practices Department vice president Tom McAvinew, co-author of the ISA book *Control System Documentation: Applying Symbols and Identification*.

The ISA5.9 cochairs are Yamei Chen of Eli Lilly and Company, Indianapolis, and Michel Ruel of BBA, Québec. Those who are interested in participating in the new ISA5.9 are asked to contact Charley Robinson, ISA Standards, crobinson@isa.org. ■

New control valve terminology standard

ISA75, *Control Valve Standards*, has completed a revision of ISA-75.05.01, *Control Valve Terminology*. The standard provides a glossary of definitions commonly used in control valve applications across industry. The standard includes a number of new or significantly revised terms, including backlash, cage guiding, intelligent/smart positioner, quick change trim, globe valve body, hysteresis, port guiding, and post guiding.

ISA75 is chaired by James Young of the Dow Chemical Company. For information on ISA75, contact Eliana Brazda, ISA Standards, ebrazda@isa.org. For information on viewing or obtaining ISA-75 standards and technical reports, visit www.isa.org/findstandards. ■

Outdoor-certified safety laser scanner

Safety laser scanners enable humans and machines to work safely alongside one another in industrial environments. OutdoorScan3 is a safety laser scanner certified to IEC 62998 for use in outdoor applications. The scanner allows automated guided vehicle (AGV) systems to navigate safely through outdoor industrial environments. Because of its outdoor-safe HDDM scanning technology, the device works in all weather—sun, rain, snow, or fog.

The laser scanner can work without errors when exposed to sunlight with an illumination intensity of up to 40,000 lux. In addition, the intelligent software algorithm detects rain and snow, filtering out these environmental influences. For example, rain up to a precipitation intensity of 10 mm/h can be filtered out. Even in fog with a meteorological visual range of up to 50 m, the OutdoorScan3 detects all obstacles, due to its special fog function.

SICK Inc., www.sickusa.com

Machine vision controller

The IPS960-511-PoE is an integrated vision controller optimized for machine vision applications. With a multicore CPU, IP40-rated design, camera communication interfaces, and real-time, vision-specific I/O with microsecond-scale and LED lighting control, this machine vision controller addresses needs across various machine vision platforms and automatic inspection cases.

The controller is powered by the LGA1151 socket with seventh- and sixth-generation Intel Core (Kaby Lake/Skylake) and Celeron processors (up to 65W) with the Intel H110 chipset. The vision system comes with dual DDR4-2133/2400 unbuffered SO-DIMM sockets for up to 32 GB of system memory. It also supports camera interfaces for connecting industrial cameras, including four IEEE 802.3at PoE LAN ports and four USB 3.0 ports.

The unit's vision I/O integrates a range of isolated I/O interfaces and real-time controls essential to machine vision applications, including trigger input, an LED lighting controller, camera trigger, and an encoder input for conveyor tracking. The IPS960-511-PoE also supports light-dimming control to identify object characteristics for different inspections. Two swappable 2.5-in HDDs are available for extensive storage needs.

To ensure performance in harsh environments, the platform system supports an operating temperature range of –10°C to +55°C. Its setup and design allow installation in space-constrained environments. It comes with front-accessible I/O connectors, including two Gigabit LAN ports, four PoE ports, four USB 3.0 ports, one real-time vision I/O, one VGA, one HDMI, one three-pin terminal block, and one audio (mic-in/line-out). The IPS960-511-PoE comes with one I/O module slot with a choice of four different types of I/O modules—a four-port RS-232/422/485 module (AX93511); a four-port isolated RS-232/422/485 module (AX93516); a one-port GbE Ethernet, two-port USB 3.0, and two-port RS-232/422/485 module (AX93519); or a two-port isolated RS-232/422/485 and eight-in/eight-out DIO module (AX93512).

Axiomtek, www.axiomtek.com

Prism line scan camera for sorting, inspection

The second 10-GigE prism line scan camera in the Sweep+ series, the SW-4000Q-10GE has four prism-mounted CMOS sensors and a 10-GigE interface that also supports backward compatibility to 5 Gbps, 2.5 Gbps, and 1 Gbps Ethernet standards. The four CMOS prisms simultaneously capture red, green, blue, and near infrared spectral wavebands for both color accuracy and multispectral analysis via the NIR channel.

Via integrated auto-negotiation technology, the camera has automatic backward compatibility to NBASE-T (5 Gbps and 2.5 Gbps) and the traditional 1000BASE-T (1-Gbps output) for companies running vision applications on these lower-speed Ethernet standards. This makes the camera suitable for the slowest to the fastest running color line scan setups, including applications in food sorting, plastic sorting, bottle/bottle cap inspection, and print/label inspection.

The camera has a maximum resolution of 4,096 pixels (4K) per channel/line, and in combination with the 10GBASE-T interface, it provides RGB + NIR output at up to 72 kHz (72,000 lines per second) over dual 10-GigE streams. The dual-stream configuration supports 8-bit or 10-bit output per channel.

The camera also has a single-stream option using the RGBa8 format where the NIR data is provided via the alpha channel. In this configuration, the camera can operate at up to 73 kHz with 8-bit-per-channel output. A third output option, capable of up to 74 kHz at full 4K resolution, includes 8-bit YUV color data on one stream combined with 8-bit or 10-bit NIR data on a second stream.

The camera supports the precision time protocol (IEEE 1588) for multicamera networked configurations and can be connected directly to rotary encoders for synchronization with conveyor belts and other motion systems.

JAI, www.jai.com

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
Automation Direct www.automationdirect.com	Cover 2
Chromatotec www.chromatotec.com	29
DGH www.dghcorp.com	28
Endress + Hauser www.us.endress.com	3
Inductive Automation www.inductiveautomation.com	Bellyband, Cover 3
ISA www.isa.org	21, 45
Keller America www.kelleramerica.com	15
MAVERICK www.mavtechglobal.com	Cover tip
Moore Industries www.miinet.com	6
ProComSol, Ltd. www.procomsol.com	28
Real Time Automation www.rtautomation.com	29

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.

Process control engineer

Tinuum Services, LLC: The engineer for this position in St. Louis will be responsible for technical programming support and expertise for the operation, maintenance, and continuous improvement of the company facility's instrumentation and process control systems. This includes hands-on technical support of PLC and HMI programming and troubleshooting via remote access or by traveling to the site. Eligible candidates should have a two-year degree or certificate in a related field (e.g., computer programming or process manufacturing with control expertise) with a minimum of five years of industrial-based control systems programming experience. Preference will be given to candidates with a bachelor's degree . . . see more at Jobs.isa.org.

SCADA system technician

City of Tallahassee: The technician in the T&I/SCADA engineering and maintenance department will perform computer configuration, systems maintenance, and support of various technical equipment and services. The technician will directly support a project manager and will exercise technical independence in determining work methods and procedures. Possession of a two-year technical school certificate of completion or an associate's degree in fiber optics, computer networks, computers, electronics, electrical engineering technology, computer technology, process control, or a related field and five years of technical experience in the installation and maintenance of process control/monitoring systems or a bachelor's degree and four years of experience is required . . . see more at Jobs.isa.org.

Quality engineer

John Deere: As a quality engineer at the Augusta Works in Grovetown, Ga., the successful candidate will support current assembly operations in the compact utility tractor factory. In addition, the engineer will investigate issues related to product and process quality, gather and analyze data, determine root causes, and facilitate and use failure modes effects analysis. Knowledge of standard quality tools, manufacturing or distribution processes, and drawing and schematic interpretation is required, in addition to one or more years of experience in related engineering areas. Knowledge of advanced data gathering and analysis techniques, a Six Sigma Green Belt, experience using statistical tools and techniques, and experience in team leadership will make the candidate stand out . . . see more at Jobs.isa.org.

Senior manager system assurance engineer

Raytheon: This engineer in El Segundo, Calif., is responsible for all system and software mission assurance efforts across the Secure Sensor Solutions (S3) programs. The engineer will lead a team of system assurance and software quality engineers through the entire program life cycle, focusing on business pursuit, program planning, product development, and qualification, and will be responsible for the implementation of the company's system and software mission assurance management system consistent with customer contractual requirements. Required skills include excellent communication, a minimum of 12 years of experience in a mission assurance or engineering development environment, and ASQ quality professional certification. The position requires 10–20 percent travel . . . see more at Jobs.isa.org.

Beware of the hype

By Dean Ford, CAP

ABOUT THE AUTHOR

Dean Ford, CAP dford2009@gmail.com) is the managing principal engineer and executive vice president of Westin Technology Solutions Engineering Practice. He is a licensed control systems engineer in 18 states and an active ISA member. Ford participates in AWWA, WEF, WRF, SWAN, and is on the Government Relations and Workforce Development committee of the Automation Federation.

Do you have a plan to combat the fear mongers and the shiny-new-thing pushers? I grew up in the plant floor automation business. I have seen a lot of change in technology, and I have seen a lot of resources wasted on things that really had no business case. Recently, this waste seems to be focused on cybersecurity and other shiny new things. In an age where the pace of technological advancement is higher than ever, our profession is being bombarded daily with the next great thing. Managers get calls from highly effective sales people and do Internet searches that teach them of all the threats they must protect against and all the opportunities they are missing because they do not have X, Y, or Z. This pressures automation professionals to also focus on cybersecurity and new technologies and usually forces them to bypass some critical decision steps.

Automation professionals are on the front lines of risk management and mitigation. The cyberthreat is merely one of many threat factors to overall risk management, and it gets far too much attention. Our profession is getting a lot of pressure to spend money on this. "Your peers are doing it, why aren't you?"

If you have heard me speak at various conferences, you have likely heard some shocking words. Cybersecurity is not the threat that it purports to be. In one session recently, I was challenged. A prominent manager at a utility had done a lot of surveys with conclusive results. Cybersecurity was in the top five biggest perceived threats to operations. I agree it is a threat, but I challenge the notion that it is our greatest threat from two sides. First, if it was truly that large of a threat, every utility would be budgeting lots of money to address it. That is not happening, and the more advanced utilities and companies are not wasting resources on it for very good reasons. Second, there are far greater threats that should be dealt with first. Planning is the key to relieving the pressures.

The cyberthreat is merely one of many, many risks that must be addressed in our operations. If your organization is currently involved in any sort of cyber-assessment or mitigation project, and you have not first assessed your risk profile, then you have missed a critical step. Ask to see the data that shows this is your number one threat to operations. I have found that in 100 percent of cases, threats exist with a far greater impact to operations than a cybersecurity incident. Bad business decisions are made in the name of cybersecurity, like removing remote access from maintenance personnel, which significantly increases costs and response time for troubleshooting. What are we really trying to protect against?

If your organization is currently involved in any sort of cyber-assessment or mitigation project, and you have not first assessed your risk profile, then you have missed a critical step.

I propose a different path. An overwhelming majority of cyberrisk can be eliminated through simple procedural and policy changes that cost no money. Instead of spending money to prevent a cybersecurity issue, first go through the exercise of assuming you will be hacked. How will you and the organization respond? What key decision-making process do you need in place? What is the hierarchy? Who is authorized to call something a disaster? Is your disaster recovery plan in place and has it addressed things like building a new automation platform from bare metal? Have you tested it? Are your backups working? The list goes on. The key point here is that if someone wants in, he or she is going to get in, and it will be through normal channels. All of the money spent to prevent a hack will be useless.

With a sound risk management and disaster recovery plan, you not only address cybersecurity incidents, but you also mitigate fires, theft, weather events, rogue employees, etc. And perhaps, during the risk mitigation planning, cybersecurity jumps out as a critical need, and you have to develop some projects for network segregation. At least then you will know that the capital is being deployed in the best way and for the correct priorities. I suspect you will find that you should be fixing the power failure scenario that causes hours of down time, or moving the server out of the control room, or simply upgrading the automation platform to current hardware with parts that you can buy from a more reputable place than eBay. ■


The Plant Floor in Your Pocket
Get an overview of your process at a glance.
Control your SCADA with a swipe.
Ignition!
Perspective
See the live demo now.
Scan this QR code with your phone
or visit demo.ia.io/tech

May/June 2019

InTech

A PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

ISA

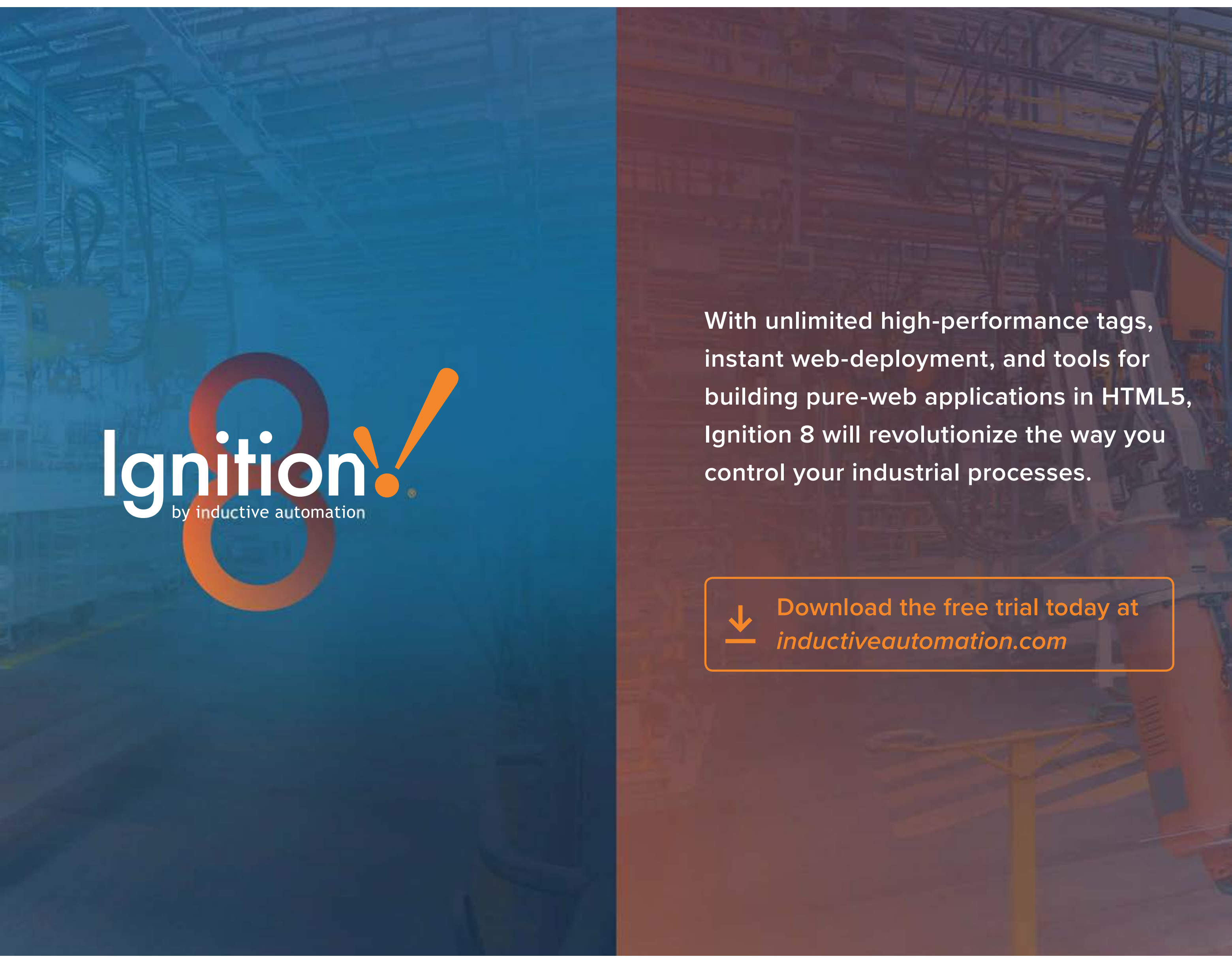
Data-driven decision making
Digitalization value
Machine vision systems
Preventive maintenance
Thin clients

CONTROL SYSTEM TURNAROUNDS
A Better Path Forward

TURN PAGE

Setting the Standard for Automation™
www.isa.org/intech


Ignition 8
by inductive automation
The Unlimited SCADA Platform of the Future is Here
Download the free trial today at
inductiveautomation.com
Back
Ignition
Start Date
End Date
Top
01/23/2019 00:00
01/23/2019 23:59
10
ALARM SUMMARY
TOTAL ALARMS 3
TOTAL DURATION 02:16:01
TOTAL UNACKNOWLEDGED 3
AVG TIME TO ACK 00:00:00
AVG TIME TO CLEAR 01:09:30
MOST FREQUENT Day Tank - 2 (66.7%)
LONGEST DURATION Tank 1 - 7621 (93.4%)
ALARMS BY HOUR
# of Alarms
Duration (sec)
Tour Feature 1/5


Ignition 8
by inductive automation
With unlimited high-performance tags, instant web-deployment, and tools for building pure-web applications in HTML5, Ignition 8 will revolutionize the way you control your industrial processes.
Download the free trial today at
inductiveautomation.com