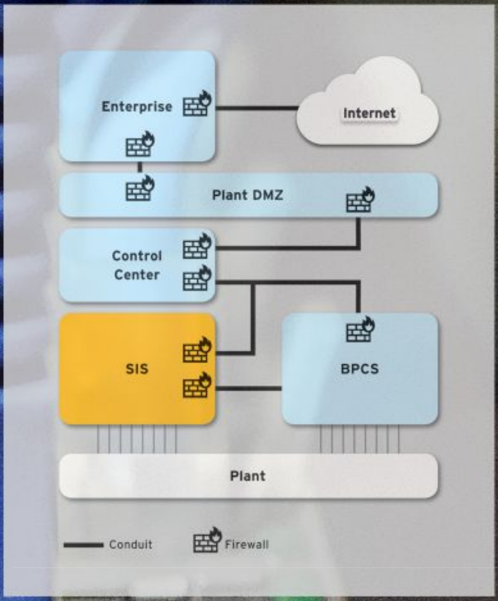
CONTROL ENGINEERING®

APRIL
2018

Covering control, instrumentation, and automation systems worldwide

Plugging into CYBERSECURITY

9-27



Artificial intelligence 28, 32

Mobility applications 35, 38

Energy efficiency 40

IIoT integration 41, 46

Embedded systems M1

Additive manufacturing M3

CFE Media®
www.controleng.com

When commercial grade just won't cut it...

Industrial Managed Ethernet Switches
starting at:
$429.00
SE2-SW8M

...get Industrial Managed Ethernet Switches **for less** from AutomationDirect.

Stride®

NEW! SE2 Series Industrial Managed Ethernet Switches

Commercial grade Ethernet switches have their place, but the harsh environment of the industrial world is not one of them. Don't risk your time, reputation, and money on managed switches that can't handle the extreme temperatures, unreliable power, hazardous locations or excessive vibration that exists in industrial facilities. Get the most out of your network and your dollar with affordable and reliable Stride Industrial Managed Ethernet Switches.

It's not just the low price, but the exceptional value you get with Stride Ethernet Switches that makes them so popular. With Stride Managed Ethernet Switches you get all this and more:

- Enhanced network security
- Fail-safe networking with intelligent redundancy
- Traffic filtering for streamlined, efficient communication
- Helpful troubleshooting tools and statistics
- Modbus TCP and EtherNet/IP management capabilities
- Web-based configurations
- Gigabit Ethernet (GbE) models available
- FREE technical support for the life of the product!

FREE shipping - orders over $49
2-day Shipping

5 YEAR WARRANTY

30-day Money-Back Guarantee

Research, price, buy at:
www.automationdirect.com/ethernet-switches

VOTED Best in SERVICE 15 YEARS

Order Today, Ships Today!

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

input #1 at www.controleng.com/information

kepware®

Connected Machines.

Efficient Communications.

Smarter Operations.

Kepware's industry-leading industrial connectivity solution provides:

A Scalable and Flexible Architecture
with connectivity to hundreds of protocols covering a wide range of PLCs, RTUs, flow computers, sensors, databases, custom applications and other industrial data sources.

Streamlined and Reliable Data Access
for HMI/SCADA, MES, Historian, ERP, custom applications and industrial IoT platforms, including ThingWorx®.

Increased Visibility
into industrial data—so everyone from the shop floor to the top floor can make smarter decisions.

Learn more at www.kepware.com/CE

ptc

input #2 at www.controleng.com/information

TEST POINT
EATON
BUSSMANN SERIES
Low-Peak™ CUBEFuse™
600VAC OR LESS
TCF30RN
TCF60RN
600VAC OR LESS
TCF100RN
DUAL ELEMENT TIME DELAY CURRENT LIMITING FUSE
MADE IN CHINA

COVER IMAGE: This photo illustrates a network switch. While industrial control system technology matters, it's only one aspect of a layered cybersecurity architecture. Courtesy: Huffman Engineering Inc.

APRIL 2018

CONTROL ENGINEERING

Vol. 65
Number 4

Digital edition? Click any headline on this page to go to the article. At the article, click the headline again to see more online.

INSIGHTS

5 | Research: Controllers in discrete manufacturing

NEWS

6 | Technology, people converge at Hannover Messe 2018

Cyber hub for manufacturing launched in Chicago

8 | IMTS, Hannover Messe USA see big growth for 2018 shows

9 | Endpoint security best practices white paper released

Lifecycle cybersecurity standard

10 | Think Again: Advice from cybersecurity incident

ANSWERS

12 | Eight ICS cybersecurity tips for a hyper-connected world

16 | Safety and security for process control applications (COVER DIAGRAM)

18 | Understanding industrial control systems security basics

22 | Cybersecurity is the common ground in IT/OT convergence

24 | Learn how to stay ahead of cyber attacks

26 | Threat intelligence is a critical organizational need

28 | Artificial intelligence's impact on the robotics industry

32 | Five smart warehousing predictions

35 | Seven benefits to using mobile software in an organization

38 | How to transition from traditional to digital plant-floor technologies

40 | Neural network chip reduces power use

41 | Integrating the Industrial Internet of Things

42 | What can the IIoT do?

44 | Integrating IIoT technologies in facilities

INSIDE MACHINES

M1 | What is an embedded system?

M3 | Building the future with robotic additive manufacturing

INNOVATIONS

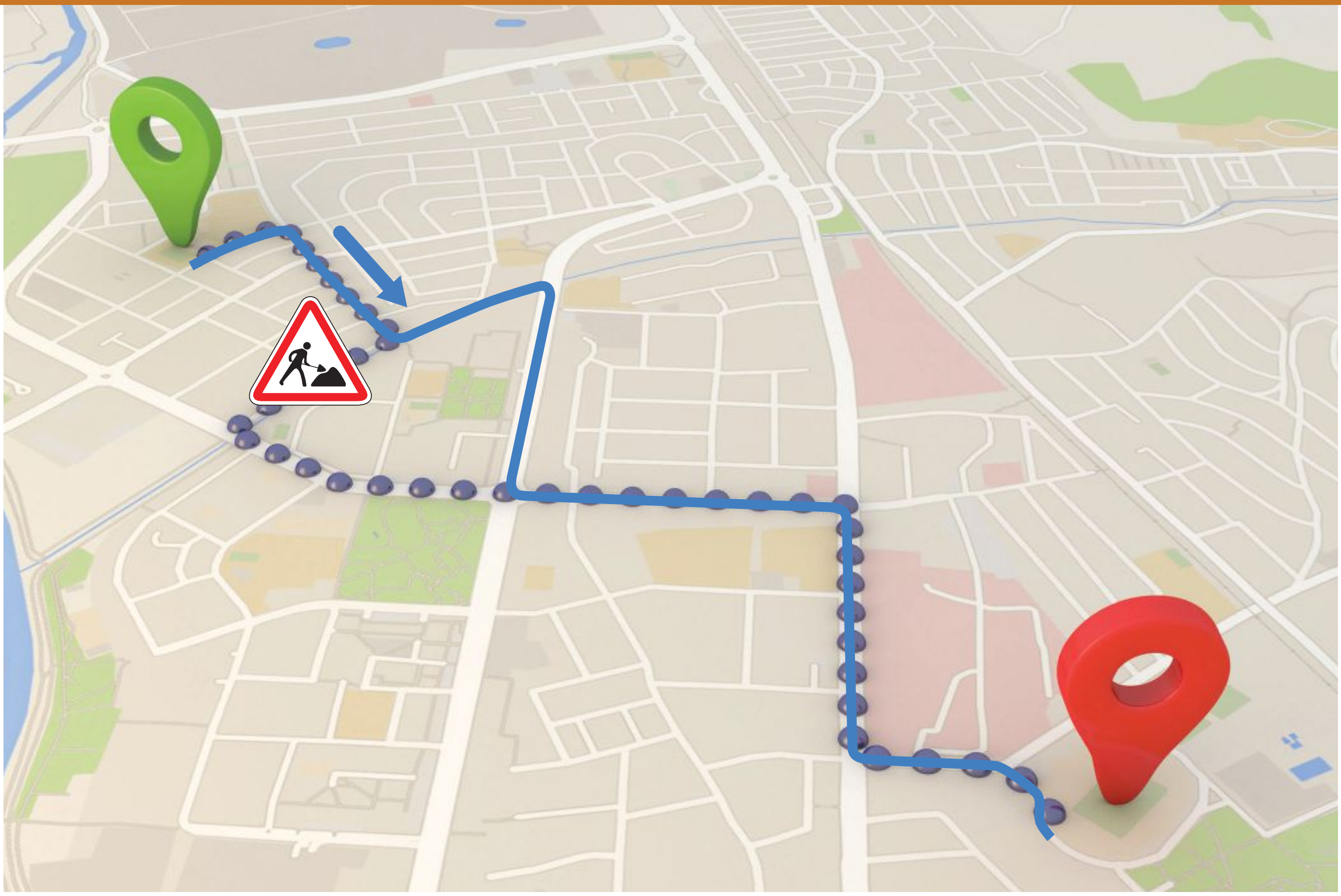
NEW PRODUCTS FOR ENGINEERS

61 | Motion control, safety PLCs, asset performance, gearboxes, and more

BACK TO BASICS

64 | Collaborative robot applications for non-standard businesses

CONTROL ENGINEERING (ISSN 0010-8049, Vol. 65, No. 4, GST #123397457) is published 12x per year, Monthly by CFE Media, LLC, 3010 Highland Parkway, Suite #325 Downers Grove, IL 60515. Jim Langhenry, Group Publisher/Co-Founder; Steve Rourke CEO/COO/Co-Founder. CONTROL ENGINEERING copyright 2018 by CFE Media, LLC. All rights reserved. CONTROL ENGINEERING is a registered trademark of CFE Media, LLC used under license. Periodicals postage paid at Downers Grove, IL 60515 and additional mailing offices. Circulation records are maintained at 3010 Highland Parkway, Suite #325 Downers Grove, IL 60515. Telephone: 630/571-4070. E-mail: customerservice@cfemedia.com. **Postmaster: send address changes to CONTROL ENGINEERING, 3010 Highland Parkway, Suite #325 Downers Grove, IL 60515. Publications Mail Agreement No. 40685520. Return undeliverable Canadian addresses to: 3010 Highland Parkway, Suite #325 Downers Grove, IL 60515. Email: customerservice@cfemedia.com.** Rates for nonqualified subscriptions, including all issues: USA, $ 150/yr; Canada/Mexico, $180/yr (includes 7% GST, GST#123397457); International air delivery $325/yr. Except for special issues where price changes are indicated, single copies are available for $30 US and $35 foreign. Please address all subscription mail to CONTROL ENGINEERING, 3010 Highland Parkway, Suite #325 Downers Grove, IL 60515. Printed in the USA. CFE Media, LLC does not assume and hereby disclaims any liability to any person for any loss or damage caused by errors or omissions in the material contained herein, regardless of whether such errors result from negligence, accident or any other cause whatsoever.



543.46
DEG C

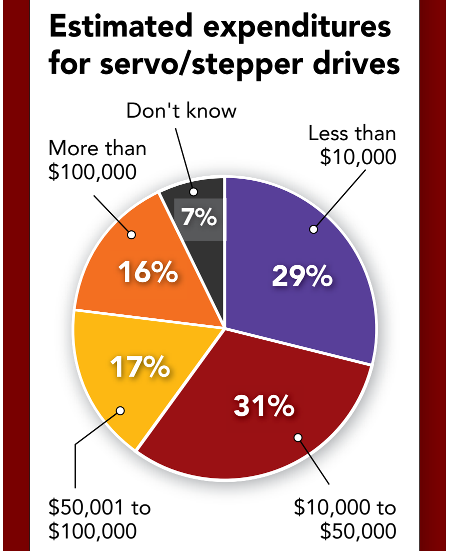


Figure 1: End users estimate an average spend of $96,000 on servo and/or stepper drive products over the past 12 months. Source: *Control Engineering* 2017 Motor Drives Study

46% of automation professionals love going to work every day; 37% are just happy to be employed. Source: *Control Engineering* 2017 Career & Salary Survey

63% of end users purchase their HMI software and/or hardware from their local distributor. Source: *Control Engineering* 2018 HMI Software & Hardware Study

75% of end users' controllers feature proportional-integral-derivative (PID) control. Source: *Control Engineering* 2017 Programmable Controllers Study

More research

Control Engineering covers several research topics each year. All reports are available at www.controleng.com/ce-research.

2017 CONTROLLERS STUDY

Controllers in discrete manufacturing

Thirty-eight percent of respondents in the *Control Engineering* 2017 Programmable Controllers Software & Hardware survey work at a facility primarily involved in discrete manufacturing. Below are five key findings as they relate to using programmable controllers in these facilities:

1. Interfacing with control systems: Forty-one percent of controllers used in discrete manufacturing facilities network with other programmable logic controllers while 24% stand alone, 14% network with a distributed control system, 13% network with industrial PCs, and 7% network with programmable automation controllers.

2. Communications protocols: The most used communication protocols for controllers in discrete manufacturing facilities are 4 to 10 mA/0 to 10 V dc (73%), EtherNet/IP (68%), RS-232/RS-485 (64%), and Ethernet (63%).

3. Integrated software, hardware: Thirty-eight percent of discrete manufacturing facilities usually buy or specify controller software that is integrated with controller hardware; 28% purchase them separately.

4. Annual spend: Discrete manufacturing facilities spent an average of $141,000 on industrial controller hardware and software in the past 12 months. Eighty-two percent of end users in these industries expect to buy industrial controller software or hardware again in the next 12 months; the average estimated spend is $132,000.

5. Cybersecurity: For controllers used at discrete manufacturing facilities, 76% of end users report restricted access to the controllers. Forty-seven percent have increased password protection procedures ,and 45% have restricted physical access to controllers as cybersecurity measures. **ce**

*View additional findings at www.controleng.com/2017ControllersReport. **Amanda Pelliccione** is the research director at CFE Media, apelliccione@cfemedia.com.*

M More RESEARCH

Control Engineering covers several research topics each year.

All reports are available at www.controleng.com/ce-research

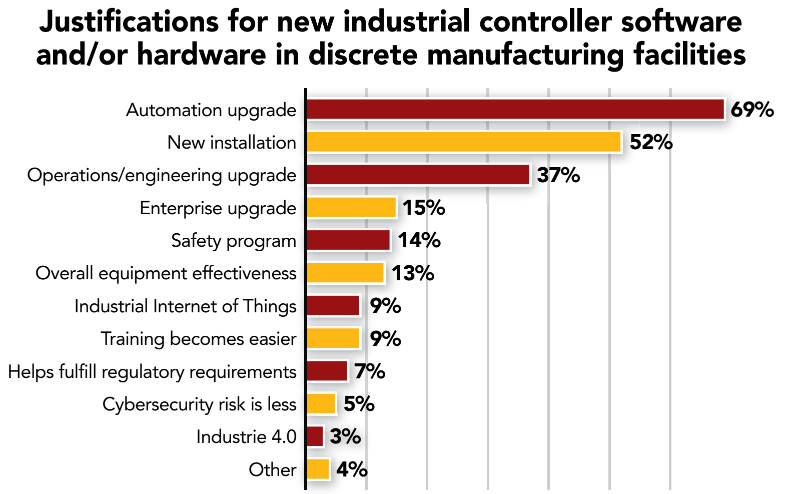


Figure 2: Discrete manufacturing facilities most commonly acquire new industrial controller software and/or hardware as a result of an automation upgrade (69%), new installation (52%), or operations/engineering upgrade (37%). Source: *Control Engineering*

Technology, people converge at Hannover Messe 2018

The convergence of technology and people will be at the forefront of Hannover Messe 2018, taking place April 23-27 in Hannover, Germany.

"The integration of automation technology, IT platforms, and machine learning will take Industrie 4.0 to the next level," said Dr. Jochen Köckler, chairman of the managing board at Deutsche Messe, in a press release. The 2018 theme for the show is "Integrated Industry: Connect & Collaborate."

Hannover Messe 2018 will be showcasing how these technologies can be used to enhance productivity and safety while meeting the needs of a changing consumer market.

"The customer is king; he expects the world and wants it right now," said Köckler, and Hannover Messe is expected to showcase how those demands will be met through technology. To do this, Hannover Messe is having a convergence of its own, as the CeMat material handling show will be co-located at Hannover Messe in 2018.

"The world's leading manufacturers of automation technology, big-name robotics providers, and global IT and software corporations will all be there, making the show an absolute global hotspot for Industrie 4.0," Köckler added.

Energy is another area of emphasis at Hannover Messe, but in this sector, the focus is not on current capabilities but rather on future needs.

The five-day event begins with the opening ceremony on Sunday, April 22, where Mexico will be feted as the Partner Country. It's the second time in three years a North American country has been the Partner Country, following the United States' presence in 2016. More than 5,000 exhibitors and 220,000 visitors are expected at the Hannover Messe fairgrounds, and more than 150 presentations will take place during the week.

Hannover Messe 2018's event will focus on the integrated industry and supply chain. Courtesy: Hannover Messe

IHS Markit, a CFE Media partner, will present a roundtable discussion entitled, "Transformative Technologies Impacting Industrial Market Dynamics," on Wednesday, April 25. The discussions will offer an overall economic update, an industrial market review, and a look at the transformative technologies in industrial automation. (See related show, p. 8)

Bob Vavra, *content manager, CFE Media, bvavra@cfemedia.com.*

Cyber hub for manufacturing launched in Chicago

The Digital Manufacturing Design and Innovation Institute (DMDII) announced in March the launch of a "Cyber Hub for Manufacturing" with $750,000 in seed funding from the U.S. Department of Defense (DoD). The hub will serve as a testbed for the creation and adoption of new cybersecurity technologies to secure manufacturing shop floors across the United States and complements DMDII's public-private partnership as one of the Manufacturing USA institutes sponsored by the DoD to advance the state-of-the-art in digital manufacturing.

The Digital Manufacturing Design and Innovation Institute (DMDII) launched a Cyber Hub for Manufacturing with $750,000 in seed funding from the U.S. Department of Defense (DoD). Courtesy: Katie Spain, CFE Media

"The launch of the Cyber Hub for Manufacturing embodies why DMDII exists," said DMDII executive director Thomas McDermott. "We need to think about securing our manufacturing equipment the way we secure our laptops, and the complexity of this issue means our partners will get there much faster by working together."

DMDII will leverage its more than 300 partners across industry, academia, and government, and its manufacturing floor to test cybersecurity use cases in a real-world manufacturing environment. It will develop hands-on cybersecurity training programs and create online, learning modules to reach manufacturers outside of the region.

The launch of the Cyber Hub for Manufacturing was announced at a celebration of the Institute's four-year anniversary, where stakeholders from across the country recognized the institute's role in catalyzing a collaboration of established manufacturing technology companies, universities, small manufacturers and startups, and many community and civic groups around the concept of helping U.S. manufacturers improve. The Cyber Hub is the result of recommendations developed through DMDII workshops with government, industry, and academic partners since the Institute's establishment in 2014.

- Edited from a DMDII press release by CFE Media.

IMTS, Hannover Messe USA see big growth for 2018 shows

Organizers of the 2018 IMTS and the co-located 2018 Hannover Messe USA have expanded space at Chicago's McCormick Place for the biannual event. Courtesy: IMTS

With manufacturing on solid footing and growth continuing in the sector, organizers of the 2018 International Manufacturing Technology Show (IMTS) and the co-located 2018 Hannover Messe USA have expanded space at Chicago's McCormick Place for the biannual event, which will be held Sept. 10-14.

"As we have done since launching the industrial technology shows at IMTS 2012, Hannover Messe USA's trade shows will leverage the power of the Hannover Messe brand by demonstrating the full range of Industrie 4.0 and Industrial Internet of Things (IIoT) solutions during IMTS 2018," said Larry Turner, President and CEO of Hannover Fairs USA (HFUSA), which produces Hannover Messe USA.

CFE Media and HFUSA also will co-organize the Global Automation Manufacturing Summit (GAMS), which will feature panel discussions on the key issues surrounding IIoT, including robotics, cybersecurity, and maintenance. GAMS will be held on Wednesday, Sept. 12 starting with an 11:30 a.m. luncheon. Beckhoff, Infor, Stratus, and UL are Gold Sponsors for the 2018 GAMS event.

Registration is open for IMTS, and attendees will be able to tour a larger exhibit space than in 2016. With six months remaining before the event, more than 1,800 exhibitors already have signed up to occupy 1.3 million sq ft of exhibit space.

Hannover Messe USA's Integrated Automation, Motion & Drives (IAMD) USA also will cover more exhibition space. Located alongside IAMD USA will be the Fluid Power special display area.

On level two, the other three Hannover Messe USA co-located trade shows—ComVac USA, Industrial Supply USA, and Surface Technology USA—will take place next to the event's Digital Factory and Industrial Energy Systems special display areas.

"We also expect to extend the overall scope and global nature of the co-located shows this year by highlighting more exhibitors from around the world in our international pavilions, including China, Germany, Italy, Korea, and Taiwan," said Turner.

***Bob Vavra**, content manager, CFE Media, bvavra@cfemedia.com.*

Endpoint security best practices white paper released

The Industrial Internet Consortium (IIC) announced the publication of the Endpoint Security Best Practices white paper. It is a document designed as a reference point for equipment manufacturers, critical infrastructure operators, integrators, and others to implement countermeasures and controls they need to ensure the safety, security, and reliability of Internet of Things (IoT) endpoint devices. Endpoints include edge devices such as sensors, actuators, pumps, flow meters, controllers, communications infrastructure and gateways, etc.

Unreliable equipment can cause safety problems, customer dissatisfaction, liability, and reduced profits," said Steve Hanna, IIC white paper co-author, and senior principal, Infineon Technologies. "The Endpoint Security Best Practices white paper moves beyond general guidelines, providing specific recommendations by security level. Equipment manufacturers, owners, operators, and integrators are educated on how to apply existing best practices to achieve the needed security levels for their endpoints."

The white paper distills key information about endpoint device security from industrial guidance and compliance frameworks.

While the white paper is targeted primarily at improving the security of new endpoints, the concepts can be used with legacy endpoints by employing gateways, network security, and security monitoring.

- Edited from an IIC press release by CFE Media. The IIC is a CFE Media content partner.

Headlines online

Top five *Control Engineering* articles
Mar. 19-25: Most visited articles included building a machine with motion design software, Big Data analytics, steam trap stations, the 2018 HMI Software and Hardware Study, and fog computing

IoT, Industrie 4.0 create M&A hotspots
The Internet of Things or Industrie 4.0 technologies drive a new wave of mergers.

Number of ICS devices connected to internet increases, raising security concerns
Report raises cybersecurity concerns.

Benefits of pick-and-place robots for manufacturers
Pick-and-place robots have become a common robotic application in today's facilities.

Industrial cybersecurity standard published
Device design and lifecycle are addressed.

Advice from cybersecurity incident

Cybersecurity incident: Human errors enabled it, but the Triconex safety controller shut down the plant as designed, say experts with Schneider Electric and ARC Advisory Group. But it's still a call to action for industry. Have you implemented changes since then?

Mark T. Hoske,
Content Manager

Breach of an industrial, triple-redundant safety controller should dispel any thought hackers might not care about industrial facilities or that process controls are low-risk cybersecurity targets. All facilities, even if already heeding advice from Schneider Electric and ARC Advisory Group, need to have a response plan in place. The Aug. 4, 2017, cyberattack on a on a Triconex safety system that included the first instance of process safety system-specific malware, dubbed TRITON, was described in a media and analyst lunch on Feb. 13. That triple-redundant safety controller brand is part of the Schneider Electric EcoStruxure Triconex safety instrumented system (SIS). A summary of advice from each expert follows.

Collaborative cybersecurity effort

The industry has a problem; hackers can reach instrumentation.

Peter G. Martin, vice president, innovation, Schneider Electric, said a cybersecurity incident that resulted in attackers injecting malware into a safety controller is a call to action for the industry because it heralds a new geopolitical climate where malicious actors have specialized knowledge, as well as unlimited resources, to carry out their cyber attacks.

These attacks can reach the instruments in a control system, especially if organizations are not compliant with industry standards, best practices, and cybersecurity procedures. That means industry end users, standards bodies, vendors, and government agencies need to come together to combat the threat. The industry shouldn't think there's no problem because the equipment performed as it was supposed to by safely shutting down the targeted plant. There is a problem because cybersecurity best practices were not followed; more work is needed in collaboration with end users, vendors, and government to lower the risk of other cybersecurity incidents from happening.

Cybersecurity wake-up call

Multiple cybersecurity lapses allowed a safety controller breach.

Gary Williams, senior director, technology, cybersecurity and communications, Schneider Electric, said this is an industry call to action. A Triconex controller model 3008, brought to market in 2001 and installed as part of a large automation project in 2007, was affected by a security breach. When the controller picked up an anomaly in the malware the attackers injected into its code, the controller reacted as it was intended: It safely brought the plant to a safe state via a shutdown on Aug. 4, 2017.

Upon being notified of the shutdown, Schneider Electric worked closely with the end user, independent cybersecurity organizations and the U.S. Department of Homeland Security/ICS-CERT and others to investigate the incident. The evidence they gathered indicates multiple security lapses allowed the breach to occur.

A remote attacker, through a corporate system, logged onto a machine and was playing with code. An individual made an error not specific to the controller and exposed it to remote access through Microsoft Windows XP [no longer supported] software. Practices outlined in controller documentation, and in the IEC 62443 series of standards on industrial automation and control systems (IACS) from the ISA99 Industrial Automation and Control Systems Security committee, if followed, would have prevented the breach.

Don't panic; assess risks

Reconsider cybersecurity processes, procedures, and training.

Larry O'Brien, vice president research for process automation, ARC Advisory Group, said the industry shouldn't panic, but it should reconsider best practices regarding processes, procedures, and people. There are ways to execute a response to and defend against a systemic, multiphase attack.

In this same incident, the attack(s) breached another vendor's distributed control system (DCS); so while the shutdown was initiated as designed, it's better not to suffer a breach and shut down a process.

Other human errors on site, including leaving the controller's keyswitch in program mode while it was in operation and leaving the controller cabinets unlocked, added significant risk for a cybersecurity attack.

To lower the risks of such incidents, customers should continue to apply cybersecurity best practices across their operations, as well as always implement the instructions vendors provide within their systems documentation. For example, a recommended practice is to dedicate a laptop for use with the DCS and not let anyone else or anything connect to the laptop.

Schneider Electric's open and helpful response to this incident has been applauded and should be a blueprint for other vendors' responses because this won't be the last incident.

What's the attraction for hackers? By reprograming the DCS and the safety system, attackers can push the plant into an unsafe state without those at the plant and the safety system realizing it. That means if an incident occurred, the expected result, i.e., the safety system shutting down the plant, wouldn't happen. Idaho National Labs demonstrated such a DCS spoofing event at least 10 years ago.

Program mode, cybersecurity standards

Have any of your controllers been left in program mode?

Eric Cosman, contributing consultant, ARC Advisory Group and co-chair of ISA99 Industrial Automation and Control Systems Security committee, said the Triton attack was not unprecedented. He advised we shouldn't underestimate the hazards posed by human denial. Cosman, who worked for Dow Chemical most of his career, said leaving a controller key in program position is inexcusable.

The ISA99 committee produced the IEC 62443, which addresses people, processes, and technologies. Risk assessment is part of that. End users don't have time to read a 1,000-page standard; practices and case studies are available along with sanitized examples of actual incidents.

Frequent cybersecurity education

Cybersecurity isn't a destination; it's a journey and a continuing process.

Gary Freburger, president, process automation, Schneider Electric, said cybersecurity, like safety, isn't something that can be done and finished; it's a continuing process. This is counterintuitive to the view not to touch a system if it's doing what it's supposed to be doing.

Breaches will happen, and cybersecurity is everyone's job, at individual and organizational levels with a commitment to industry, standards, and transparency. Three best practices follow.

1. Commit to educate and address people, processes, and technologies with a relentless drive to publish and standardize best practices and share information.

2. Use common standards across all equipment and across multiple providers, with feedback and guidance from those involved.

3. Ensure collaboration through transparency. Don't say or believe anything is secure. A lot of people are trying to get into these systems. Everyone needs to respond correctly knowing what was done before, to know how to correct it.

Peter G. Martin
Vice president, innovation, Schneider Electric

Gary Williams
Senior director, technology, cybersecurity and communications, Schneider Electric

Larry O'Brien
Vice president research for process automation, ARC Advisory Group

Eric Cosman
Contributing consultant, ARC Advisory Group and co-chair of ISA99 Industrial Automation and Control Systems Security committee

Gary Freburger
President, process automation, Schneider Electric

In this case, Freburger said Schneider Electric experts were on site within four hours of being notified. End users struggle in cybersecurity incidents, he said, and vendors can use their expertise to help. **ce**

Mark T. Hoske *is content manager,* Control Engineering, *CFE Media, mhoske@cfemedia.com.*

More INSIGHTS

GO ONLINE

If reading from the digital edition, click on the headline for more cybersecurity resources. www.controleng.com/magazine

See related cybersecurity coverage at www.controleng.com and in articles on the next pages of this issue.

CONTROL ENGINEERING

3010 Highland Parkway, Suite 325, Downers Grove, IL 60515. 630-571-4070, Fax 630-214-4504

Content Specialists/Editorial

Mark T. Hoske, Content Manager
630-571-4070, x2227, MHoske@CFEMedia.com

Jack Smith, Content Manager
630-571-4070, x2230, JSmith@CFEMedia.com

Kevin Parker, Senior Contributing Editor, IIoT, OGE
630-571-4070, x2228, KParker@CFEMedia.com

Emily Guenther, Associate Content Manager
630-571-4070, x2229, eguenther@CFEMedia.com

Amanda Pelliccione, Director of Research
978-302-3463, APelliccione@CFEMedia.com

Chris Vavra, Production Editor
CVavra@CFEMedia.com

Contributing Content Specialists

Suzanne Gill, *Control Engineering Europe*
suzanne.gill@imlgroup.co.uk

Ekaterina Kosareva, *Control Engineering Russia*
ekaterina.kosareva@fsmedia.ru

Seweryn Scibior, *Control Engineering Poland*
seweryn.scibior@trademedia.us

Lukáš Smelík, *Control Engineering Czech Republic*
lukas.smelik@trademedia.us

Aileen Jin, *Control Engineering China*
aileenjin@cechina.cn

CFE Media Contributor Guidelines Overview

Content For Engineers. That's what CFE Media stands for, and what CFE Media is all about – engineers sharing with their peers. We welcome content submissions for all interested parties in engineering. We will use those materials online, on our website, in print and in newsletters to keep engineers informed about the products, solutions and industry trends.

www.controleng.com/contribute explains how to submit press releases, products, images and graphics, bylined feature articles, case studies, white papers, and other media.

* Content should focus on helping engineers solve problems. Articles that are commercial or are critical of other products or organizations will be rejected. (Technology discussions and comparative tables may be accepted if non-promotional and if contributor corroborates information with sources cited.)

* If the content meets criteria noted in guidelines, expect to see it first on our Websites. Content for our e-newsletters comes from content already available on our Websites. All content for print also will be online. All content that appears in our print magazines will appear as space permits, and we will indicate in print if more content from that article is available online.

* Deadlines for feature articles intended for the print magazines are at least two months in advance of the publication date. Again, it is best to discuss all feature articles with the appropriate content manager prior to submission.

Learn more at: www.controleng.com/contribute

Keith Mandachit, Sean Creager, and Jay Steinman, Huffman Engineering Inc.

Eight ICS cybersecurity tips for a hyper-connected world

Implementing a cybersecurity strategy against internal and external threats are key steps toward securing an industrial control system (ICS).

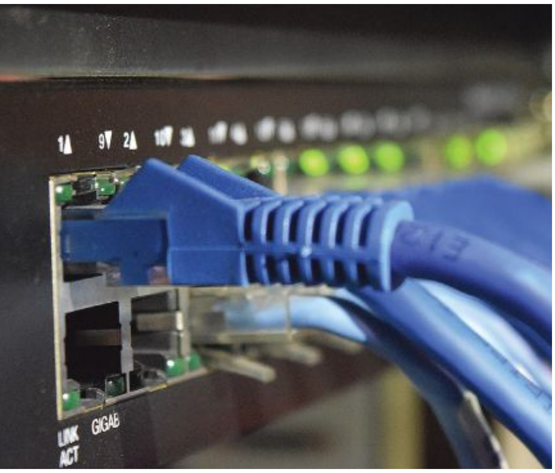
Industrial control systems (ICS) can achieve lower cybersecurity risk by building a defense-in-depth cybersecurity plan and following the eight tips highlighted below.

In the modern age of smart manufacturing, the Internet of Things (IoT) and Industrie 4.0 bring important competitive advantages—connectivity is the way of the future. Some companies are on the leading edge to embrace cybersecurity, but others don't take it seriously until they have a threat or breach. Building a robust cybersecurity strategy to help prevent cyber attacks requires a holistic and layered approach. Following the key tips below is key for developing a robust ICS cybersecurity plan.

Defense-in-depth cybersecurity plan

"Defense-in-depth" is the term used to describe a planning strategy to secure an ICS; it refers to the ideal state of having many layers of security systems and access controls. Begin by identifying the internal, external, physical, and virtual threats to the control system. Assess how large of a risk each threat poses, and this should be a guide for how to best allocate the budget for a successful cybersecurity plan.

Make a comprehensive plan to mitigate those risks to an "acceptable" level (which will differ for each entity). Follow up with a process of how to address each threat or breach if it does occur. Plan for system monitoring and alerts to notify users a breach is in progress or has happened.



On the Cover: This photo illustrates a network switch. While industrial control system technology matters, it's only one aspect of a layered cybersecurity architecture. All graphics courtesy: Huffman Engineering Inc.

1. Segmentation

Segmentation is a defense-in-depth strategy using the principle of dividing up a network to limit the amount of damage that could be done if there was a breach. Segmentation creates isolated, self-contained networks (segments) within the larger network to prevent unwanted access to and limit the vulnerability of the system. Segmentation can be created physically by using additional hardware such as cabling and switches, but this is a time-consuming and more costly approach than to do so virtually.

Isolated networks are normally created within the larger system by using virtual local area networks (VLAN). Segmentation can be very basic, such as separating the manufacturing network from the business network, or more complex by creating a different segment for each manufacturing cell.

For example, in the pharmaceutical industry, each manufacturing cell or packaging line can be segmented individually from each other. If network segments need to communicate, a firewall can offer additional protection. The firewall is a separate device that decides whether the network traffic is allowed to pass or is blocked.

When plants are regional, having each as a segment protects the whole system from a potentially catastrophic failure. If further separation is desired, segments can be created in each plant for systems such as the instrumentation, control, and visualization networks.

2. Demilitarized zone

A special case of segmentation is a demilitarized zone (DMZ) between a company's industrial and manufacturing systems, its business and IT networks, or the internet. Although not universally implemented in ICSs, a DMZ is important for certain situations. A properly designed DMZ does not allow traffic to traverse directly across the DMZ from the business network or internet, to the ICS network. Inside the DMZ, servers or devices act as intermediaries to communicate across the DMZ.

3. Regular backups and updates

Ensure systems are backed up regularly. Create images for all hard drives, backup virtual machines, and store configurations and programs on a storage device such as a network attached storage (NAS) device. The backups should be duplicated to another off-site device for additional protection. No matter how secure a defense may be, it's never 100%. Backups are key to a quick and painless recovery.

Keep systems updated with the latest patches and upgrade any computers that run unsupported operating systems. On these obsolete platforms, vulnerabilities are often made public even though patches are no longer offered through the manufacturer.

Get on email distribution lists with the automation equipment manufacturers to receive relevant security bulletins. Additionally, sign up for ICS-CERT notifications through the Department of Homeland Security (DHS).

4. Special purpose security appliances

A few manufacturers make cybersecurity products specifically for ICSs. Firewall security tools have hardware and software are tailored for ICSs. These tools allow rules to be defined, governing which devices are allowed to communicate with the system, and what ports and protocols they may use. The firewall locks down communication to the existing devices to ensure proper traffic flow. The firewall recognizes if the communication doesn't look the way it's supposed to, and traffic is blocked. Notifications or alarms can be set up in addition to the traffic block.

5. Develop a strong security culture

Cybersecurity combines common sense and education. Many threats and attacks originate internally and accidently, which underscores the need to get personnel on board with the process and to be vigilant. Create a continuing education plan and include a training process for future employees. Train employees about common social engineering tactics. Social engineering is the art of manipulating people so they give up confidential information—phishing emails that appear to come from a legitimate source, or phone calls to trick people into revealing information. Teach them what to look for, what not to click on, and how to avoid other common traps.

M More ANSWERS

KEYWORD: cybersecurity

Implementing a defense-in-depth cybersecurity strategy

How to secure and help protect an industrial control system (ICS).

GO ONLINE

Additional information can be found at the U.S. Department of Homeland Security's website for the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) https://ics-cert.us-cert.gov/.

Also link to more about Huffman Engineering in the Global System Integrator Database.

CONSIDER THIS

What steps can be added to your facility to help protect your ICS?

6. Employ limited access and unique passwords

Use the strategy of "least-privileges," only gives employees access to what they need to do their jobs, and no more. Force users to have unique passwords, and never leave the system set to the default password. Additionally, users should not write passwords in public view, in the vicinity of the equipment, or elsewhere. Add in two-factor authentication whenever possible by using technology such as a rolling code, biometrics, etc. Two-factor authentication should be mandatory for all devices offering remote- access to the internal system.

7. Physical access defense

Proper physical security measures are often overlooked. For physical access defense, start by securing the entrance to the facility. Consider using security guards, access control systems, fenced perimeters, and locked doors to critical infrastructure systems such as servers and supervisory control and data acquisition (SCADA) control rooms. Remove the key on programmable logic controllers (PLCs) that allows the program to be altered, if available, and lock control cabinets to prevent unauthorized people from accessing them. Also disable or lock the control system's USB ports.

Viruses can be transmitted or data can be stolen through these USB ports, and employees can inadvertently compromise security by charging cell phones through them as well.

8. Maintain a good relationship with a system integrator

Having another set of eyes that knows a company's automation systems inside and out is an invaluable asset. For example, last year, a series of ransomware attacks were mounted against companies globally. A trusted system integrator can assist in or after a cyber attack and help provide a quick recovery if the integrator has intimate knowledge of the customer's ICS applications, processes, and thorough documentation of software programs including recent backups.

Implementing a defense-in-depth cybersecurity strategy doesn't have to be a costly and time-consuming undertaking.

Implementing a few defenses will greatly increase the level of security for an ICS. Control system integrators work directly with a customer's IT department to design and install the desired type of manufacturing cybersecurity technologies and provide training.

Integrators work hand-in-hand with customers or can act as an advisor if required. ce

***Keith Mandachit** is engineering manager, **Sean Creager** is senior electrical engineer, and **Jay Steinman** is mechanical engineer, Huffman Engineering Inc. Edited by Emily Guenther, associate content manager,* Control Engineering, *CFE Media, eguenther@cfemedia.com.*

RADWELL INTERNATIONAL, INC.
RADWELL INTERNATIONAL, INC.

Alexander Horch, HIMA Paul Hildebrandt GmbH

Bringing safety and security together for process control applications

It is important to understand the interaction between safety and security in process control applications to make better overall decisions.

Every production process comes with inherent risks. To achieve the greatest degree of safety and security, it is vital to implement an effective separation of the process control and safety systems, which is required for functional safety and cybersecurity standards. There is a lot at stake, including the employees' health, the company's assets, and the environment.

For a better understanding of the interaction between safety and security, it is helpful to clarify several terms. There are numerous definitions of safety. A general definition of safety is the absence of danger. This means a condition is safe when there are no prevailing hazards. It often is not possible to eliminate all potential risks; especially in complex systems.

A more common definition of safety is the absence of unacceptable risks. Reducing risks to an acceptable level is functional safety's task. An application's safety depends on the function of a corresponding technical system, such as a safety controller. If this system fulfills its protective function, the application is regarded as functionally safe.

This can be clarified with these two examples: oil flowing out of a pipeline and endangering people in the vicinity is a safety issue. A system that cannot prevent icing in a pipeline, even though that is supposed to be its task, and then a critical situation arises, is a functional safety issue. Functional safety systems protect people, facilities, and the environment and are intended to prevent accidents and avoid downtime of equipment or systems.

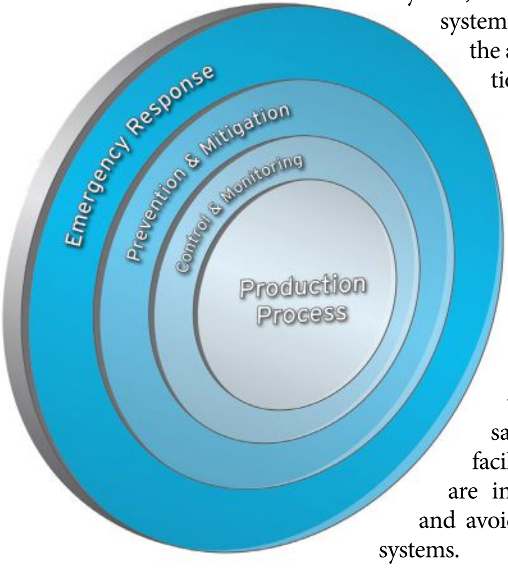


Figure 1: IEC 61511 prescribes separate safety layers for control and monitoring, prevention and containment, as well as emergency measures. Courtesy: *Control Engineering Europe/ HIMA*

Separate layers reduce risks

The process industry increasingly is becoming aware of the importance of relevant standards for the safety and profitability of systems. Technical standard IEC 61511, Functional safety - Safety instrumented systems for the process industry sector, defines the best way to reduce the risk of incidents and downtime. It prescribes separate safety layers for control and monitoring, prevention and containment, as well as emergency measures (see Figure 1). Each of these three layers provides specific functions for risk reduction, and collectively they mitigate the hazards arising from the production process.

IEC 61511 also prescribes independence, diversity, and physical separation for each protection level. To fulfill these requirements, the functions of the different layers need to be sufficiently independent of each other. It is not sufficient to use different I/O modules for the different layers because automation systems also are dependent on functions in I/O bus systems, CPUs and software.

To be regarded as autonomous protection layers in accordance with IEC 61511, safety systems and process control systems must be based on different platforms, development foundations, and philosophies. In concrete terms, this means the system architecture must, fundamentally, be designed so no component in the process control system level or the safety level can be used simultaneously.

Rising risk

In the last 10 years, the risk of cyber attacks on industrial systems has risen due to increasing digitalization. In addition to endangering information security, these attacks increasingly pose a direct threat to system safety. System operators need to be aware of these risks and address them. This can be achieved in a variety of ways. Unlike functional safety systems, which are intended to protect people, these systems

GET MORE THAN YOU PAY FOR . . .
Order Today, Ships Today
12
3
6
9
day if ordered by 6 p.m. ET
FREE shipping - orders over $49
AUTOMATIONDIRECT
2-day Shipping
FREE Technical Support
Located in USA
Voted Best in Service - 15 years straight
VOTED Best in SERVICE 15 YEARS
FREE software and manuals
SureServo
30-day Money-Back Guarantee
30 day
from AUTOMATIONDIRECT.com
The common sense way to buy industrial controls.
We have your stuff! → 99.7% of orders ship complete same day.

AutomationDirect: much more than just a ".com"

AutomationDirect is a non-traditional industrial controls company using the best ideas from the consumer world to serve the automation market. Because of that approach, we can deliver quality products to you for much less than traditional suppliers. See below . . .

AutomationDirect.com HQ, Developmen

AutomationDirect.com HQ and wareho

AutomationDirect.com
Engineering, Development and Research

Our campus is located
We're all here - o
accounting, and of cours

You need quality products at great prices.

Since 1994 our prices have been typically 50% less than traditional suppliers.

Product	AutomationDirect Price/Part Number	VS.	Competitor Price/Part Number
Proximity sensor, 18 mm, 3-wire PNP DC shielded, with quick disconnect	$14.00 PBK-AP-1H		$88.16 A-B 872C-D5NP18-D4
AC Drive, 5 hp, 460V	$410.00 GS2-45P0		$1,320.00 A-B 22B-D010N104
NEMA 12 Enclosure, steel, wallmount (20" x 16" x 8")	$253.00 N12201608		$465.00 Hoffman A-201608LP

*All prices are U.S. published prices, subject to change without notice. AutomationDirect prices as of December 2017 Price List
Hoffman prices are taken from www.newark.com 12/13/2017. Allen-Bradley prices are taken from www.wernerelectric.com 12/13/2017.
Prices may vary by dealer. Many other part numbers are available from vendors.

For decades we've been offering a better value on industrial controls by running our business efficiently and passing the savings on to our customers.

www.AutomationDirect.com/price

FREE shipping - orders over $49
2-day Shipping

You don't want to wait for your order.

We have same-day shipping, it's even FREE if your order is over $49.*

AutomationDirect has always maintained a huge inventory, allowing us to ship 97.5% of orders complete the same day.

*Order over $49, and get free 2-day (transit) shipping within the U.S. and Puerto Rico. (Certain restrictions apply; Canadian orders may take longer based on destination)

30-day Money-Back Guarantee

You want to be confident you're buying quality products.

We stand behind our products and guarantee your satisfaction.

We want you to be pleased with every order. That's why we offer a 30-day money-back guarantee on almost every stock product we sell, including our software. (See Terms and Conditions online for exclusions.)

Voted Best in Service - 15 years straight
VOTED Best in SERVICE 15 YEARS

You insist on getting and you want it FREE

Our technical support ha
voted best in service for 1
in a row. And it won't cos

Many independent industry magazine reader su
the top of their lists for service. In Control Design
voted tops in service for multiple product categor

www.AutomationDirect.com/servic

FREE software and manuals

You want complete p to make the right pu

We have FREE document
of FREE videos, FREE soft
FREE CAD drawings avail

Whether you're deciding on purchasing our prod
you buy, why should you have to pay for the ma

Download the manuals - no purchase necessa

We have **hundreds of videos online** for you to ge
and learn about our products. When shopping onl
looking at has video, it will be available right there

And for almost-FREE online videos that dive dee
product lines, go to **www.interconnnectingauto**
and in-depth training libraries.

Programming software for a complex product ca
help you out by offering **FREE fully enabled sof**
popular products, including the Do-more PLCs, P
CLICK PLCs and C-more Micro HMI. No license or
and **our support is free too**!

In addition to software and documentation onli
drawings for the majority of our product lines.

www.AutomationDirect.com/suppo

99.7% of orders ship comp
See for yourself at www.Auto

nt Center and Warehouses

uses

about 45 minutes north of Atlanta, GA, USA.
ur sales and technical support teams, purchasing,
e our huge warehouses and speedy logistics team.

better service
E.

s been
15 years
t you a cent!

rveys have placed us at
magazine alone, we've been
ies fifteen years in a row.

e

roduct information
rchase decision.

tation, hundreds
ware, and
able 24/7 online.

ucts or learning our products after
nuals? That doesn't make sense.

ry.

et up to speed quickly
line, if a product you're
for you to view.

per into our PLC and HMI
omation.com for intuitive

n be costly, so we try to
tware for a number of our most
roductivity series controllers,
upgrade fees to deal with,

e, we have **FREE CAD**

rt

plete same day!
mationDirect.com

FREE Technical Support
Located in USA

Order Today, Ships Today

This ".com" is powered by ".awesomepeople"!

For over twenty years our sole focus has been customer service. That takes many forms: great prices, fast delivery, and quality products. But regardless of our product selection and other tangibles like pricing, the intangible value of customer service is something that cannot be faked, automated or glossed over.

Our team members here at AutomationDirect.com approach every day with this one goal in mind - serve the customer. It's a simple philosophy that many companies forget or make too complex and fail at. If the answer to any decision is **"Yes, this is good for our customers"**, then we do it.

It's common sense.

"Should we have real upfront pricing online and realtime stock availability?
Yes, this is good for our customers."

"Should we have FREE tech support before, during, and after any sale instead of charging yearly fees for tech support?
Yes, this is good for our customers."

"Should we offer FREE software on many products instead of charging licensing fees?
Yes, this is good for our customers."

"Should we have all our documentation online for FREE so people can access anytime, even before they choose to purchase?
Yes, this is good for our customers."

"Should we offer more selection by consistently introducing more new quality products with great prices monthly, sometimes weekly?
Yes, this is good for our customers."

"Should we offer FREE shipping for orders over $49?
Yes, this is good for our customers."

"Should we be fiscally responsible and run an efficient business so customers can rely on us decade after decade after decade?
Yes, this is good for our customers."

All these are discussions we've had internally and all have had certain aspects of "can we do that?", "that will be hard to accomplish", "no one else is doing that, how can we?". But if you bring it back to the simple answer, "Yes, this is good for our customers", then the perceived obstacles really don't matter.

Our company has evolved dramatically since 1994 and it's this type of decision making by all our team members over the years that keeps our customers coming back and new customers checking us out daily.

If you're a current customer, we sincerely thank you for your business. We wouldn't be here if it wasn't for you and promise to do our best for you every day. If you're new and checking us out for the first time, we hope you give us an opportunity to serve you.

AUTOMATIONDIRECT.com

and measures protect technical information systems against intentional or unintentional manipulation as well as against attacks intended to disrupt production processes or steal industrial secrets.

Safety and security have become more closely meshed. Cybersecurity plays a key role, particularly for safety-oriented systems, because it forms the last line of defense against a potential catastrophe.

Standards define the framework

Compliance with international standards is necessary in the design, operation, and specification of safety controllers. IEC 61508, Functional Safety, is the basic standard for safety systems, which applies to all safety-oriented systems (electrical, electronic, and programmable electronic devices). IEC 61511 is the fundamental standard for the process industry and defines the applicable criteria for the selection of safety function components.

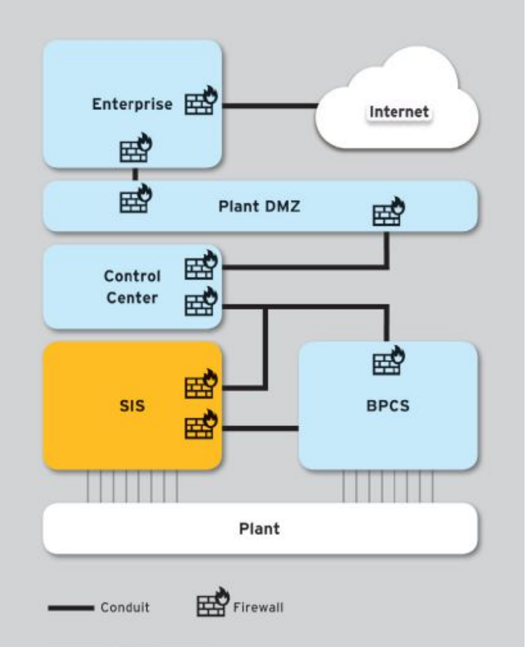
The IEC 62443 cybersecurity series of standards for information technology (IT) security in networks and systems must also be considered. It specifies a management system for IT security, separate protection layers with mutually independent operating and protection facilities, and measures to ensure IT security over the full life cycle of a system. It also requires separate zones for the enterprise network, control room, safety instrumented system (SIS), and basic process control system (BPCS), each of which must be protected by a firewall to prevent unauthorized access (See Figure 2).

Cybersecurity by design

Safety and security are closely related aspects of process systems, which must be considered separately and as a whole.

Standardized hardware and software in process control systems require regular updates to remedy weaknesses in the software and the operating system. However, the complexity of the software architecture makes it difficult or impossible to assess the risks analytically, which could arise from a system update. For example, updates to the process control system could affect the functions of the safety system integrated into the control system.

To avoid critical errors with unforeseeable consequences in safety-relevant processes as a result of control system updates, the process control system must be technologically separate from the safety system. For effective cybersecurity, it is not sufficient to upgrade an existing product by retrofitting additional software functionality. Every solution for functional safety must be conceived and developed with cybersecurity in mind, from the start. This applies equally to the firmware and the application software.



COVER DIAGRAM, figure 2: IEC 62443 requires separate zones for the enterprise network, control room, SIS, and BPCS, each of which must be protected by a firewall to prevent unauthorized access. Courtesy: *Control Engineering Europe/HIMA*

An example of effective protection is a proprietary operating system specifically designed for safety-oriented applications and runs on autonomous safety controllers. It includes all functions of a safety PLC and excludes all other functions, making it immune to typical attacks on IT systems. The CPU and the communication processor need to be separate for operational security even in the event of an attack on the communication processor.

The controllers allow several physically separate networks to be operated on a single communication processor or processor module. This prevents direct access to an automation network from a connected development workstation. In addition, unused interfaces can be disabled individually.

A common feature of the process industry standard and the cybersecurity standard is the required separation of the SIS and the BPCS. This independence of safety systems is a good idea from a practical and economic perspective. The SIS and BPCS have, for example, very different life cycles and rates of change. System operators are free to choose "best-of-breed" solutions from different manufacturers.

Systems independent of the process technology, which can be integrated into process control systems despite physical separation, offer the highest degree of safety and security for critical applications. They are the best way to increase the operational reliability and availability of process systems and improve the overall profitability of a production process. **ce**

***Alexander Horch** is head of the R&D and product management business area at HIMA Paul Hildebrandt. This originally appeared in a Sept. 10 article on the* Control Engineering Europe *website. Edited by Chris Vavra, production editor,* Control Engineering, *CFE Media, cvavra@cfemedia.com.*

M More ANSWERS

KEYWORDS: process control, process safety

Functional safety systems protect people, facilities, and the environment and are intended to prevent accidents and avoid downtime of equipment or systems.

The risk of cyber attacks on process control system has increased due to increased digitalization and can pose a major threat to system and worker safety.

Systems independent of process control technology offer the highest degree of safety and security for critical applications.

GO ONLINE

Read this article online at www.controleng.com for more information about safety and security for process control applications.

CONSIDER THIS

What other steps can companies take to better protect their process control systems from safety and security risks?

Sunil Doddi, CAP, Hydro-Chem, a division of Linde Engineering North America

Understanding industrial control systems security basics

It's critical to implement an in-depth cybersecurity plan to help protect industrial control systems (ICSs) against a cyber attack. Identify threats, vulnerabilities, standards, and documents.

An industrial control system (ICS) is a general term used for any distributed control system, programmable logic controller, supervisory control and data acquisition or any automation system used in industrial environments that includes critical infrastructures. ICS security is designed to protect the system from any interference either intentional or unintentional, which may lead to unintended ICS operations.

Industrial control system security

ICS security can be very broadly categorized as cybersecurity. Though the word "cybersecurity" implies the intention is to look at only the "internet" connection, that is not the case when it comes to ICS environments.

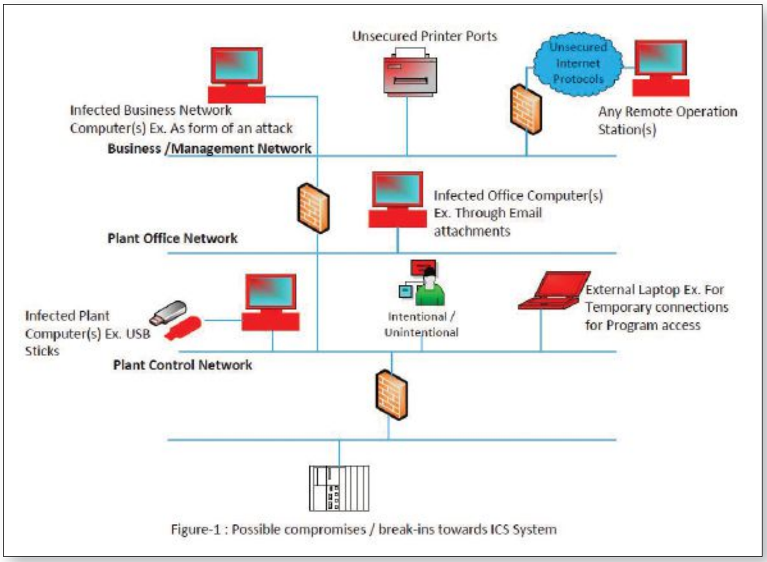

Unsecured Printer Ports
Unsecured Internet Protocols
Infected Business Network Computer(s) Ex. As form of an attack
Business /Management Network
Any Remote Operation Station(s)
Infected Office Computer(s) Ex. Through Email attachments
Plant Office Network
Infected Plant Computer(s) Ex. USB Sticks
Intentional / Unintentional
External Laptop Ex. For Temporary connections for Program access
Plant Control Network
Figure-1 : Possible compromises / break-ins towards ICS System

Figure 1: This illustration shows how safety control systems could be compromised at various points. In addition, unintentional mistakes may happen due to procedural errors at the control network. All graphics courtesy: Sunil Doddi

The necessity of ICS security is sought after even more now that the number of threats has increased. Regulations are being enforced and companies have a legal, moral, and financial obligation to limit the risk. IEC 61511:2016-Functional Safety-Safety instrumented systems for the process industry sector also demands security assessments on safety instrumented system (SIS) design in control systems.

Because of the recent outcry over cyber attacks, ICS security has received more attention as a necessity to protect against external hackers. However, cybersecurity is one part of ICS security; threats against modern control systems come in many forms.

Identify threats

Threats can be external or internal and can be categorized as deliberate, intentional and accidental, or unintentional. Typical external threats are hackers, rival business competitors, or rival organizations/states. Typical internal threats are erroneous actions, inappropriate behavior, disgruntled employees, etc.

To protect against external threats, more needs to be done than just strengthening the network. Not all internal threats can be avoided by strengthening the internal procedures/policies. Optimal ICS security is achieved by strengthening the network and backed up correct policies and procedures.

Identify ICS security vulnerabilities

ICSs used to be standalone systems, but not anymore. ICSs are vulnerable to external threats primarily because of using commercial off-the-shelf (COTS) technology and being highly connected within a network for various reasons. Internal threats occur primarily because of erroneous actions.

A control system's top vulnerabilities are inadequate policies/procedures, no defense-in-depth design, inappropriate remote access controls, improper software maintenance, inadequate wireless communication for control, using control bandwidth for on-control purposes, failure to observe inappropriate

STREAMLINE YOUR CABINET. UNLEASH THE SERVO.

www.br-automation.com/ACOPOSmotor

- → 1 cable for a modular machine design
- → Integrated safety technology CAT 4 / PL e / SIL 3
- → STO, STO1, SBC, SOS, SS1, SS2, SLS, SDI, SLI, SMS, SLP, SMP, Safe Homing, Safe Robotics
- → Local I/O
- → 500 W up to 4 kW
- → CNC, robotics, motion control
- → reACTION Technology with 1 µs response time

ETHERNET POWERLINK

open SAFETY

PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

B&R

input #10 at www.controleng.com/information

activity in the system, control network data is unauthenticated and inadequate to support critical components and systems. A threat can use many pathways to enter into a control network (See Figure 1).

Firewalls can help disrupt a threat's pathway into a system. Installing a firewall is easy, programming one is difficult, and programming correctly is very difficult. An improperly configured firewall is equal to not having one.

An SIS is susceptible to threats if COTS technology is being used. Especially if they are integrated as part of the control network and communicate over an insecure, open protocol. Compromising an SIS may lead to temporary setback or a loss.

System availability is the prime objective since continous and time-critical operations are performed by ICSs. Human safety is also paramount. In IT environments, confidentialty matters and system availability is not a major priority. In ICS environments, companies can't afford to lose control for even a few seconds because response time is critical.

Security standards for ICSs

Governments and other industry organizations are developing security standards to provide guidance and suggesting best practices to strengthen systems against potential threats.

Some of the main standards are:

- ISA99 – Industrial Automation and Control Systems Security /IEC 62443 series of standards
- The National Institute for Standards Technology (NIST) SP 800-82 – Guide to Industrial Control Systems Security standard
- The North American Electric Reliability Council CIP series of standards.

Like a functional safety lifecycle, a cybersecurity's lifecycle also depends on three fundamental components: analysis, implementation, and maintenance. The lifecycle is a continuous process and feedback is crucial (See Figure 2).

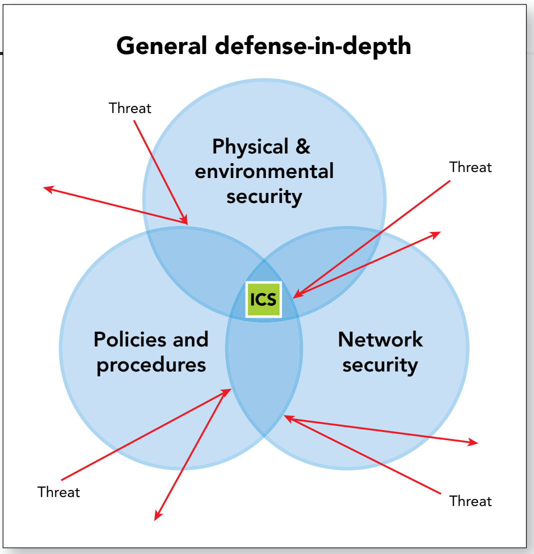


Figure 2: Defense-in-depth can be incorporated by strengthening security measures. If the network security is broken, it can be countered with correct policies and procedures.

It's difficult for some companies to maintain a budget to implement and maintain a cybersafety lifecycle. Without the commitment of company leadership, the cybersafety lifecycle likely will fail. Present a business case to management outlining the potential threats, consequences, and benefits to the business.

A proper risk assessment should occur to suit the organization's needs. The risk assessment may include the plan, the test environment, and metrics and documentation.

Various tools are available to evaluate risk assessments. A qualitative or quantitative approach can be chosen based on the organization's requirements to evaluate the impacts of a safety cycle. In a quantitative assessment, previous data is used. In qualitative assessments, proper definition consequence parameters are required.

In suitable test environments, a scanner can perform a vulnerability assessment. Results from scanner tools, as Figure 1 shows, are not enough. ICS security alone does not protect against from cyber attacks but also involves personnel, physical, and environmental security.

Physical security requirements may include controlling access to restricted areas, CCTV, motion sensors, thermal video systems, and other areas. Environmental protection against dust, temperature, and toxic gases can be achieved with a proper HVAC system and proper alarm systems for failure identification.

Awareness, policies, and procedures are crucial for addressing accidental and internal threats. Access and authorization control to access and perform particular actions needs to be addressed through policies and procedures that are put in place. Logs also can be used to keep track of access levels.

Security plans also need to be incorporated while developing software to achieve software security assurance. Cybersecurity certified components shall be used in the control system. An in-depth defense technique is necessary to secure the ICS and minimize the risk.

Since cyber threats rapidly change, security risk management should be a continuous process. A periodic review and audit of the cybersafety lifecycle is necessary to maintain operations. This includes patch management, antivirus updates, and being aware of industry trends and risks. **ce**

***Sunil Doddi** is a controls systems engineer at Hydro-Chem, a division of Linde Engineering North America. Edited by Emily Guenther, associate content manager,* Control Engineering, *CFE Media, eguenther@cfemedia.com.*

M More ANSWERS

KEYWORDS: Industrial control system, safety lifecycle

Determining security standards for industrial control systems (ICSs)

The purpose of implementing cybersecurity measures for an ICS

Threats that leave ICSs vulnerable to cyber attacks.

CONSIDER THIS

What pathways are vulnerable in your system that needs to be protected against threats?

GO ONLINE

See related articles on cybersecurity on www.controleng.com.

Read more online about ICS security standards and various cybersecurity tools.

SIEMENS
Ingenuity for life
// TIA Portal Openness
DeviceAggregation devices = _tiaProject.
devices.Where(device => device.Subtype
.Select(device => device.DeviceItems)
Start
Devices & networks
PLC programming
Motion & technology
Configuration of control devices
Visualization
Online & Diagnostics
Open existing project
Create new project
Migrate project
Close project
Welcome Tour
First steps
Install software
First steps
Project: "Project2" was opened successfully. Please sele
Devices & networks
PLC programming
Motion & technology
Control devices
Visualization
Configure a dev
Write PLC progr
Configure technology objec
Configure/select
Configure an HMI

Robert Wakim, Stormshield

Finding common ground in IT/OT convergence

The interconnection of information technology (IT) and operational technology (OT) is a source of new opportunities and challenges. Manufacturing and engineering companies are becoming more connected, but this exposure to external data flows inevitably leads to new risks.

One of the biggest challenges facing the industrial sector is understanding the risk and impact cybersecurity attacks can have as the transition to Industrie 4.0 and the Industrial Internet of Things (IIoT) gains momentum. Companies are starting to realize there is a significant gap between the priorities of operations technology (OT) and information technology (IT) teams and this has a major effect on cybersecurity initiatives.

For engineers on the OT side, the focus is on available services. Production must continue because any interruption could result in a serious setback and it must be safe because engines, motors, and processors carry a physical risk to operators. IT, however, is worried about a computer network security breach.

However, many manufacturers either believe their production processes are unconnected to the internet, or they haven't considered there was even an internet connection in the factory.

The gap between the factory and the internet has become virtually non-existent. With the growth of IoT-connected devices, cybersecurity risks are escalating. For most engineering firms, however, the focus remains on designing sophisticated systems that are robust and safe, and this is having a detrimental effect on securing networks.

How high is the risk?

In many ways, the lack of real concern in the industrial sector to date is understandable. The technology used in manufacturing enterprises is rarely standard, highly complex, and often unique. This would mean a malicious attack on industrial processes would have to be very specific in order to do harm.

The status quo is about to change. Reports about a new virus called Industroyer have indicated it has the power to seriously damage or compromise industrial control systems (ICSs). This virus can speak four industrial languages and is highly customizable and can be used in targeted attacks.

Industrial operational systems, while robust, are not safe from attack, and they aren't compatible with today's interconnected environment. Now, as OT and IT systems converge, there is an urgent need to find a balance between ensuring availability and securing themselves against cyber attacks.

Changing mindsets

Engineers speak a different language than IT managers. They need to agree upon a common approach and strategy.

The influence of Industrie 4.0 on automation is bringing about major changes and greater adoption of cloud and cognitive computing. This creates a need for massive computer resources to support the flow of data to and from the cloud via IoT-connected devices. Factories are communicating in real-time across networks and they need to be secure.

Standard firewalls and security software are not enough. Next-generation firewall hardware needs to be built to adapt to industry prerequisites such as DIN-rail mounts.

OT and IT need to work together to combat the risks regardless of what they are. The threat to the new generation of manufacturing enterprises does not have to impact companies if appropriate consideration is given to safety, availability, and security. ce

Robert Wakim is industrial offer manager at Stormshield. This originally appeared in a November 6 article on the Control Engineering Europe *website. Edited by Chris Vavra, production editor,* Control Engineering, *CFE Media, cvavra@cfemedia.com.*

M More ANSWERS

KEYWORDS: cybersecurity, Industrie 4.0

Increased connectivity increases the risk of a potential cybersecurity attack against manufacturers.

Operations technology (OT) and information technology (IT) need to work together to combat cybersecurity risks.

GO ONLINE

Read this article online at www.controleng.com for more information about cybersecurity and how OT and IT can work together.

CONSIDER THIS

What else can be done to better protect OT and IT systems as they become more connected?

Push the Edge

What's your biggest challenge? Compliance? Efficiency? Prevention? Productivity?

Chances are, SeaConnect hardware coupled with SeaCloud software can reinvent your challenge as an opportunity, providing continuous, secure connection, control and data. So give us a call, and find out what SeaConnect can do for you.

PROUDLY MADE IN THE USA

SEALEVEL®

We put the I/O in IoT.™

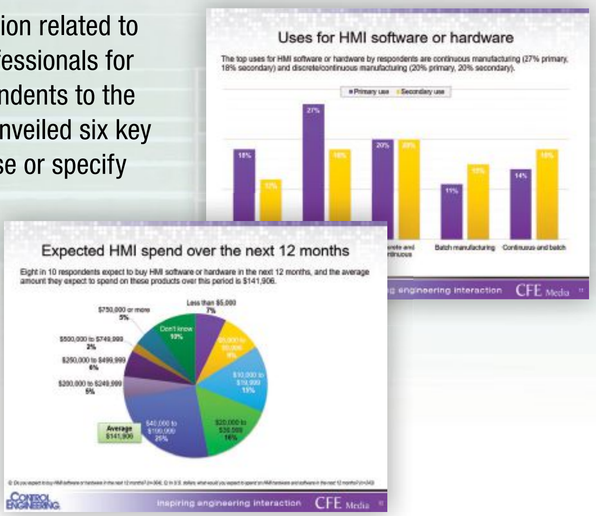
Sealevel.com • 864.843.4343

input #12 at www.controleng.com/information

research

2018 HMI Software & Hardware Research

Control Engineering performed this research to acquire information related to the buying and specifying habits of automation engineering professionals for human-machine interface (HMI) software and hardware. Respondents to the *Control Engineering* 2018 HMI Software & Hardware study unveiled six key findings regarding what end users expect and how they purchase or specify human-machine interface (HMI) software and hardware.


Uses for HMI software or hardware

The top uses for HMI software or hardware by respondents are continuous manufacturing (27% primary, 18% secondary) and discrete/continuous manufacturing (20% primary, 20% secondary).

Expected HMI spend over the next 12 months

Eight in 10 respondents expect to buy HMI software or hardware in the next 12 months, and the average amount they expect to spend on these products over this period is $141,906.

According to the data in the 2018 report, the top uses for HMI software or hardware by respondents are continuous manufacturing (27% primary, 18% secondary) and discrete/continuous manufacturing (20% primary, 20% secondary). Also according to the study, eight in ten respondents expect to buy HMI software or hardware in the next 12 months, and the average amount they expect to spend on these products over this period is $141,906.

Download the new *Control Engineering* HMI Software & Hardware Research today!

www.controleng.com/2018HMIReport

CONTROL ENGINEERING®

Ken Modeste, UL

Learn how to stay ahead of cyber attacks

Use a risk-based approach to minimize risk against cyber attacks, especially for critical infrastructure facilities and industries.

As governments, businesses, and individuals become more connected each day, the risks of cyber attacks are increasing exponentially and in tandem with this connectivity. An interesting shift is starting in cyber attack activity, intention, and attribution.

Independent hackers or organizations used to be at the forefront of cyber attacks; now, nation-state sponsored attacks against government institutions, businesses (especially those in the critical infrastructure segments) have increased.

The cyber-weaponization of global nations and the attacks that inevitably follow are not necessarily new, but this territory has recently been forced into the spotlight, and now is the time for companies to take action to guard against the risk of a cyber attack.

Fortunately, companies can learn a lot from past attacks, even from those outside their industry, to improve their defensive postures and to take necessary cybersecurity measures.

Looking at what made some of these nation-state cyber attacks successful, it is possible to identify patterns in attack methods, understand common access paths, and address ways in which businesses can safeguard their sensitive systems and information against malicious activity. Due to the constant evolution of technology and software that is used to carry out cyber attacks, there is no one solution. However, with training and robust internal processes, organizations can help minimize the risk of a cyber attack and the potential damage that can occur.

More ANSWERS

KEYWORD: Cyber attack

Defining different types of cyber attacks

How to minimize the risk against a cyber attack.

GO ONLINE

Read more online about cybersecurity strategies and risks at www.controleng.com.

CONSIDER THIS

How can you help your organization minimize the risk of an external or internal cyber attack?

History of cyber attacks

One aspect of cyber attacks (or cyber warfare) that makes them difficult to track and assess is it's difficult to identify who is to blame for the attack. It is still possible to assess patterns from one attack to the next, and regardless of attribution, most major attacks share two common traits: sophisticated technology (though not exclusively) and exploitation of the human element. From the now-infamous Russian hacker group, "Cozy Bear," to North Korea's elite hacker group, "Bureau 121," these attacks are meticulously planned and, in some situations, carried out in multiple stages over long periods of time. To illustrate common tactics, software, and malware often used by nation-state attacks, three examples are highlighted.

1. Dragonfly 2.0, critical infrastructure

As a major component of critical infrastructure, the energy sector has become a prime target for cyber attacks. One of the most prominent recent attacks is the Ukrainian power outage that occurred in December 2016, and it is possible that another group, currently referred to as "Dragonfly 2.0," is currently pursuing the same end goal in Europe and North America.

The main strategy of this hacker group appears to be gaining access to the victim's network and, again, humans are being exploited as the main access point. By deploying several strategies, including malicious emails, watering hole attacks (when frequently visited websites are infected with malware), software infected with trojan viruses and various malware programs, it is now believed Dragonfly spent 2011 through 2014 gathering information and credentials before resurfacing in 2017 to potentially launch an attack.

2. Sony Pictures Entertainment

Prior to the release of 2014's "The Interview," Sony pictures cancelled New York openings due to threats of violence from a hacker group that also claimed responsibility for the Sony data breach earlier that year. Though this was an attack aimed at a private company, the breach was used as leverage to threaten physical harm while the prior attack left many internal communications exposed and forced Sony to take thousands of systems offline.

3. 2016 Democratic National Convention email

The hacking of the Democratic National Convention email system and subsequent hacking of

Democratic candidate Hillary Clinton's personal email made global headlines. Arguably, this particular attack brought the threat of nation-state cyber warfare to the main stage.

Although it was initially difficult to identify the cyber attack source, CrowdStrike, a cybersecurity company, identified Cozy Bear and Fancy Bear, as the groups responsible. Here, the human element was exploited. Spear-phishing emails—emails that appear to be from trustworthy sources but actually contain malware or other malicious content—were sent to government agencies, nonprofits, and contractors.

Developing a proactive cybersecurity strategy

Understanding the unique motivation of nation-state cyber attacks is essential to developing a strategy to safeguard a system against an array of potential breaches. Though traditional espionage is rooted in the desire to learn, nation-state cyber attacks often seek to sabotage through direct action or interference.

Due to the complexity of these cyber attacks, they are often conducted in stages, beginning with information gathering. Fortunately, despite the end goal of these attacks being fairly unique, nation-state sponsored hackers typically use the same methods–some sophisticated, others fairly off-the-shelf as independent attacks in their plan.

First, these groups aim to establish a regular presence in the system by using advanced persistent threats (APT) and remote access tools (RAT) to avoid detection and bypass security at unprepared facilities. From there, data mining would begin as the hackers worked to harvest information that ultimately will be used to complete the attack (leak the data, leverage the data, use the data to control/damage the system/infrastructure, etc.) or launch subsequent attacks.

Because of these threats, it is tempting for organizations to want to double down on technology in an effort to keep pace, but approaching the issue from a strategic standpoint by taking a risk-based approach would be more effective overall.

Secure systems and facilities by improving the human side of systems interaction. In nearly every cyber attack, humans unwittingly gave access to hackers by opening and spreading infected emails and clicking on links. To minimize the likelihood of damage, limit user access to critical systems as necessary as a starting point. Continuous, regularly updated staff training is the keystone to mitigating cybersecurity threats and developing a solid cybersecurity strategy.

Cybersecurity tools

Tools and technology remain important, but with government-backed hacking groups having access to the latest technology, it is clear these individuals and organizations need to stay one step ahead—especially with legacy software and systems. An effective cybersecurity strategy needs to involve more than just technology.

By training staff to understand the risks of cyber attacks and the common pathways for these attacks, such as spear-phishing, potential issues can be reported and mitigated before malicious activity can set in. Even the most effective security system can be thwarted by human error.

> ❛ Due to the constant evolution of technology and software that is used to carry out cyber attacks, **there is no one solution.** ❜

Nevertheless, software security remains a valuable part of a cybersecurity solution, and it is important to identify, assess, and correct vulnerabilities in software applications before the software is integrated into a system and while it is in use.

Fortunately, while working to improve technology, the industry has also been working to develop criteria necessary to assess the software used to protect sensitive information and critical infrastructure from cyber attacks. Engaging with a third-party for these evaluations can help save time and resources while instilling confidence in the software.

Cybersecurity programs help minimize risk by helping ensure that all software is secure and remain secure. By deploying consistent testable criteria, companies can begin to reduce exploitation, address known malware, enhance security controls, and expand security awareness. All of these are essential steps for conducting business today.

With a strong software foundation in place–including procedures to ensure that the evaluated software remains updated, effective, and secure–staff training creates a final, necessary layer of protection and another set of watchful eyes.

With every new security development, new malware and access methods are being tested and deployed by hackers globally. This is the reality of living with the convenience of a connected world. However, it is possible to remain aware and ready in the face of increasing cyber attacks. **ce**

__Ken Modeste__ is cybersecurity lead and global principal engineer, UL. Edited by Emily Guenther, associate content manager, CFE Media, Control Engineering, *eguenther@cfemedia.com.*

Anil Gosine, MG Strategy +

Threat intelligence is a critical organizational need

Continuous threat intelligence collection, analysis, and optimization can help organizations improve cybersecurity measures.

Cybersecurity managers face many challenges, with corporate boards demanding awareness of cyber risks, faster processing of complex data, and efficiently managed services for an increasing number of intelligent devices. Security teams are in a better position to defend their organizations against threats if they take the proper preventive measures. Tools and staff need to be augmented with threat intelligence.

Threat intelligence is no longer just for large, well-funded organizations. It is now required to be an overall component of mitigation strategies for all businesses that operate within this evolving technological environment. Small businesses can access credible threat intelligence sources that can be based on an organization's profile and supply chain. Critical data that used to be in a secured data center now moves across an increasingly complex ecosystem of networked environments including the Industrial Internet of Things (IIoT), Internet of Things (IoT), cloud servers, virtualized environments, and mobile devices.

Cybersecurity and threat intelligence

The rate of change in some enterprise environments is so rapid many organizations struggle to keep pace with the evolving nature of cyber threats or have the ability to stay tuned into the threats that arise. To build an effective cybersecurity strategy, an organization needs to be aware of specific cyber threats and understand how those threats impact the organization.

Threat intelligence provides context, indicators, increased awareness, and actionable responses about current or emerging threats. This is designed to aid in decision-making at an operational, tactical, or strategic level. Cyber adversaries are using more sophisticated tools, techniques, and procedures that evade stand-alone security plans. Organizations need an evidence-based, holistic view of the threat landscape with a proactive security posture to defend organizations from a wide array of potential threats.

The goal behind threat intelligence services is to provide organizations with the ability to become aware, recognize, act upon attack indicators, and comprise scenarios in a timely manner that better protect against zero-day threats, advanced persistent threats, and exploits. Security teams across the world are challenged to discover, analyze, and interpret the vast number of daily events to discover attacks. Security consortiums are leading efforts to automatically detect, contextualize, prioritize, perform forensic analysis, automate compliance, and respond to incidents go beyond security information management to security threat intelligence.

Facility owners should define what they hope to achieve from threat intelligence; including:

- Types of alerts needed
- Vendor news
- How intelligence is collected, reported and communicated to relevant stakeholders
- Analysis process
- How threat intelligence would be used.

Threat intelligence feed

An analysis identifying the organization's needs through an internal assessment of the organization's processes, infrastructure, requirements, ability to manage threat intelligence and security posture should be performed. Customers should compare the data feed and capabilities, alerts and reports, relative subscription prices and support offered by providers.

Threat intelligence feeds are becoming a dominant method as an intelligence gathering process for organizations that are developing their threat intelligence capability. These feeds provide a major benefit of combining intelligence into one source that is easy to digest. The real-time nature of threat

More ANSWERS

KEYWORDS: **Threat intelligence feeds, cybersecurity**

The importance of threat intelligence feeds

Implementing a successful mitigation strategy against cyber attacks

CONSIDER THIS

How would implementing a threat intelligence feed improve your organization's defense against a cyber attack?

GO ONLINE

See related articles on cybersecurity at www.controleng.com intelligence feeds is critical, especially when integrated with security information and event management (SIEM) platforms to allow for automatic comparisons of other feed entries.

Most organizations lack the resources and maturity in their security platforms to take advantage of threat intelligence feeds, which should evaluate the threat information against internal vulnerability assessments to allow for better prioritization of security controls.

A threat intelligence platform should prepare a defense for the organization. Combining threat intelligence capabilities to an organizations' software, hardware, and policy defense strategy enhances the staff's ability to search for advanced attacks, profile atypical malware, and detect potential adversaries. Typical internal threat intelligence teams have been deployed and structured in a way that is costly, hands-on, and misaligned to the organization's security posture.

Customers should work with their provider to improve subscription offerings, selected offerings, technical indicator feeds for integration, specific summary reports on events and emerging cyber threats, trends within the various business sectors and ensure that it is aligned to a long-term vision with integrated processes, and business requirements.

Too few cybersecurity professionals, tools

The industry still has to address the growing shortage of skilled cybersecurity professionals, isolated security products, lack of integration with other devices and management tools, lack of funding, and inadequate correlation of threat data. Companies must be mindful implementing programs to avoid the typical failings such as not integrating threat intelligence into the enterprise platform, consuming but not sharing data, manual processes becoming a burden, no real-time data to provide security awareness, and lacking contextualized information.

In a global environment where cyber attacks are generated at a machine level, customers must ensure the identification, sharing, comprehension, and application of threat intelligence is as automated as possible. An automated platform allows for easy access to the intelligence and the ability to contextualize and prioritize attacks for immediate mitigation strategies. Effective intelligence assesses intelligence from various sources and source types to create a better threat and risk image for an organization.

The value to end customers is not the quantity of the various intelligence feeds, but the applicability of those feeds to their entire environment. The ability to customize dashboards and filters to continuously illustrate threats allows security teams to focus on threats that impact the organization. The threat intelligence market offers different types of information feeds that are not necessarily aligned to any industry or large manufacturer installed base. Though intelligence platforms must be recognized as a critical component to cybersecurity, organizations must define their high-level requirements, functional requirements, and visibility requirements.

> ‘**Threat intelligence feeds are becoming a dominant method** as an intelligence gathering process for organizations that are developing their threat intelligence capability.’

Through collecting continuous threat intelligence, analysis, and optimization, organizations can increase their protective measures and strengthen their security tools. Significant and beneficial trends for cybersecurity in the following areas include:

- Threat awareness over the past 5 years, has risen from 25% to 75%. Companies have realized that cyber attackers had the advantage of knowing more about their networks than they did and are now becoming more proactive.
- The percentage of organizations that have formalized in-house/out sourced teams to address threat intelligence has risen from 25% to 45% over the past two years.
- The overall level of satisfaction with various threat intelligence elements that companies use is approximately 73%. This may be skewed as some may not understand what they are not receiving from other threat intelligence.

The industry also is making progress as data science and machine-learning models are delivering entirely new ways of looking at threats; this has the effect of avoiding the dependency of seeing the threat previously to provide security. Data science and machine-learning models can evaluate the traffic based on the collective knowledge of all internal and external threats previously to ascertain discrepancies that may become threats. According to recent research including reports from Statista and IDC, it's estimated that global external threat intelligence services spending is expected to increase to over $1.6 billion by the end of 2018. **ce**

__Anil Gosine__ is a global program manager at MG Strategy +, a CFE Media content partner. Edited by Emily Guenther, associate content manager, Control Engineering, *CFE Media, eguenther@cfemedia.com.*

Tanya M. Anandan, RIA

Artificial intelligence's impact on the robotics industry

Researchers and manufacturers are teaching robots how to learn and handle complex tasks with artificial intelligence (AI), but capabilities remain short of what people believe robots can achieve. AI is defined more broadly now than it was previously, which may create some confusion.

Researchers and entrepreneurs with decades of working in artificial intelligence (AI) are trying to help people better understand its elusive nature. They're working to reduce some of the confusion and misconceptions around AI and show how it's being used in robotics for industrial applications.

"I think the biggest misconception is how far along it is," said Rodney Brooks, chairman and CTO of Rethink Robotics. "We've been working on AI, calling it AI since 1956 (when the father of AI, John McCarthy, coined the term "artificial intelligence"), so roughly 62 years. But it's much more complicated than physics, and physics took a very long time. I think we're still in the infancy of AI."

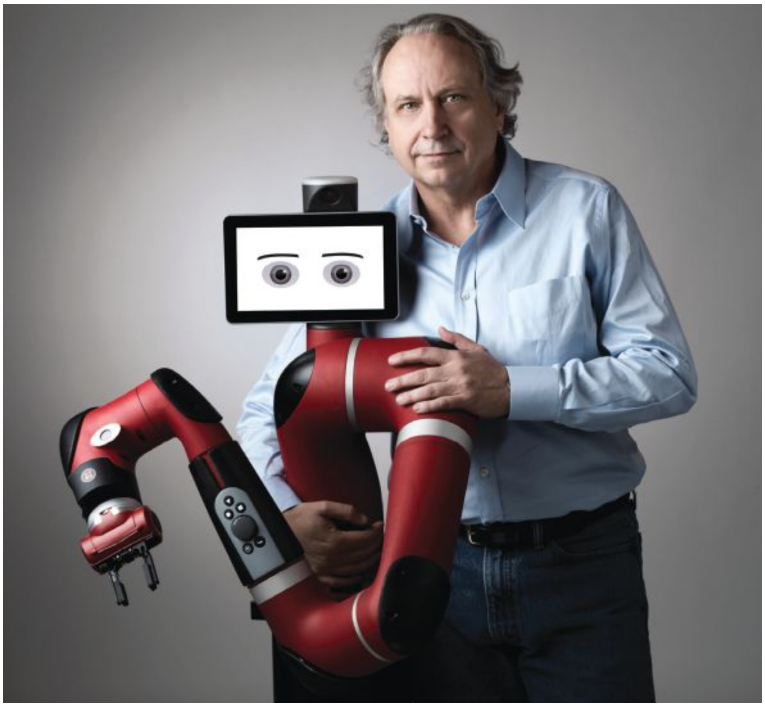


Figure 1: Rodney Brooks says artificial intelligence (AI) is still in its infancy. There's no foreseeable competition between machine intelligence and human intelligence; humans remain smarter. Courtesy: Rethink Robotics/Robotic Industries Association (RIA)

Brooks believes much of the AI hype comes from recent press covering jaw-dropping demonstrations of anthropomorphic and animal-inspired robots, or spectator sports pitting AI systems against humans playing chess, Jeopardy!, ping-pong, and Go. AI is here, but it is taking baby steps.

Some of the misunderstanding stems from equating machine performance with competence. When we see a human perform a certain task, we can assume a general competence—skills and talent—the person must possess to perform that task. It's not the same with AI.

"An AI system can play chess fantastically, but it doesn't even know that it's playing a game," said Brooks. "We mistake the performance of machines for their competence. When you see how a program learned something that a human can learn, you make the mistake of thinking it has the richness of understanding that you would have."

Knowing what AI is and isn't

AI has become a marketing buzzword. Like "robot" before it, now everything is seemingly AI-powered. What is and isn't AI is sometimes difficult to pinpoint. Even the experts hesitate when it comes to identifying definitively what is and isn't AI. As Brooks noted, what was considered AI in the 1960s is now taught in the very first course on computer programming. But it's not called AI.

"It's called AI at some point," said Brooks. "Then later it just becomes computer science."

Machine learning, and all of its variations, including deep learning, reinforcement learning, and imitation learning, are subsets of AI.

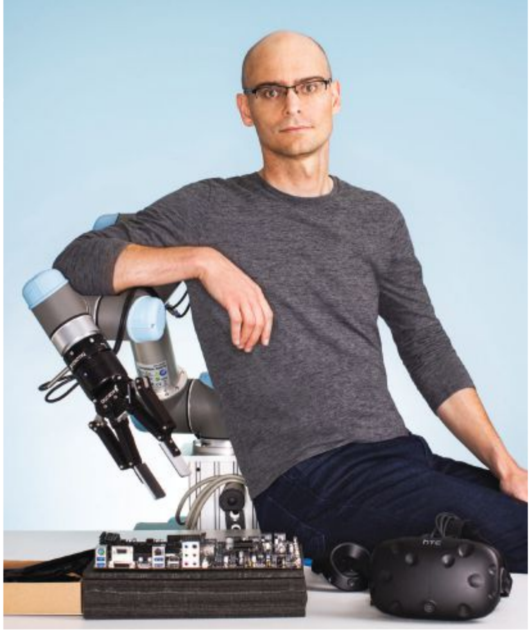


Figure 2: Pieter Abbeel is transitioning breakthrough research in machine learning into real world industrial applications for robots that can learn new skills on their own. Courtesy: Embodied Intelligence/RIA

"AI was a very narrow field for a while. Some people saw it very specifically around a set of search-based techniques," said Ken Goldberg, a professor and distinguished chair in industrial engineering and operations research at the University of California (UC) Berkeley. "Now AI is widely seen as an umbrella term over robotics and machine learning, so now it's being embraced as a whole range of subfields."

Advanced forms of computer vision are a form of AI. "If you're just inspecting whether a screw is in the right place, we've had that since the '60s. It would be a stretch to call that AI," said Goldberg. "But at the same time, a computer vision system that can recognize the faces of workers, we generally do think of that as AI. That's a much more sophisticated challenge."

Lack of context

An important distinction between human intelligence and machine intelligence is context. As humans, we have a greater understanding of the world around us. AI does not.

"We've been working on context in AI for 60 years and we're nowhere near there," said Brooks. "That's why I'm not worried that we're going to have super intelligent AI. We've been successful in some very narrow ways and that's the revolution right now, those narrow ways. Certainly speech understanding is radically different from what we had a decade ago. I used to make the joke that speech understanding systems were set up so that you press or say '2' for frustration. That's no longer true."

He cited Amazon's Alexa as an example. Google's Assistant and Apple's Siri are two more.

"You say something to Alexa and it pretty much understands it, even when music is playing, even when other people in the room are talking," said Brooks. "It's amazing how good it is, and that came from deep learning. So some of these narrow fields have gotten way better. And we will use those narrow pieces to the best advantage we can to make better products.

"When I started Rethink Robotics, we looked at all the commercial speech understanding systems. We decided at that point it was ludicrous to have any speech recognition in robots in factories. I think that's changed now. It may make sense. It didn't in 2008."

Speech recognition compiles the right word strings. Brooks said accurate word strings are good enough to do a lot of things, but it's not as smart as a person.

"That's the difference," he said. "Getting the word strings is a narrow capability. And we're a long way from it being not so narrow."

These narrow capabilities have become the basis for many optimistic AI predictions that are overly pessimistic about our role as humans in that future.

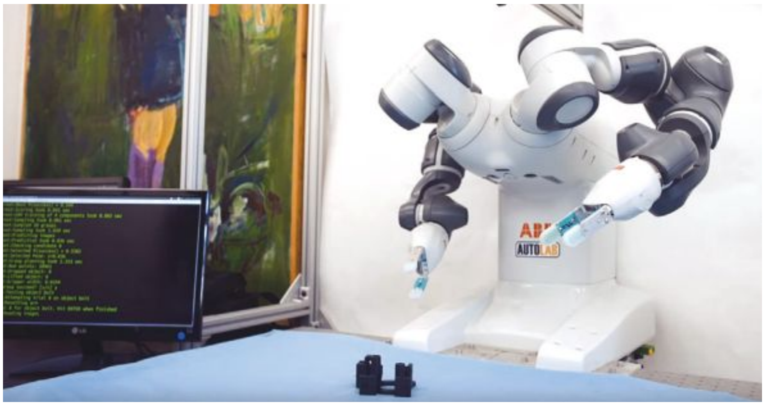


Figure 3: A robot manipulates objects it has never encountered before after researchers teach a neural network how to recognize objects from millions of 3-D models and images. Courtesy: University of California, Berkeley/RIA

AI research in the real world

Goldberg stresses multiplicity over singularity, noting the importance of diverse combinations of people and machines working together to solve problems and innovate. This collaboration is especially important as AI's applications exit the lab and enter the real world.

Pieter Abbeel, a professor in the department of electrical engineering and computer sciences at UC Berkeley, who is working to bring AI to the industrial world as president and chief scientist of Embodied Intelligence, also stresses the importance of humans and machines working together.

"That's part of the challenge," said Abbeel. "How are humans able to use this technology and take advantage of it to make themselves smarter, rather than just have these machines be something separate from us? When the machines are part of our daily lives, what we can leverage to make ourselves more productive, that's when it gets really exciting."

While Abbeel is excited about AI's prospects, he thinks some caution is warranted.

"I think there is a lot of progress, and as a consequence, a lot of excitement about AI," he said. "In terms of fear, I think it's good to keep in mind that the most prominent progress like speech

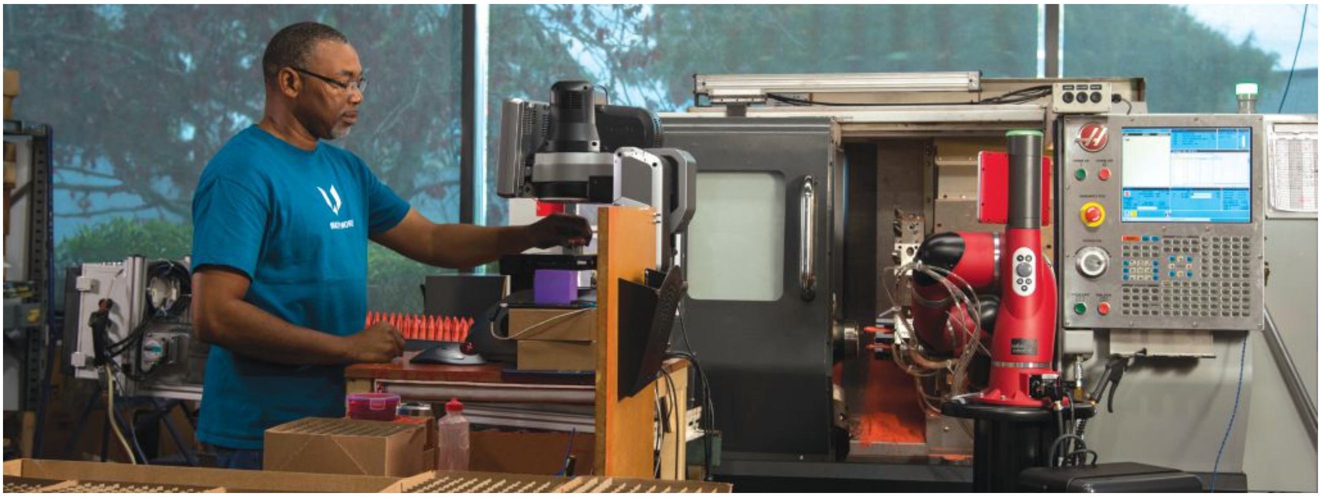


Figure 4: A collaborative robot with integrated artificial intelligence (AI) tends a computer numerical control (CNC) lathe at a custom injection molder, automating the process of improved product quality and production efficiency, and saving operators from repetitive tasks. Courtesy: Rethink Robotics/RIA

recognition, machine translation, and recognizing what's in an image are examples of what's called supervised learning."

Abbeel said it's important to understand the different types of AI being built. In machine learning, there are three main types of learning: supervised learning, unsupervised learning, and reinforcement learning.

"Supervised learning is just pattern recognition," said Abbeel. "It's a very difficult pattern to recognize when going from speech to text, or from one language to another language, but that AI doesn't really have any goal or any purpose. Give it something in English, and it will tell you what it is in Chinese. Give it a spoken sentence, and it will transcribe it into a sequence of letters. It's just pattern matching. You feed it data—images and labels—and it's supposed to learn the pattern of how you go from an image to a label.

"Unsupervised learning is when you feed it just the images, no labels," said Abbeel. "You hope that from just seeing a lot of images that it starts to understand what the world tends to look like, and then by building up that understanding, maybe in the future it can learn something else more quickly. Unsupervised learning doesn't have a task. Just feed it a lot of data.

"Then there's reinforcement learning, which is very different and more interesting, but much harder. (Reinforcement learning is credited for advancements in self-driving car technology.) It's when you give your system a goal. The goal could be a high score in a video game, or win a game of chess, or assemble two parts. That's where some of that fear can be justified. If AI has the wrong goal, what can happen? What should the goals be?"

It's important humans and artificial intelligence don't evolve in a vacuum from each other. As we build smarter and smarter machines, our capabilities as humans will be augmented.

"What makes me very excited about what we're doing right now at Embodied Intelligence is that the recent events in artificial intelligence have given AI the ability to understand what they are seeing in pictures," said Abbeel.

Deep learning for robot grasping

Goldberg's Autolab has been focused on AI for over a decade and has been applying it to projects in cloud robotics, deep reinforcement learning, learning from demonstrations, and robust robot grasping and manipulation for warehouse logistics, home robotics, and surgical robotics.

The lab's Dexterity Network (Dex-Net) project has shown AI can help robots learn to grasp objects of different size and shape by feeding millions of 3-D object models, images, and the metrics of how to grasp them to a deep-learning neural network. Previously, robots learned how to grasp and manipulate objects by practicing with different objects over and over, which is a time-consuming process. By using synthetic point clouds instead of physical objects to train the neural network to recognize robust grasps, the latest iterations of Dex-Net are much more efficient, achieving a 99% precision grasping rate.

In the long term, Goldberg hopes to develop highly reliable robot grasping across a wide variety of rigid objects such as tools, household items, packaged goods, and industrial parts.

Deep-learning collaborative robots

Rethink Robotics' Intera 5 software is designed to make Baxter and Sawyer collaborative robots smarter. Brooks said there's a lot of AI in the robots' vision and training capabilities.

"Traditional industrial robots don't have much intelligence," said Brooks. "But going forward, that's what we're doing. We're putting deep learning into the robots. We're trying to deal with variation because we think that's where 90% of manufacturing is with (robots) working in the same space as humans."

Sawyer and Baxter robots have a train-by-demonstration feature that puts AI to work.

"When you're training it by demonstration, you show it a few things by moving its arm around, and it infers a program called a behavior tree," said Brooks. "It writes a program for itself to run. You don't have to write a program."

Intera 5 is a graphical programming language. Brooks said you can view it, modify it, or you can write a program in a behavior tree, which bypasses the option for the program to do it automatically.

AI changes robot programming

AI is changing the way robots are programmed. Abbeel and his team at Embodied Intelligence are harnessing the power of AI to help industrial robots learn new, complex skills.

Their work evolved from Abbeel's research at UC Berkeley, where they had a major breakthrough in using imitation learning and deep reinforcement learning to teach robots to manipulate objects. The startup uses a combination of sensing and control to teleoperate a robot. For the sensing, an operator wears a virtual reality (VR) headset that shows the robot's view through its camera.

On the control side, VR devices come with handheld devices that the operator holds. As the operator's hands move, that motion is tracked. The tracked coordinates and orientation are fed to a computer that drives the robot. That way the operator has direct control, like a puppeteer, over the motions of the robot grippers.

"We allow the human to embed themselves inside the robot," said Abbeel. "The human can see through the robot's eyes and control the robot's hands."

He said humans are so dexterous that there's no comparison between robot grippers and our hands. By working through the VR system, the operator is forced to follow the robot's constraints.

"You teach the essence of the skill to the robot by giving demonstrations," said Abbeel. "It doesn't mean that it will be robotically fast at that point. It will do it at human pace, which is slow for most robots. That's the first phase (imitation learning). You teach the robot through demonstrations. Then in phase two, the robot will run reinforcement learning, where it learns from its own trial and error. The beauty here is that the robot has already learned the essence of the task. Now the robot only has to learn how to speed it up. That's something it can learn relatively quickly through reinforcement learning."

Abbeel said their technology is suited particularly for challenging vision and manipulation tasks that are currently too complex for traditional software programming techniques.

Eventually, Embodied Intelligence will let other people use this software to reprogram their robots by doing their own demonstrations. This will allow any company, large or small, to quickly redeploy robots for different tasks.

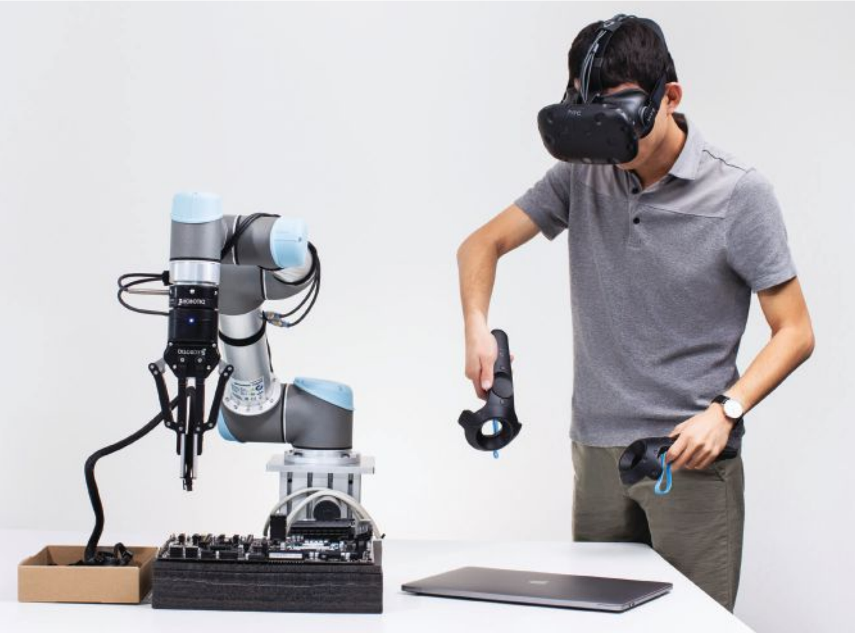


Figure 5: Operator wearing a VR headset and holding motion-tracking devices teleoperates a robot, showing it how to grasp and manipulate objects so it can learn how to perform new skills on its own using reinforcement learning. Courtesy: Embodied Intelligence/RIA

Our collective potential

Cloud robotics, machine learning, computer vision, speech recognition—all the facets of AI are making progress, and at times remarkable strides in specific areas. However, AI still has nothing on humans.

Even if robots, with the help of AI and human engineering, are someday able to approach our dexterity, they may never truly grasp the world around them in all of its fragility and potential. Context and ingenuity will remain in the realm of humans. Technology is neither bad nor good; it's how we use it. With AI and robotics, we humans have tremendous potential for good. **ce**

***Tanya M. Anandan** is contributing editor for the Robotic Industries Association (RIA) and Robotics Online. This article originally appeared on the RIA website. The RIA is a part of the Association for Advancing Automation (A3), a CFE Media content partner. Edited by Chris Vavra, production editor,* Control Engineering, *CFE Media, cvavra@cfemedia.com.*

M More ANSWERS

KEYWORDS: robotics, artificial intelligence

Artificial intelligence (AI) is developing, but it isn't as smart as humans.

Humans can use machine learning to help robots learn new skills with the help of AI.

Cloud robotics can assist collaborative robots; AI requires large quantities of data.

GO ONLINE

Read this article online at www.controleng.com for more information about AI and robotics and related links, including the original article from RIA, "Why AI won't overtake the world, but is worth watching."

CONSIDER THIS

What particular skills could robots be taught that would have a major impact in manufacturing and industrial automation?

Chris Middleton, Vinelake

Five smart warehousing predictions

Warehousing is evolving from being a static component in the supply chain to an area ripe for smart transformation. Five predictions including robotics and predictive maintenance are highlighted.

Customers want goods made to order and delivered as soon as possible in a way that suits their flexible lifestyles. This is a byproduct of the mobile, app-driven, on-demand age. For many organizations and their warehousing and logistics experts, those customer wants can shine a harsh spotlight on legacy business models.

Smart warehousing is making rapid technology advancements the norm, which is forcing those companies to change how they manage their storage and logistics to compete with next-day delivery cycles.

Broad-spectrum automation is happening on the back of advances in industrial robotics. Related technologies, such as drones, are becoming faster and safer around human beings in complex settings such as warehouses.

Internet of Business asked four experts for predictions about how warehousing will develop in 2018 and the five trends that will be the driving force behind these changes.

1. Robotics and cognitive computing

Taking a cue from Amazon, Alibaba, and others, process automation will move center stage—not only via the use of physical robots that replicate manual tasks, but also through robotic software applications and cognitive computing services, such as artificial intelligence (AI) and machine learning.

Thiagu Bala, a senior manager at Deloitte Consulting, said, "In 2018, two technologies will combine: robotic process automation (RPA)—involving small, repeatable software programs or bots—and cognitive computing. This will make a huge difference when it comes to data, by enabling labor to focus on truly mission-critical activities. When RPA is combined with cognitive analysis, it gives programs the ability to act like humans by making business decisions on the fly."

Bala added, "When you combine the transactional processing of purely repeatable tasks with business processes—and also root-based decision-support systems—that's truly a game-changer."

2. Predictive maintenance

A mix of different technologies is impacting the traditional idea of maintenance. Until the advent of the Internet of Things (IoT) and supporting technologies, maintenance had been a passive, reactive process.

Today a mix of technologies, including enterprise asset management, digital twins—exploded 3-D representations of objects and their components such as sensors—radio frequency identification (RFID) tags, smart supply chains, and AI are allowing organizations to gain unprecedented insight into the lifecycle of products, components, and even materials.

Using these and other technologies, objects can not only tell organizations when they need fixing, maintenance, or upgrade, but also predict when they're likely to fail, enabling end-to-end lifecycle management. Warehouses around the world are increasingly adopting proactive maintenance processes so that costly and time-consuming equipment failures are less likely to happen. And the same processes can be used to protect perishable stock.

Eberhard Klotz, the head of the Industrie 4.0 division at Festo, said, "There will be comprehensive condition monitoring, which helps to avoid or reduce downtime and optimizes maintenance procedures and mobile maintenance."

Essentially, the faster an issue can be brought to awareness and analyzed, the faster a repair can be implemented before a minor issue becomes a major problem.

3. Warehousing on-demand

Most people are familiar with how sharing-economy platforms and apps, such as Uber, Airbnb, and

More ANSWERS

KEYWORDS: robotics, warehousing

Technology developments are changing warehouses' role in the supply chain and making them more active overall.

Robotic process automation (RPA) and cognitive computing are expected to combine in warehouse operations to provide smarter information in real-time for manufacturers.

Three-dimensional printing and collaborative robots will provide more flexibility for warehouses in their operations.

GO ONLINE

Read this article at www.controleng.com for links to additional stories about the IIoT.

CONSIDER THIS

What other changes and developments will have a positive effect on smart warehouses?

2018 Global Automation & Manufacturing Summit

HANNOVER MESSE USA

September 12th

Join *Control Engineering*, *Plant Engineering* and Hannover Fairs USA for the Global Automation and Manufacturing Summit, part of the Industrial Automation North America (IANA) pavilion at the 2018 IMTS Show at McCormick Place in Chicago. This one-day summit is designed to bring plant managers, control engineers, and manufacturing business leaders together to highlight plant improvement opportunities and deliver strategies that manufacturing personnel can take back to their plants and implement immediately.

Sponsored by:

BECKHOFF

infor

Stratus

UL

GAMS Agenda

REGISTRATION: 11:30 a.m. to 12 p.m.
LUNCH: 12 p.m. to 12:30 p.m.

KEYNOTE: 12:30 p.m.
Global manufacturing: The race to serve 7 billion potential customers, and how to win the race.
In a global, competitive manufacturing environment, how can American manufacturers compete? The same way they've lifted the U.S. economy out of the Great Recession: By being smarter, leaner (and Leaner) and using technology and data to point the way to a better manufacturing strategy.

SESSION 1: 1 p.m. to 1:45 p.m.
Cybersecurity: How far do we need to go?
The problem of security for (IIoT) is one of the most discussed issues as manufacturers look to deploy this technology solution. We'll look at the real issues, perhaps debunk a few myths, and talk about the common-sense ways manufacturers can secure their data and their operational integrity. The presentation will be led by Dr. Richard Soley, chairman of the Industrial Internet Consortium, Chairman and Chief Executive Officer of OMG (Object Management Group) and executive director of the Cloud Standards Customer Council.

SESSION 2: 2 p.m. to 2:45 p.m.
Embrace your robot: A guide to the future
No longer a science fiction story, robots are real, valuable to manufacturing, and winding up in more plants than ever. How can you find the best way to utilize robots in your plant? Listen to our experts who will discuss the practical ways robots can enhance manufacturing—and all the ways humans are still vital to your operation. The panel will be led by a representative from the Robotics Industries Association (RIA), a CFE Media Partner.

SESSION 3: 3 p.m. to 3:45 p.m.
IIoT in discrete manufacturing: Managing the process
When it comes to IIoT, manufacturers in discrete industries, particularly in the metalforming and CNC industries, have a different set of expectations from those in the process industries—and a different set of challenges. We'll talk with industry experts to look at how to get the most out of IIoT, and how to use data to improve operations, supply chain and safety.

SESSION 4: 4 p.m. to 4:45 p.m.
Maintenance and IIoT: Follow the numbers
The data generated by IIoT can point a maintenance professional to a problem on the plant floor— if he's looking at the right numbers at the right time. More sophisticated analytics are helping maintenance teams focus on the right data at the right time, and we'll talk with them on how this strategy can lead to more uptime and better safety. The presentation will be led by Sal Spada, research director for discrete manufacturing for ARC Advisory Group.

COCKTAIL AND NETWORKING RECEPTION: 5 p.m. to 7 p.m.
After a great day of information, continue the discussion in the lobby. Cocktails, light snacks and conversation about the day's events will follow.

CFE Media®   CONTROL ENGINEERING   PLANT ENGINEERING

Laundrapp, have disrupted centuries-old sectors, such as personal transport, accommodation, and cleaning. What few people realize is the model now is being applied to industrial warehousing.

Startups in the U.S. and the UK have created apps and cloud platforms that transform both the buy and sell sides of the market. They're allowing warehouse owners to lease out spare capacity, and clients to rent it on-demand over timescales ranging from days to months.

The idea might seem simple enough, but the implications could be transformative.

For example, organizations no longer need to think of warehousing in terms of massive regional hubs that require long-distance road haulage. Instead, they can now manage it as a national or international grid of smaller facilities that can be expanded or contracted on demand.

> **In the future, the distinctions between factory floor and warehouse** may begin to disappear once some factories move away from the monolithic, mass-production and distribution cycles.

On the sell side of the equation, organizations no longer need to carry vast amounts of unused capacity that cost money, especially when the economy is unpredictable. With these new on-demand platforms, unused space becomes a commercial asset.

In turn, the model could help regenerate brownfield sites and unused buildings, in the same way Airbnb has pushed people to invest in and renovate private accommodations.

"If you have it on a flexible model, you can just dial down your warehousing in line with your business needs and reduce your liability," said Stowga CEO Charlie Pool. "From our customers' perspective, in good times it allows them to be agile, move quickly, open a new market—or close a new market, which is equally important. They can test it, and if it doesn't work out they can try it somewhere else."

4. 3-D printing and collaborative robots (cobots)

In the future, the distinctions between factory floor and warehouse may begin to disappear once some factories move away from monolithic, mass-production and distribution cycles. For example, some warehouses may become smaller, smarter, and more closely integrated with manufacturing, even as others follow the Alibaba model by becoming larger and more automated.

Technologies such as programmable cobots, which are designed to work alongside human beings, will be increasingly important in these cases, following the smartphone model by becoming programmable platforms for a range of process- or industry-specific apps.

Printing in 3-D will be another ingredient in the mix. Most organizations are familiar with the concept of using this emergent technology for small, specialized projects. However, some Industrie 4.0 analysts believe 3-D printing will become an increasingly important tool on a larger scale.

Andrew Hughes, a principal analyst at LNS Research, sees a prominent role for 3-D printing in rapid fulfillment: "3-D printing brings design, manufacturing, and service flexibility to many industries," he says. "As speed, quality, and materials improve, those that exploit the new possibilities will be the winners. What you make today is a limiting factor for most manufacturers, but we are already seeing manufacturing hubs, where a facility can produce items to order for an enormous variety of customers and deliver in a short timescale."

Hughes added, "Manufacturing really is becoming a critical part of the supply chain and logistics. Print-to-order manufacturing flexibility means having the right printers, materials, and designs ready for any customer order. It brings us back to the fact that Industrie 4.0 is, in fact, all about data."

5. IoT standards and regulations

Today's smart warehouses are increasingly rolling out transformation strategies that deploy sensors connected to the IoT—so robots, workers, managers, and even smart vehicles know the location of every item and can track them on their journeys.

Kristi Montgomery, vice president of innovation at Kenco Innovation Labs, pointed out that no standards yet define how IoT devices should communicate with each other, or store and process information.

She thinks that will change, and soon: "The promise of IoT is disrupting all industries, and it seems like the future is bright. The emergence of IoT is an amazing thing for supply chain executives. And it's especially exciting as the enabling technology is becoming less expensive and more readily available, meaning that large-scale deployments are now possible.

"However, despite all the excitement and possibilities, some real roadblocks remain, namely, IoT technology is like the Wild West: there are no existing standards," she added. "These will define how IoT devices will communicate and how data will be collected, processed, handled, stored, and summarized. Those concerns extend from 2018 into the future, as companies work to establish a regulatory standard, though nothing has emerged yet." **ce**

__Chris Middleton__ is the editor of Internet of Business (IoB), a CFE Media content partner. This article originally appeared on the Internet of Business' website. Edited by Chris Vavra, production editor, CFE Media, cvavra@cfemedia.com.

Mariana Dionisio, Emerson

Seven benefits to using mobile software in an organization

Intuitive mobility automation and engineering software helps organizations attract and retain talent, and drive greater competitive advantages.

Mobile technologies have become pivotal to the way companies operate. Employees—millennials in particular—value mobile tools that help them stay informed and productive. By implementing built-for-purpose mobile automation solutions, organizations can redefine the way plant staff operates, creating a draw for the best and brightest people, while simultaneously delivering improvements to operations and production.

Mobile technology benefits

As responsibilities around the plant increase, personnel have an increasing need for secure, on-demand access to critical information to enhance operational safety, productivity, and efficiency. Mobile technologies are a core component of solving this challenge by providing these seven benefits:

1. Freedom to multitask

Mobile automation tools can provide the same real-time data available from the operator console to mobile phones and tablets without being tethered to the control room or remotely connect to a PC. Any parameter or alarm that has been configured in the distributed control system (DCS) can be delivered to mobile devices easily and securely, giving users confidence they will always have the most up-to-date information about their operations.

To speed up time to success in the field, these mobility solutions provide out-of-the-box filtering and targeted notifications to ensure that critical alerts are only sent to the right people and not buried under a flood of nuisance alarms. Users will only see needed events and not have to sift through irrelevant data.

Secure mobile access to data means freedom and flexibility to move around the plant (or the world) and multitask, allowing staff to more efficiently perform tasks and collaborate across the organization.

2. Stability and safety

Next-generation workers value the ability to collect and have data at their fingertips from anywhere on and off-site. They see mobile software as a means to reduce time-consuming manual operator rounds, which can require physical equipment checks in dangerous or remote locations.

By integrating mobility into automation workflows, these workers are provided with the flexibility they have grown to expect. Secure mobile access to data can increase productivity and safety by reducing or eliminating the need for manual rounds.

3. Deliver a positive user experience

Providing tools to help users increase safety and efficiency can have a significant impact on an organization's ability to attract and retain talent. However, providing mobility plant personnel will appreciate—and more importantly, use—is about more than providing continuous visibility to the DCS. Modern mobility solutions need to be designed for a simple, secure user experience.

Many millennial engineers entering plants have come to expect mobile technology. Mobile devices have likely played a central role in their social lives and previous work experience. These users thrive with mobile devices and applications that are intuitive and are easy to integrate into their workflows.

Plant management should focus on implementing mobile solutions that provide easy, secure access and require minimal configuration.

4. Meeting user expectations

There are many ways to provide mobility, but it is essential to provide secure access that helps users operate more efficiently. Just as today's most successful mobile apps don't require complicated, time-consuming configuration to function, mobile solutions for automation systems must also be ready to work out-of-the-box.

Layered mobile solutions that are complicated to configure and integrate with a DCS or historian are no longer necessary. Organizations should look

M More ANSWERS

KEYWORDS: **Mobile automation software, mobility benefits**

Benefits to mobility software

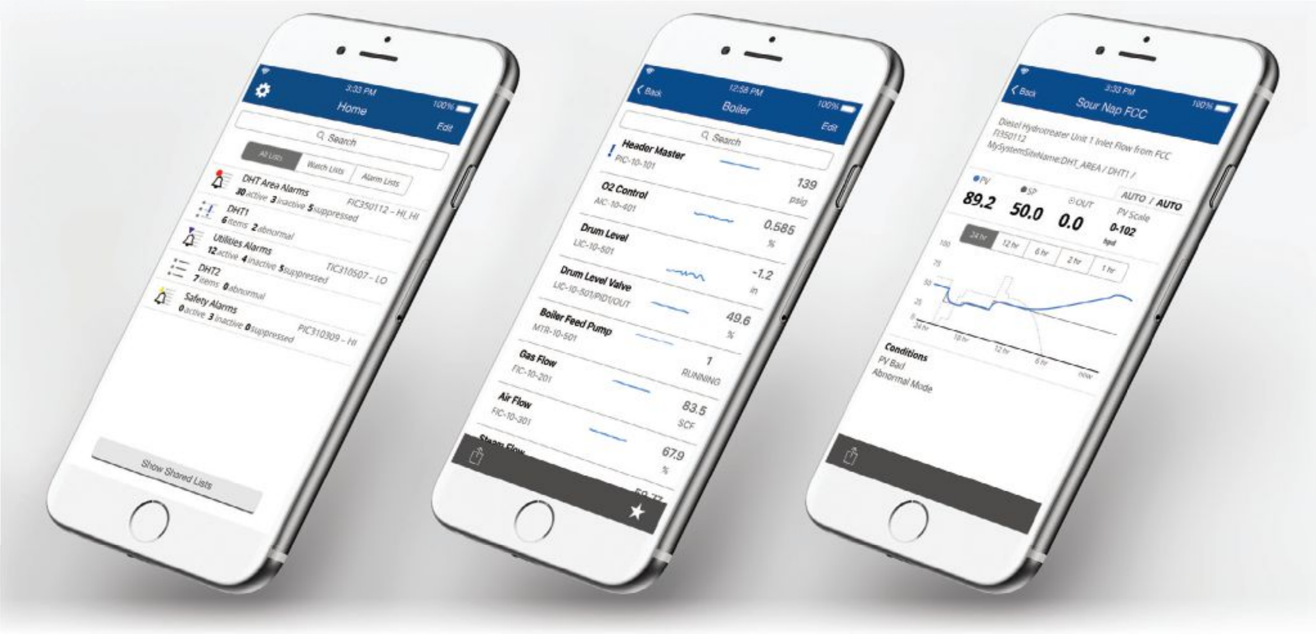
How mobility software can optimize operations.

GO ONLINE

Learn more about mobile technology at www.controleng.com/info-management/mobility.

CONSIDER THIS

Which applications should be mobile but are not?



Designed for Apple iOS and Android, DeltaV Mobile provides users with intuitive, easy, and secure mobile software, with out-of-the-box functionality and native DCS integration. Image courtesy: Emerson

beyond layered solutions and instead provide personnel with modern, secure mobile solutions that are natively integrated with the DCS, designed to operate with Android and Apple iOS devices ensuring no additional DCS configuration is required. Users receive the same real-time information and alarms that are available on the operator console, with relevant process data and rich content that layered solutions cannot readily provide.

5. Secure mobile data access

As mobile technologies have evolved, so too have user expectations of secure mobile access to data.

Mobile software for process automation also can offer integrated security features that are nearly invisible to the user. Designed with read-only access, these applications prevent users from inadvertently affecting operations. In addition, mobile access to process and diagnostic data is typically provided through dedicated secondary servers located above the automation control network, giving the user an extra layer of security.

The best solutions will provide these features out-of-the-box with little to no administrator configuration and no end-user configuration. Leveraging user-friendly technologies simplifies plant workflow is a key role in retaining millennial talent.

6. Improve departmental communications

Organizations that provide fast, easy access to critical data—coupled with the ability to easily share that information across the enterprise—creates a significant competitive advantage. Collaboration tools enable fast dissemination of data across the organization and enable key personnel to stay informed despite their location, which builds a network of subject matter experts that drive efficiency and success.

In many organizations, data is difficult to transfer because it is siloed in individual departments or databases. Collecting data from various sources in the plant or throughout the organization can be a cumbersome process and lead to serious consequences.

Mobility solutions can break down organizational barriers by integrating data from multiple sources into mobile views, delivering new opportunities for faster decision making. They also can be designed for collaboration across the enterprise.

Users can drill down on alerts to view recommended actions and relevant contextual process data, helping workers make faster and better decisions.

7. Workforce support

Employees value organizations that provide them with the tools and technologies they need to perform their jobs as safely and efficiently as possible. Employer investment in tools, guidance, and opportunities helps millennial workers perform and prepares them to be successful throughout their careers.

The millennial workforce has grown up with mobility as an important and inherent aspect of their lives, and they expect similar user experiences with mobile software in the plant: secure and easy access to data, out-of-the-box functionality with minimal configuration, and intuitive user interfaces.

Bringing these mobile solutions into the workplace provides plant personnel with the tools to enhance safety, efficiency, and collaboration to ultimately improve the operations of an organization. The mobile workforce has arrived. The organizations that harness it will gain the competitive advantage for years. **ce**

Mariana Dionisio, *DeltaV product manager at Emerson. Edited by Emily Guenther, associate content manager,* Control Engineering, *CFE Media, eguenther@cfemedia.com.*

Nate Kay and Lindsey Kielmeyer, MartinCSI

How to transition from traditional to digital plant-floor technologies

Improving plant efficiencies starts with bridging the gap between workforce generations. Generation X can help connect traditional industrial applications with digital manufacturing. See three benefits of mobility on the plant floor and implementation advice.

By leveraging Generation X's interpersonal skills, the understanding of processes before and after technological advancements, and the patience acquired during times of transition, manufacturers can use Gen Xers to facilitate mentoring programs between older and younger workers to keep everyone engaged with new technologies—mobile industrial technologies specifically.

Millennials are getting a lot of attention in part because of the gap between them and the aging baby boomer generation. It's understandable, millennials now make up the largest share of the American workforce, and baby boomers are continuing to work well into their 60s and 70s. Gen X is the demographic of people following the baby boomers and precede millennials, and they can help bridge the gap between the two to help improve a plant's overall efficiency by understanding traditional analog technology and adopting mobile technologies.

Gen X wasn't born with technology; technology grew with Gen X. They remember a time before cell phones and desktop computers. They should be the generation that connects traditional analog ways and the digital information age.

For example, imagine the baby boom generation is a plant running traditional analog technologies and the millennials are the mobile computers and connected devices in the age of digital manufacturing. With a lot of conflict and contrast between the two, there's a need for compromise and bridge the arc. Gen X can be the bridge between analog and digital by connecting the plant floor to mobile devices. Going mobile offers many benefits and it can be implemented while keeping cost and security in mind.

Three benefits of going mobile

Going mobile offers many potential advantages. While the individual benefits vary depending on the application and the client's needs, see three common benefits below.

1. Plant-floor mobility saves time.

Most industrial controls systems rely on operator interface screens to monitor and control a system or process. Typically, these interfaces run on a PC or industrial computer installed in a fixed location such as inside a control room or mounted to the front of an industrial enclosure. Having to monitor and control the system from a fixed location can have an adverse impact on productivity and troubleshooting. The user may have to stop what they are doing, walk over to the operator interface, and take readings or make setpoint changes before returning to the production area. While troubleshooting an issue, maintenance personnel often walk back and forth between the operator interface and the system they are working on to compare the physical system with the information displayed on the operator interface.

Mobile technology allows plant personnel to monitor and control the system freely from any location on the plant floor. They can inspect or operate the physical process while viewing the operator interface simultaneously.

2. Remote monitoring and notifications decrease travel.

With remote access, managers can receive alarm notifications and real-time status updates on their

M More ANSWERS

KEYWORDS: Generation X, baby boomers, millennials

How Generation X can help improve efficiencies within a plant

How mobile solutions can optimize plant operations

Implementing a mobile system.

GO ONLINE

Read more online about mobile solutions at www.controleng.com

CONSIDER THIS

How can your plant facility improve efficiencies with mobile solutions?

mobile devices, which assists with troubleshooting, reduced downtime, and help eliminate travel time.

For example, remote monitoring and notifications were set up for an original equipment manufacturer (OEM) client that produces and maintains machines throughout the United States. They received a call that one of their machines, located in a different state, was having an issue. Typically, a technician would have to go onsite to troubleshoot the issue. However, by using mobile alarm notifications, the client determined a programmable logic controller (PLC) battery was low and shipped a new battery.

3. Data collection and sharing identify bottlenecks.

Going mobile also permits data from the plant floor to be collected, analyzed, and merged with data from the business side. Machine data previously invisible or not tracked can now be seen in real-time.

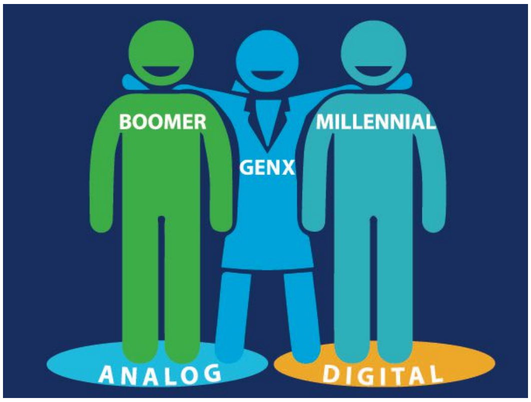
For example, a cloud-based mobile data collection system was designed for an industrial manufacturer. This allowed the company to collect data from machines on the plant floor, store it in a database, and share this data with business managers to bridge the information gap between the plant floor and the office floor.

On the business side, information technology (IT) professionals analyzed the collected data, merged it with available information, and used the combined results to determine the machine was operating at 50% efficiency. Business intelligence software was then used to provide managers with real-time access to these reports. Management, engineering, and IT were working together for the first time to create a strategic plan to improve machine efficiency.

Implementing a mobile system

A common misconception is the customer will have to perform a major or expensive upgrade of existing equipment to go mobile. However, this is often not the case. When it comes to older equipment and non-Ethernet protocols such as serial, Profibus and DeviceNet, a variety of communications gateways can be added to enable mobile communications without having to upgrade existing equipment. While it is often a good idea to upgrade legacy equipment, a pre-configured mobile interface can be added to many legacy systems without having to perform expensive upgrades if cost is a prohibiting factor.

Strong security involves a layered approach and begins with the basic network architecture. One common misconception related to the network architecture is that to facilitate mobile access, the existing controls equipment should be placed on the business/enterprise network or given direct internet access.



Generation X – the bridge between baby boomers and millennials. Courtesy: MartinCSI

In most cases, this is not necessary and would also be inconsistent with best cybersecurity practices. Controls equipment such as PLCs and supervisory control and data acquisition (SCADA) computers often exist on a private network and, in most cases, should remain on a private network.

This does not mean the equipment needs to run in a secured vault without outside access. One method for achieving access is the creation of an industrial demilitarized zone (DMZ). DMZs, used in many IT applications, allow for secure mobile access to industrial control systems (ICSs). DMZs maintain isolation between the private controls network and the public-facing enterprise network. They allow the two networks to communicate through a firewall or another controlled access point.

Instead of merging controls equipment directly onto the enterprise network, or giving the equipment direct internet access, an industrial DMZ can be set up by using devices, such as edge-of-network gateways, proxy computers, and virtual private networks (VPNs) to allow for secure and controlled access with mobile devices. Mobile devices and other public facing devices can then access information about the control system through the DMZ.

Gen X plant floor bridge

Gen X has the skills needed to build that bridge between the divide between the baby boom and millennial generations. By going mobile, manufacturers can attract the millennial workforce and reap the benefits of improved efficiency, increased productivity, and reduced time for troubleshooting and maintenance on the plant floor. **ce**

Nate Kay *is a project manager at Martin CSI and* ***Lindsey Kielmeyer*** *is the marketing coordinator at MartinCSI. Edited by Emily Guenther, associate content manager,* Control Engineering, *CFE Media, eguenther@cfemedia.com.*

Larry Hardesty, MIT News Office

Neural network chip reduces power consumption

MIT researchers have developed a chip designed to reduce neural networks' power consumption by up to 95%, making them practical for battery-powered devices.

Most recent advances in artificial-intelligence systems such as speech- or face-recognition programs have come courtesy of neural networks, densely interconnected meshes of simple information processors that learn to perform tasks by analyzing huge sets of training data.

MIT researchers have developed a special-purpose chip that increases the speed of neural-network computations by three to seven times over its predecessors, while reducing power consumption 94 to 95%. That could make it practical to run neural networks locally on smartphones or even to embed them in household appliances.

Learning efficiency

"The general processor model is that there is a memory in some part of the chip, and there is a processor in another part of the chip, and you move the data back and forth between them when you do these computations," said Avishek Biswas, an MIT graduate student in electrical engineering and computer science, who led the new chip's development. "Since these machine-learning algorithms need so many computations, this transferring back and forth of data is the dominant portion of the energy consumption. But the computation these algorithms do can be simplified to one specific operation, called the dot product. Our approach was, can we implement this dot-product functionality inside the memory so that you don't need to transfer this data back and forth?"

Biswas and his thesis advisor, Anantha Chandrakasan, dean of MIT's School of Engineering and the Vannevar Bush Professor of Electrical Engineering and Computer Science, describe the new chip in a paper that Biswas presented at the International Solid State Circuits Conference in February.

Back to analog

Neural networks typically are arranged into layers. One processing node in one layer of the network generally will receive data from several nodes in the layer below and pass data to several nodes in the layer above. Each connection between nodes has its own "weight," which indicates how large a role the output of one node will play in the computation performed by the next. Training the network is a matter of setting those weights.

A node receiving data from multiple nodes in the layer below will multiply each input by the weight of the corresponding connection and sum the results. That operation—the summation of multiplications—is the definition of a dot product. If the dot product exceeds some threshold value, the node will transmit it to nodes in the next layer, over connections with their own weights.

The neurons' firing rates and the electrochemical signals that cross the synapse correspond to the data values and weights. The MIT researchers' new chip improves efficiency by replicating the brain more faithfully.

In the chip, a node's input values are converted into electrical voltages and then multiplied by the appropriate weights. Only the combined voltages are converted back into a digital representation and stored for further processing.

The chip can thus calculate dot products for multiple nodes in one step, instead of shuttling between a processor and memory for every computation. ce

Larry Hardesty is with the MIT News Office, Massachusetts Institute of Technology; edited by Chris Vavra, production editor, Control Engineering, *CFE Media, cvavra@cfemedia.com.*

M More ANSWERS

KEYWORDS: Energy efficiency, neural network

Research on a chip with faster speed and less energy.

CONSIDER THIS

Where could a 95% power reduction help?

GO ONLINE

Search the headline for more *Control Engineering* energy and power stories.

www.mit.edu

MIT researchers have developed a special-purpose chip that increases the speed of neural-network computations while reducing power consumption up to 95%. Courtesy: Chelsea Turner, MIT

Daniel Repp, Lenze

Integrating the Industrial Internet of Things

Original equipment manufacturers (OEMs) and design engineers wrestle with integrating new technologies with the Industrial Internet of Things (IIoT) to compete in today's evolving and interconnected world.

As corporations push digital transformation efforts to capture higher efficiencies and larger market shares, manufacturers and machine builders face more digitalization demands than ever before. The Industrial Internet of Things (IIoT) can meet those demands by providing companies with enhanced capabilities, increased speed, and more flexible production. However, the challenge original equipment manufacturers (OEMs) and design engineers must overcome is integrating new technologies in a way that allows them to compete in today's evolving and interconnected world.

Transitioning to connected, flexible machines

Automation components or machines that can be rearranged without manual configuration or new programming are one of the foundational elements of a digital transformation. It is also a crucial prerequisite for exploiting the IIoT's benefits. The more flexible the equipment, the more agile the manufacturer.

Incorporating advanced modular components and subsystems can boost reusability and overall equipment efficiency. It also relieves high-value engineers of time-consuming rote programming and maintenance tasks. Embedded connectivity compounds these efficiencies for OEMs and end users alike.

Modularization and standardization of interfaces, dynamic reuse of complete machine modules, and networked connectivity are the first steps toward true "plug and produce" systems where production can be started following a quick reconfiguration performed remotely.

Flexible, decentralized solutions and advanced digital engineering tool chains require project teams with the knowledge to install this kind of production architecture. OEM partnerships between automation solution suppliers and service providers experienced in modular, connected solutions are a key factor to successfully implementing the IIoT.

Turn data into intelligence

One of the biggest challenges OEMs and end users face is what to do with the overwhelming flow of data. Data collected and analyzed in the right way over time is what predictive models are built upon and is what will allow end users the ability to reduce costly unplanned downtime.

While there are many solutions on the market designed to collect data from a machine and send it to the cloud, OEMs are often left with the responsibility of programming an interface to read the technology stream and display information that is useful.

The OEM needs to work with the automation solution supplier to interpret the meaning of this data so the end users can get the meaningful information they need to make intelligent decisions about the machine's operation.

When machine builders work with automation solution suppliers to standardize and streamline data collection, analysis, and reporting no prior knowledge of information technology (IT) or Big Data is required.

Data from a machine is transferred via encrypted channels to high security data centers and is available preconfigured to OEMs. Machine builders specify the desired data points in the required application to carry out remote diagnosis and maintenance, or to begin exploring the possibility of offering predictive services.

The result is a system that enables the end user to operate the machine at top efficiency, giving them an edge over the competition.

It is clear that strong and cooperative partnerships will be an important element of working faster and smarter. **ce**

__Daniel Repp,__ industry manager, automation, Lenze. Edited by Chris Vavra, production editor, Control Engineering, *CFE Media, cvavra@cfemedia.com.*

M More ANSWERS

KEYWORDS: IIoT, Integration

Integrating the Industrial Internet of Things (IIoT) can help companies integrate and provide enhanced capabilities, increased speed, and more flexible production.

OEM partnerships between automation suppliers and service providers are a key factor to successfully implementing the IIoT.

Machine builders that embrace innovations such as flexible machine concepts and leverage data will see their business grow.

GO ONLINE

Read this article online at www.controleng.com for links to additional stories about the IIoT.

CONSIDER THIS

What else would benefit from IIoT integration?

John Clemons, Maverick Technologies

What can the IIoT do?

The Industrial Internet of Things (IIoT) enhances manufacturing operations by improving connectivity, equipment management, monitoring production, and customer relationships. See nine benefits.

In the industrial world, it's called the Industrial Internet of Things (IIoT)—a huge buzzword in manufacturing and the topic seems to be everywhere. Like the Internet of Things (IoT), the IIoT connects devices and people and collects and shares large amounts of data. The IIoT enables more intelligent machines, more autonomous machines, and enables those machines to talk to each other.

Unfortunately, many people haven't heard much else when it comes to the IIoT. Beyond smart devices, and collecting and sharing data, most people haven't heard what the IIoT can do. Nine additional IIoT benefits are highlighted below.

1. Monitor production

With the IIoT connecting smart machines and collecting and sharing large amounts of data, it is now possible to monitor production in real-time. This allows for immediate responses to production upsets, helps eliminate wasted time, and reduce in-process inventory. Planned production can be compared in real-time to actual production; machine and line speeds can be changed in real-time, and in-process inventory adjustments can be made, as well. The IIoT enables production to finish on time and in sync with the in-process and raw materials inventories.

2. Manage equipment remotely

IIoT-enabled machine connections allow equipment to be managed remotely. A worker has the ability to manage or monitor the equipment from anywhere and is not restricted to being right in front of the piece of equipment that needs maintenance. Smart sensors can be used to better understand what's actually happening with the equipment. Protocols can be established to proactively manage the equipment, conserve energy costs, and reduce overall operating costs.

3. Equipment maintenance

Condition-based maintenance alerts can be easily implemented using the IIoT. The IIoT is a key enabler for reliability-centered maintenance and for machine-learning paradigms used to support predictive maintenance. This adds up to increased throughput, reduced downtime, lower maintenance costs, high machine reliability, and a greater return on invested capital in the form of better machine use and output.

4. Item identification and communication

Barcodes are mostly on everything and radio-frequency identification (RFID) is increasingly being used in the place of barcodes because of its greater flexibility. Coupled with GPS, RFID provides enhanced capabilities, but collecting and sharing the data can still be an issue. The IIoT can connect barcode systems and RFID systems and eliminate many inherent communications problems by allowing these systems to collect and share large amounts of data on products, materials, work-in-process, locations, and movements for improved real-time management.

5. Continuous improvement with data analysis

Lean manufacturing and six sigma and other continuous improvement paradigms need a lot of data. This is why the IIoT is so important. The IIoT helps aggregate product data, process data, and other data and helps get it to the right people and the right places for analysis. This is exactly the continuous improvement people need to identify problems, get to the root cause, implement improvements, and confirm those improvements worked.

6. Autonomous material handling

The IIoT can connect to just about anything including material handling equipment such as automated guided vehicles (AGV) and automated storage and retrieval systems (ASRS). The production line can trigger an AGV to pick up

M More ANSWERS

KEYWORD: **Industrial Internet of Things (IIoT)**

How IIoT can improve manufacturing operations

The capabilities of the IIoT in manufacturing operations.

GO ONLINE

See the *Control Engineering* IIoT page at www.controleng.com, upper left.

CONSIDER THIS

How can the IIoT improve your daily operations and customer relationships?

The Industrial Internet of Things (IIoT) offers many benefits to manufacturing operations that enhances and optimizes facility operations by connecting devices, data, and people to increase efficiencies and operate smarter. Image courtesy: Maverick Technologies

products or drop off materials. The AGV can trigger the ASRS to put some products into storage, and the production line can trigger the ASRS to send more raw materials, which in turn triggers an AGV. This can all work autonomously with each unit by communicating with the others in real-time.

7. Improved communication with suppliers

The IIoT enables communications with suppliers by providing operational information to the suppliers for remote process automation and optimization. IIoT-based communications with suppliers can be expanded to include production throughput, inventory levels, work-in-process and material levels, all to support just-in-time inventory delivery, vendor-managed inventory programs, and better management of inventory and materials.

8. Improved customer relationships

When it comes to customers, the IIoT can provide cross-channel visibility into finished goods inventory levels. This allows reduced inventory levels, reduced transportation costs, reduced warehousing and distribution costs, and better customer service. It helps manufacturing and distribution operations get the right products to the right places at the right times, which helps keep customers happy.

9. Enhanced management decisions

In a highly competitive environment, the management team must have real-time information to make decisions that can have a significant impact on a company's costs and profits. The IIoT enables management getting the right information to see what's happening on the manufacturing floor so they can make the decisions necessary to better manage overall operational costs and improve company profits.

The IIoT can do a lot more than most people have considered. It connects devices and people, collects and shares large amounts of data, and enables and integrates more intelligent and autonomous machines. IIoT is a great tool and can enable manufacturers to improve a wide range of operations. Pick an opportunity and go. **ce**

John Clemons *is the director of manufacturing IT at Maverick Technologies. Edited by Emily Guenther, associate content manager,* Control Engineering, *CFE Media, eguenther@cfemedia.com.*

Integrating IIoT technologies to maximize facility operations

Gain valuable data insights by integrating operations, information technology (IT) systems, and creating a more effective Industrial Internet of Things (IIoT) solution.

Control Engineering (CE) asked Michael Risse, vice president of Seeq, for advice on how controls, automation, and instrumentation help with integration using Industrial Internet of Things (IIoT) technologies. Integrating operations and information technology (IT) systems can be made easier with the following considerations.

CE: When those in automation and operations consider integrating IIoT concepts, what technologies are they most often talking about? Also, what technologies should be considered but may be overlooked?

Risse: The basic components and systems of the IIoT have been a fact of life in industrial automation and operations for decades: sensor, data collection, application, storage, and analytics. What's needed are insights to improve outcomes in terms of quality, yield, margins, safety, etc.

Most of the promises of digitization transformation, IoT, etc., are about bringing that opportunity for insight to things that didn't have it (connected cars, smart refrigerators, brilliant parking lots, etc.) to solve the same types of problems seen in industrial plants and facilities by providing predictive analytics, operational insight, and visibility to things not in front of them via remote access. The next step is to extend the visible range of results to partners, upstream (supply chain) and downstream (customer use)—and across organizations (x-plants).

The IIoT is not the same old stuff in industrial applications because there are very significant innovations driving opportunities and lower cost such as:

- **Cloud:** connectivity, data collection, sharing, simplicity
- **Sensors:** more, cheaper, wireless, edge processing, OPC unified architecture (UA) and message queuing telemetry transport (MQQT) protocol support
- **Analytics:** More data can now be used to provide much more insight by implementing new approaches. Software platforms makes this possible by using technologies such as Big Data, machine learning, open source, etc.
- **Business models:** remote monitoring of assets by vendors, selling thrust versus engines, distributing risks.

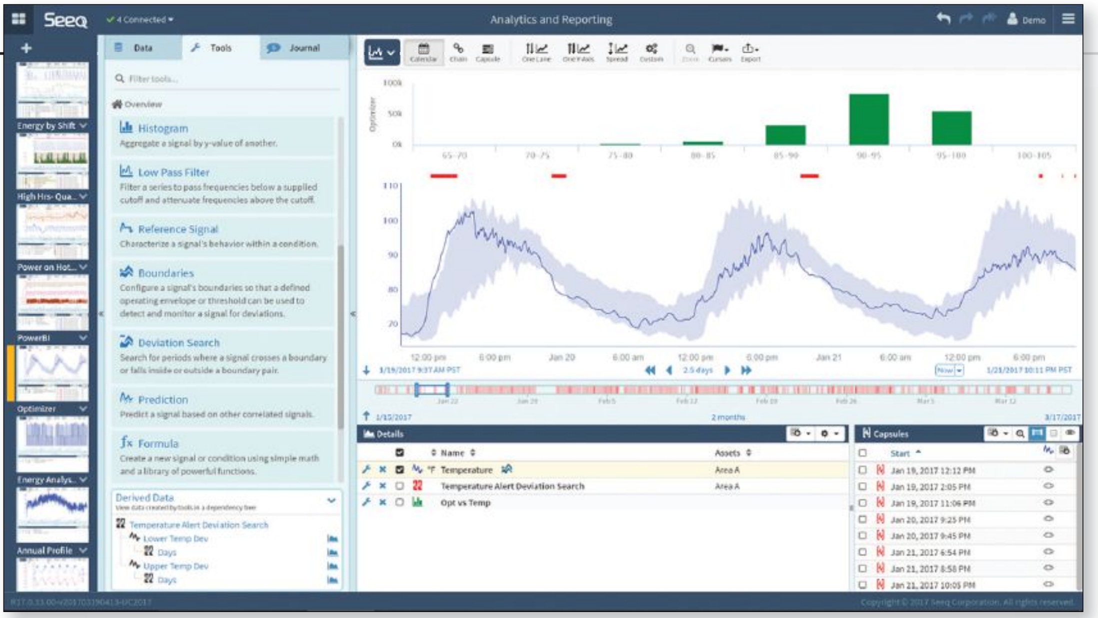
CE: How can controls, automation, and instrumentation help with integration and use of IIoT technologies?

Risse: Stick to a business case, start small and create value. Just don't overthink this as top down—IIoT projects often take too long and cost too much. Try to find a greenfield in a brownfield scenario—something new in something existing (use case should depend on what matters most—ingredient quality, energy use, emission compliance, etc.) For example:

- **Skunkworks:** Raspberry Pi to track sensor data on wireless to inform/contextualize a sensor.
- **Midsize:** cloud IIoT platform for disconnected data sets (remote assets) that expand visible range for operators, or optimization context for engineers.
- **High level:** remote monitoring center to centralize operations.

CE: What value is being created and how, with integration of operations and information technology (IT) systems?

Risse: Value doesn't have to be in dollars. It could be safety or any other priority for the organization such as regulatory compliance. The value is in the time to insight to improvement. Or, to put it another way: sooner means value, and the insight means value, and the sooner the insight



Histogram
Aggregate a signal by y-value of another.

Low Pass Filter
Filter a series to pass frequencies below a supplied cutoff and attenuate frequencies above the cutoff.

Reference Signal
Characterize a signal's behavior within a condition.

Boundaries
Configure a signal's boundaries so that a defined operating envelope or threshold can be used to detect and monitor a signal for deviations.

Deviation Search
Search for periods where a signal crosses a boundary or falls inside or outside a boundary pair.

Prediction
Predict a signal based on other correlated signals.

Formula
Create a new signal or condition using simple math and a library of powerful functions.

Derived Data
View data created by tools in a dependency tree
- Temperature Alert Deviation Search
  - Lower Temp Dev
    - Days
  - Upper Temp Dev
    - Days

Details

☑	Name	Assets
☑	°F Temperature	Area A
□	Temperature Alert Deviation Search	Area A
□	Opt vs Temp	

Capsules

□	Start
□	Jan 19, 2017 12:12 PM
□	Jan 19, 2017 2:05 PM
□	Jan 19, 2017 11:06 PM
□	Jan 20, 2017 9:25 PM
□	Jan 20, 2017 9:45 PM
□	Jan 21, 2017 6:54 PM
□	Jan 21, 2017 8:58 PM
□	Jan 21, 2017 10:05 PM

Providing subject matter experts with visual representations of data allows them to interact directly to solve problems, without the need for assistance from data scientists and IT personnel. Image courtesy: Seeq Corp.

is the square of value (or multiplier) because it's sooner (like area under the curve). How it's created is insight.

Many vendors love to talk about sensors, wireless, and other technologies, but the point of all this is improved outcomes through quicker insights and delivering the profit impact of doing something better, sooner. Also, the value could be the same insight an organization has been wanting to achieve for years. Now it's profitable to do so because the cost of achieving the insight went down (cheaper data storage, collection, new analytics, faster insights). The IIoT is a point in progression in terms of lower costs for most of the components in these types of systems.

CE: How can data analytics help make sense of existing data and the additional information created when previously disparate systems are connected?

Risse: Data analytics is a huge help because one of the keys for successful IIoT implementations is tapping the innovation in analytics technologies so subject matter experts (SMEs) can find insights faster. This allows them to answer the questions they have wanted to analyze but were just too hard/too long to do with traditional tools such as spreadsheets.

So for existing data, there is untapped potential in data already collected no matter where it resides. Data analytics can enable a bridge across data silos to simplify contextualization by putting data in its frame of reference. Previously this was done mostly by hand, mostly by an SME in Microsoft Excel or as part of a massive information technology (IT) project. Now this can be done by any SME. With new data sources, this will become even more of an issue. Perhaps an answer is data lakes or data roll ups for multi-plant scenarios, but data collected in one place without analytics is just a bigger headache than when it's spread out.

CE: What other advice or tips would you offer on IIoT integration relevant for *Control Engineering* subscribers?

Risse: Beware of all systems requiring new data storage. Typically, it's not the data that needs help; it's the analysis of the data to produce insights. Starting small and soon should not require undertaking some Big Data transformation/cloud movement effort.

There has to be a midpoint between hopelessly global (IT top down takes forever) and mindlessly local (plant-by-plant skunkworks with disconnected and nonstandard tools or approaches). This midpoint can be implemented by getting started now on existing problems. Even if one tosses out a local project due to lack of success, it can inform what you need to know and how you can make better decisions, and at very quickly and with low implementation costs. If there are no local initiatives, competitors will outperform laggards; so it's best to get started sooner rather than later. ce

Michael Risse is vice president at Seeq Corp. Edited by Emily Guenther, associate content manager, Control Engineering, *CFE Media, eguenther@cfemedia.com.*

More ANSWERS

KEYWORDS: **Industrial Internet of Things (IIoT), Big Data**

Exploring IIoT integration best practices

How to use data analytics for a successful IIoT integration

The value behind integrating systems and operations.

GO ONLINE

See the *Control Engineering* IIoT page, upper left, at www.controleng.com.

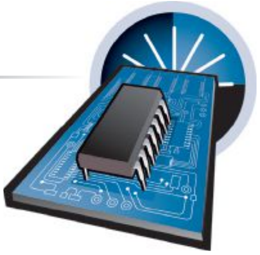
MORE TO CONSIDER

How will integrating IIoT technologies help maximize efficiency, safety, and operations?

ANSWERS

INSIDE MACHINES AND EMBEDDED SYSTEMS

Mark T. Hoske, *Control Engineering*



What is an embedded system?

The meaning of an embedded system varies depending on the application; system integrators, end users, and original equipment manufacturers (OEMs) may have different views.

An "embedded system" is an engineering-related term that can vary in meaning by application, who's using the term, and in what context. Examples of embedded systems are described below. At any of these levels, an embedded system is likely to contain elements of hardware, software, and communications, integrated cybersecurity, and may include one or more control loops (sense-decide-actuate). Embedded systems often run in closed-loop (automated) or in open-loop mode (with human approval or acknowledgement at one or more step).

Embedded systems also can link to or communicate with local or cloud-based connected components, devices, systems, and networks.

Embedded system examples

Value chain or supply chain: Most broadly, embedded systems can operate in and connect various plants and sources within a supply chain (or value chain, as some say), as connected systems of software.

Plant or facility: At the plant level, various departments can have embedded systems. Traditionally, engineering design and procurement may have been in separate silos; interconnection and integration of such systems are increasing.

Plant floor: Maintenance, controls and automation, logistics, engineering systems each are embedded on the plant floor, along with the computers, databases, and communications for each. Power systems also may be considered embedded.

Automation and controls: Embedded systems within automation and controls includes various control systems and controls, across the plant, in the building, fire and life safety, lighting, HVAC, air handling, power, and other systems. These can be discrete control (things) process control (continuous flow), batch control (in tanks or vats), or hybrid control.

Cell level: Within and between various work cells, individual machines and connecting motion controls each can be called embedded systems. In process settings, embedded systems may be considered the controls for the cracker, the fermenter, reactor, etc.

Machine level: Within a machine, an embedded system could operate as stand-alone controller, such as an industrial PC, programmable automation controller, or programmable logic controller outside the machine.

Device level: Within a device, an embedded system can be the board or the silicon chip providing the logic, the network, power, or sensors when each may have their own logic, software, and communications.

Board level: Board-level systems can include sensors, logic elements, and actuators, along with communications. (Unless otherwise specified, most embedded systems, for control engineering, are usually at this level.)

Chip level: Once only logic devices, micromechanical systems have brought the embedded systems discussion to the silicon level. Logic is involved with many processors now operating on one chip, and communication systems are involved. Chips also can have gears, actuators, valves, and embedded microsystems. Within embedded memory and instructions, logic can be permanent.

A related semantic challenge: Is the term system integration (singular) or systems integration (plural)? Are we integrating devices within a system or multiple systems in a connected system of embedded systems? Again, it depends.

Going from bottom to top, one can envision how a chip-level embedded system could be part of a board-level embedded system, which could be part of a device level system (in a controller or smart valve), and on up the line. System integration and interoperability gain importance with the need to exchange data for analysis and smarter decisions from embedded system to embedded system among peers or up the line. **ce**

***Mark T. Hoske** is content manager,* Control Engineering, *CFE Media, mhoske@cfemedia.com.*

M More ANSWERS

KEYWORDS: Embedded systems, system integrator

Embedded systems exist on many levels.

Board-level systems often are embedded systems for control engineers.

GO ONLINE

If reading from the digital edition, click on the headline for more resources. *Control Engineering* has an embedded systems page under Control Systems menu at www.controleng.com.

CONSIDER THIS

Do engineers you work with define their terms?

EPSITRON®
INPUT
OUTPUT
WAGO
787-1012
ADJ.
OUTPUT 24V DC / 2.5A
Adjust
DC OK
787-712
Overload
INPUT
110-240V AC / 1.32A / 50-60Hz
787-1675
787-850
24.0
9.75

Tanya M. Anandan, RIA

Building the future with robotic additive manufacturing

Additive manufacturing (AM) is changing how engineers and part designers think and robots are enabling the technology by making AM machines and processing faster and more accurate.

Additive manufacturing (AM) is not only transforming the way we make things; it's changing how engineers and part designers think. They have to forget limitations imposed by conventional manufacturing methods and open their eyes to new design possibilities. These possibilities are expected to catapult the AM industry to $17 billion by 2020. There are several types of AM processes, including selective laser sintering (SLS), stereolithography (SLA), and fused deposition modeling (FDM).

All are digital manufacturing methods where computer-aided design (CAD) data is used to fabricate a 3-D object by adding layer upon layer of material, whether it's liquid, powder or sheet, or some other type of material. Even human tissue can be used. AM is used to create myriad structures, from dental appliances, to advanced aircraft components, an entire bridge, and even works of art.

Robots help make it possible. Robots are not only enabling additive manufacturing, they're tending 3-D printing machines (which are also robotic), automating AM post-processing, and allowing architects to envision new ways to build.

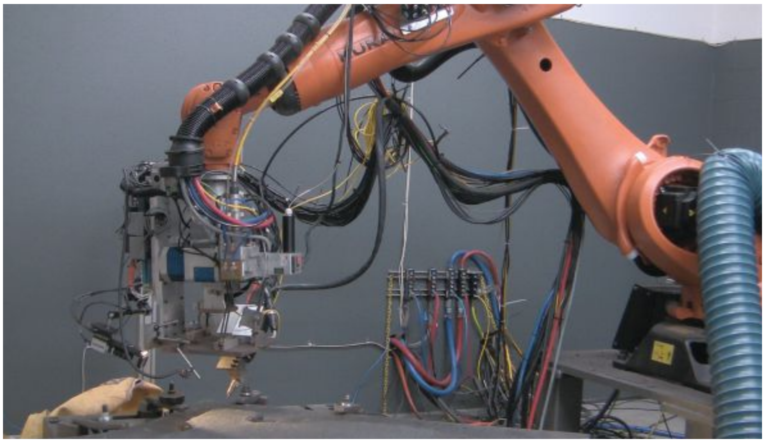


Figure 1: Additive manufacturing process uses a robot equipped with a laser head and hot wire deposition to build a metal part layer by layer. Courtesy: Midwest Engineered Systems Inc./RIA

Layer by layer

At Midwest Engineered Systems Inc. (MWES) in Waukesha, Wis., they are using laser AM to create complicated metal parts that would otherwise be extremely difficult, if not impossible, to manufacture. A six-axis articulated robot drives the process, combining hot wire deposition and a laser to build metal parts layer by layer on an existing substrate. Exotic metals are deposited with precision and speed to build prototypes and small batches of high-value complex parts.

MWES, with 25-plus years of expertise in complex systems integration, developed this process, which was unveiled at the International Manufacturing Technology Show 2016. In a show floor demo, a propeller took shape during the layer-by-layer process.

MWES named their system ADDere, which was derived from the Latin word meaning to add. The process is similar to wire and laser additive manufacturing (WLAM), where a metal wire is fed into a melt pool generated by the laser beam on the substrate. The wire and substrate consequently form a metallurgical bond. The difference is that MWES uses a hot wire process.

"We heat the wire to the point that it's molten at the tip," said Scott Woida, president and founder of MWES. "Since the wire is already molten, we then use the right amount of laser power to melt the substrate underneath to form a strong bond. You're able to use less laser power when you're not trying to melt the wire as well as the substrate. The hot wire allows you to get higher deposition and put less heat into the part."

The process always starts with a substrate. In the show floor demo with the propeller, it was a cylinder.

| PC1148USA |

Meet the smallest Industrial PC from Beckhoff.

The ultra-compact C6015 IPC for automation and IoT.

www.beckhoff.us/C6015

With the ultra-compact C6015 Industrial PC, Beckhoff has again expanded the application possibilities of PC-based control. Wherever space or cost limitations previously prevented the use of a PC-based control solution, this new IPC generation offers an excellent price-to-performance ratio in an extremely compact housing. With up to 4 CPU cores, low weight and unprecedented installation flexibility, the C6015 is universally applicable in automation, visualization and communication tasks. It is also ideal for use as an IoT gateway.

- Processor: Intel® Atom™, 1, 2 or 4 cores
- Interfaces: 2 Ethernet, 1 DisplayPort, 2 USB
- Main memory: up to 4 GB DDR3L RAM
- Housing: Die-cast aluminum-zinc alloy
- Dimensions (W x H x D): 82 x 82 x 40 mm

input #18 at www.controleng.com/information

Flexible installation via rear or side panel mounting, or on DIN rail.

GOLDEN MOUSETRAP AWARDS 2018 WINNER

CONTROL ENGINEERING 2018 ENGINEERS' CHOICE AWARDS HONORABLE MENTION

New Automation Technology **BECKHOFF**

"We can either use the substrate as part of the final part, or we can cut the substrate away and just have the part made of weld bead," said Woida. "But we have to start with something. It can be as simple as an eighth of an inch thick piece of steel."

Wire and laser, plus robot

The primary elements of the system include a high-precision industrial robot, the laser system, an integrated MIG wire and laser head, and the MWES controls system. The process includes active head control and dynamic deposition measuring to closely monitor the process before, during, and after the build.

CAD data is imported into CAD/CAM software, where it is prepared for the additive process. The part is then "sliced" into layers and the robot path is generated offline. Process information can be added automatically or manipulated manually. The generated path and process information is translated through a post processor and automatically transferred to the robot controller. Then the robot executes the program and builds the part layer by layer. Applications include:

- Prototypes
- Small batch production runs
- Replacement parts
- Rebuilt surfaces
- Cladding.

The ADDere system uses a six-axis long-reach robot, which provides for path flexibility and a large working envelope. It's merged with a multi-axis part positioner. Woida said 2 x 8 x 40 m working ranges are possible.

Achievable tolerances are +/- 0.5 to +/- 1.5 mm, depending on deposition rate. Post-processing usually requires some machining. The additive process creates a hardened form of the material, so soft metal also requires annealing.

Freeform fabrication leads to less waste

System advantages include rapid development of new metal parts, quick design changes without adding tooling costs, and low initial cost to production. Woida said one of the main advantages is the ability to take multiple part subassemblies and combine them as one unit.

As an example, GE Aviation took this concept to a whole new level with the AM process for its Advanced Turboprop engine. GE designers were able to reduce 855 parts down to just 12. More than a third of the engine is 3-D printed.

With MWES' ADDere system, solid freeform fabrication allows the use of different metals on different areas of the part to create engineered characteristics specific to an application. This is particularly cost-effective when you want to clad a less expensive metal with a more exotic metal for particular properties like high wear resistance. The process also can be used for repairs by first machining a part to a stable structure and then building up the part to its original state.

"We're getting properties similar to casting, closer to forged," Woida said. "Compared to subtractive methods, you waste less base material because you're building to near net shape."

Wire AM also results in less waste than powder-based AM processes. Woida said they achieve 99% utilization.

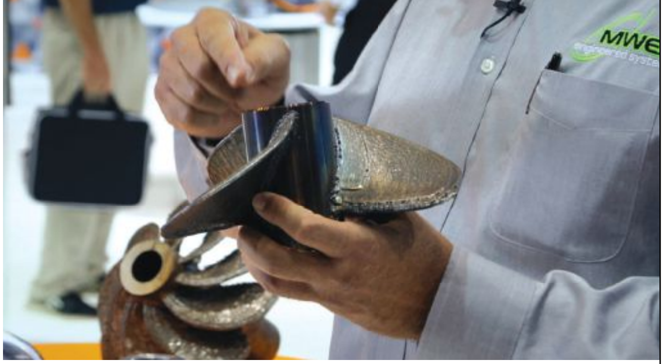


Figure 2: Propeller blades built with a robotic laser additive manufacturing process shown near net shape before finishing. Courtesy: Midwest Engineered Systems Inc./RIA

"When we're running the wire for manufacturing our component, all that wire ends up getting used to make that part," he said. "There is very little waste of the wire (as opposed to powdered metal AM processes where the excess powder falls by the wayside and needs to be recycled). The only thing that happens is that you're machining the outside of that component to get from your near net shape to your net shape. Typically you only machine your mating surfaces. You don't have to machine the whole part."

For the propeller in the demo cell, Woida said you may only need to machine about 5% of that part after the AM process. He said it's also 10 times the speed of powder-based AM processes.

"We can put down 32 lb per hour of stainless steel right now, and that's with a 14 kW laser. Soon we'll have a 20 kW laser. When the material has a high dollar value and it's really hard to machine, this process makes sense," he said.

Not suited for this process are small components, parts that have low manufacturing costs, and parts that require little machining from billet.

"When the part is done, it has a casting-like quality to it," said Woida. "You can either machine the part or we can use a laser to smooth out the outside for a better surface finish. But a lot of our customers are less interested in surface finish as much as they are functionality."

High-value parts, exotic metals

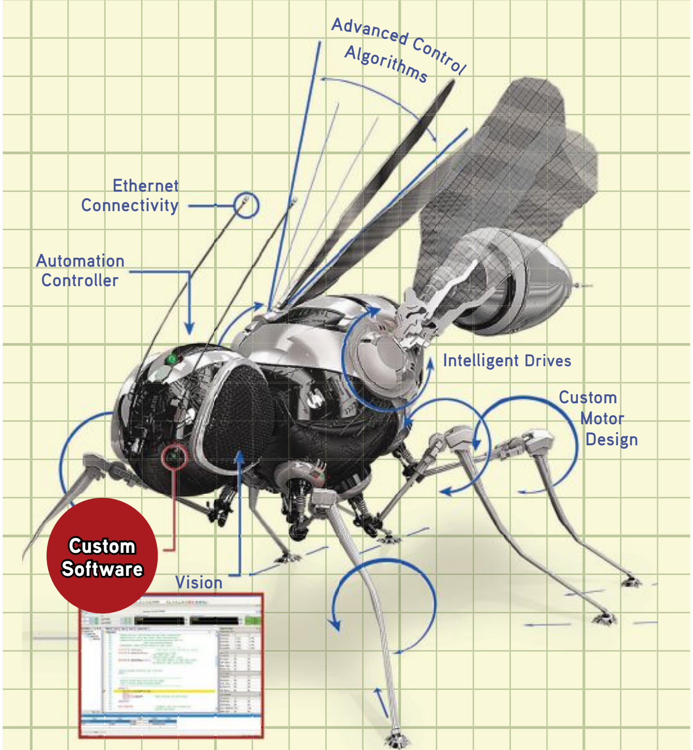
The ADDere system is available as a turnkey product for purchase or as a manufacturing service.

"The parts we are working on to date are basically validation for customers that we can make the components to their specifications," said Woida. "Mass production hasn't started, but we are providing sample sets to customers to verify the capability of the system. They are evaluating them for quality and then they will be buying them in larger quantities from us, or buying the system."

One of those parts undergoing testing in MWES' R&D system is an 1,800-lb bulkhead for an aircraft carrier. Rather than having to waste valuable space with spare parts inventory aboard the ship, imagine being able to use AM to create or repair parts, on demand, while at sea.

The ADDere AM system has application for aerospace, drive train, suspension, naval, military, oil and gas, construction, mining, and agricultural equipment. Materials best suited for these applications are typically exotic metals, such as stainless steel, aluminum, titanium, cobalt, Inconel, and tungsten alloys.

Woida said their experience in laser welding is paying off. "We typically get involved in highly engineered systems, so we



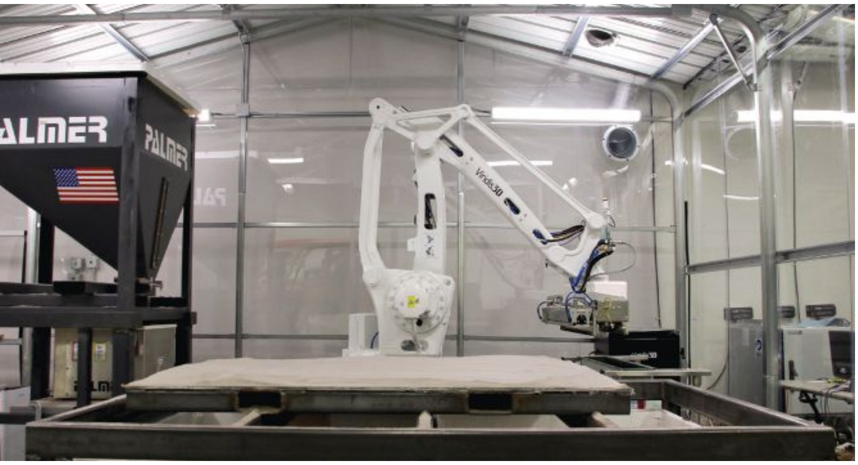


Figure 3: Robotic additive manufacturing system uses a proprietary 3-D printing process to produce sand molds and cores for the metal casting industry. Courtesy: Viridis3D/RIA

have a lot of exposure to the latest technologies, whether it's the latest laser technology or robotic technology," he said. "On a daily basis, we design systems that don't exist in a catalog, that are highly engineered. You need a lot of diverse experience. You need mechanical engineers because these systems are fairly complex. You need software people to make this easy and viable to sell on the open market. You need robotic engineers to then integrate all that. You need weld engineers that can verify and make sure the metallurgical properties are what they're supposed to be. You need a whole lot of people to bring this together."

Metal casting

AM and robotic automation also are ushering in a new digital world for the metal casting industry. 3-D printing was born in the 1990's at the Massachusetts Institute of Technology with student Jim Bredt, who was working on his doctoral thesis investigating the creation of inkjet on powder technology.

The term 3-D printing originally was used to describe how intermittent layers of powdered materials and liquid binder are dispensed in a programmed pattern to form a 3-D object. Bredt said the term was coined by his thesis advisor, and eventually adopted by industry at large. Now, 3-D printing often is used interchangeably with AM and encompasses many different types of processes.

Bredt, research and development director at Viridis3D in Woburn, Mass., has nearly 30 years in the 3-D printing industry, but he never lost sight of his first love. Bredt helped start Z Corp. in 1995 after graduating from MIT. Z Corp. is credited for the first commercial introduction of inkjet-based 3-D printing technology. Z Corp. was then acquired by 3-D Systems, whose cofounders invented stereolithography.

Bredt left 3-D Systems to launch Viridis3D in 2010, where he was eager to get back to metal casting. The goal was to build a 3-D printing machine that was more versatile in the types of materials it could process and more hardened industrially to handle the rigors of working in a foundry. The Viridis3D team focused its sights on the sand casting industry.

"A lot of the components that you really need a 3-D printer for are things you can't make by conventional processes, like cores especially, which can be very intricate," said Bredt. "It increases the capabilities of your process in such a way that you can take more risks in your design. You don't have to spend all that on tooling. If you 3-D print a part and it's a failure because the design is too fragile, then you didn't really lose that much. By being able to take more risks in your design, it expands the gamut of geometric shapes that you can create with the technology."

Breaking the mold

Among reimagining ways of making things, Bredt questioned how 3-D printing machines were designed. "A 3-D printer is basically a robot with a material dispenser attached to it," Bredt said. "When we created Viridis3D, I asked why should I try to build my own robot. My background is in materials, not in machine design. Why don't I just buy a robot? Then I can focus on material dispensing."

For Viridis3D, using an off-the-shelf industrial robot in its 3-D printing system was a major break from the competition.

"Our use of a commercial robot is an interesting distinction," Bredt said. "Our competitors by and large use gantry systems to lug their much heavier printing engine around. By using an arm instead of a gantry system, our print head is designed to be light, rugged, and reliable."

3-D printing with robots

While development was underway on its robotic AM system, Viridis3D partnered with EnvisionTEC, a provider of 3-D printing solutions. Now a wholly owned subsidiary, Viridis3D can continue to fund further development. Earlier this year, Viridis3D commercialized the first robotic 3-D printer, the RAM 123.

The system uses a standard four-axis robot to create sand molds and cores for casting metal parts. The robot is equipped with a powdered material feeder that distributes the sand and a print head that dispenses the liquid binder into the sand. Spreading sand and dispensing binder intermittently, the robotic 3-D printer builds the mold layer by layer.

The print head can be heavy, especially when loaded with sand. Bredt said a four-axis robot, rather than a six-axis robot, is preferred because it has a larger load capacity.

"These printing elements really only work if they are held horizontally," he said. "The print head travels in a plane and very gradually rises up. Four-axis is ideal because they are constrained to always travel in a plane, at least the wrist. It has a high-load capacity and stays accurate."

Viridis3D's RAM system has an open architecture. The molds are built on a stationary table. The tabletop is a pallet that can be used to move parts on and off the machine with a forklift.

"Ours is an open table, so you can build parts of different sizes without having to fill the entire box with materials," Bredt said. "One of the reasons we went to a stationary table is that it was clear to me during the later years at Z Corp., when we were building larger and larger machines, that pretty soon the substrate would weigh more than the machine."

Short lead times, space savings

"Pattern-making is a dying art," said Bredt. "Companies with these 50-year-old patterns send in a guy with a can of Bondo to try and fix it. In some cases, all they have is drawings or maybe they have to reverse engineer existing product. People that buy our system really like the option of switching over to digital manufacturing because you get rid of the overhead for storing those patterns. This is a perfect example of disruptive technology taking over old technology."

Bredt said they are widening their sights on other materials beyond sand that offer higher resolution, including plastic powders, ceramics, and even powdered metals. Robots will continue to shoulder the load. Together, AM and robotics will transform the way we think about manufacturing. **ce**

Tanya M. Anandan *is contributing editor for the Robotic Industries Association (RIA) and Robotics Online. This article originally appeared on the RIA website. The RIA is a part of the Association for Advancing Automation (A3), a CFE Media content partner. Edited by Chris Vavra, production editor,* Control Engineering, *CFE Media, cvavra@cfemedia.com.*

More ANSWERS

KEYWORDS: robotics, additive manufacturing

Additive manufacturing is transforming the way things are made and has opened up new design possibilities for engineers and part designers.

Robots help additive manufacturing become more precise and efficient and allow it to perform more sensitive tasks.

Additive manufacturing and robotic automation are changing the metal casting industry by making it more digital and precise.

GO ONLINE

Read this story online at www.controleng.com for more information about robotics and additive manufacturing, including a story from June 2016.

CONSIDER THIS

In what other industries could robotics and additive manufacturing be useful?

ADVERTISEMENT

White Paper Connection

Preserving Brands and Accelerating Growth:

Battery Ventures' Industrial Technology "Buy-and-Build" Strategy

Jesse Feldman and **Zack Smotherman**

Battery's industrial technology team uses fundamental research to identify promising markets, then strives to create industry-leading businesses through a combination of organic growth and acquisitions.

We target industrial technology companies that 1) offer value to customers through highly engineered products and services, and 2) generate financial and operational metrics that are significantly superior to those of diversified industrial companies, and are more akin to those of high technology companies. Battery has acquired more than 40 industrial technology businesses and brands over the last decade, including in areas including test-and-measurement, sensor technology and analytical instrumentation.

BRAND
BV
Battery Ventures
TALENT
TECH

Preserving Brands & Accelerating Growth

Battery Ventures' Industrial Technology "Buy-and-Build" Strategy

BV

Battery Ventures

One of the key elements of our investment approach is preserving the brand and legacy of the businesses we acquire. A company's brand is obviously the product of years of investment decisions, hiring choices and internal development projects. We know it's impossible to sustain a leading brand without continued investment in technological leadership and talented personnel—so when we get involved in a company, we acknowledge those investments and work hard to leverage them, instead of discarding them.

Preserving brand is a key issue for us because many of our deals involve creating platform companies through roll-up acquisitions. In fact, Battery's industrial-technology team has created six different platforms over the last decade in which we have implemented our multi-brand, M&A strategy and leveraged acquisitions across a larger group.

Battery recognizes that pursuing a multi-brand, buy-and-build strategy is a complicated process that requires careful planning and execution to maximize value for all parties. As our track record demonstrates, we believe in the value of quality brands with leading products and talented managers. The bottom line: We work hard alongside our portfolio companies to preserve what we invest in, accelerate growth, and strengthen the future legacy our businesses.

Register to download the paper at:
http://www.controleng.com/batteryventures-wp

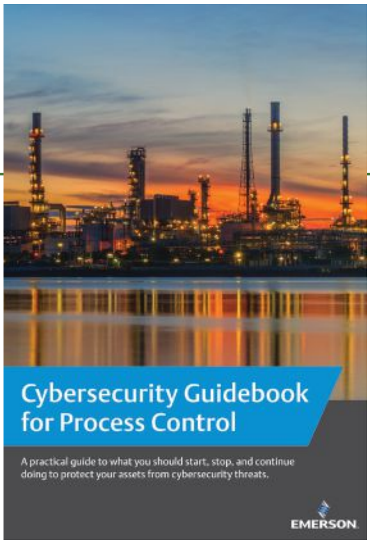
BV
Battery Ventures

industrialtech@battery.com
1-617-948-3600
www.battery.com/private-equity

ADVERTISEMENT

White Paper Connection

Cybersecurity Guidebook for Process Control



Cybersecurity Guidebook for Process Control

A practical guide to what you should start, stop, and continue doing to protect your assets from cybersecurity threats.

EMERSON

Emerson has put together a comprehensive **Cybersecurity Guidebook for Process Control** aimed at providing practical solutions to help you assess and reduce your organization's risk level.

Adopt a Risk-based Approach to Cybersecurity

A risk-based approach to cybersecurity can help you make strategic decisions based on the likelihood and impact of each vulnerability.

Tighten System Access

Building a culture of security by creating and enforcing security best practices will help your employees realize they are a crucial part of keeping your operations safe and secure.

Establish Strong Policies

Strong administrative policies can protect your control system from unauthorized physical access or compromised media devices.

Upgrade to a More Secure Control System

Most cybersecurity threats are avoidable and many options are available to eliminate most risks.

Go Beyond Perimeter Protection

Hackers count on organizations forgetting the backdoors they've left open. Using the tools at your disposal, you can shut those doors and lock them tight.

Keep Remote Access in the Right Hands

Knowing exactly when and how devices connect to your control system will put you in control.

Know Your Control System

After a breach, you need to react quickly and efficiently and comprehensive system monitoring, helps you do so sooner.

Download the guidebook here:
www3.emersonprocess.com/deltav/cybersecurity

EMERSON™

www.emerson.com

input #23 at www.controleng.com/information

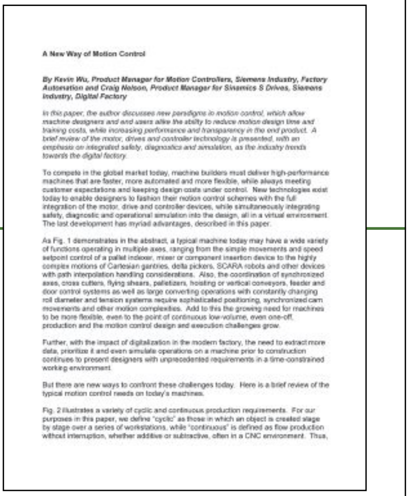
ADVERTISEMENT

White Paper Connection

A New Way of Motion Control

Kevin Wu | *Product Manager for Motion Controllers, Siemens Industry, Factory Automation*

Craig Nelson | *Product Manager for Sinamics S Drives, Siemens Industry, Digital Factory*



A New Way of Motion Control

By Kevin Wu, Product Manager for Motion Controllers, Siemens Industry, Factory Automation and Craig Nelson, Product Manager for Sinamics S Drives, Siemens Industry, Digital Factory

In this paper, the author discusses new paradigms in motion control, which allow machine designers and end users alike the ability to reduce motion design time and training costs, while increasing performance and transparency in the end product. A brief review of the motor, drives and controller technology is presented, with an emphasis on integrated safety, diagnostics and simulation, as the industry trends towards the digital factory.

To compete in the global market today, machine builders must deliver high-performance machines that are faster, more automated and more flexible, while always meeting customer expectations and keeping design costs under control. New technologies exist today to enable designers to fashion their motion control schemes with the full integration of the motor, drive and controller devices, while simultaneously integrating safety, diagnostic and operational simulation into the design, all in a virtual environment. The last development has myriad advantages, described in this paper.

As Fig. 1 demonstrates in the abstract, a typical machine today may have a wide variety of functions operating in multiple axes, ranging from the simple movements and speed setpoint control of a pallet indexer, mixer or component insertion device to the highly complex motions of Cartesian gantries, delta pickers, SCARA robots and other devices with path interpolation handling considerations. Also, the coordination of synchronized axes, cross cutters, flying shears, palletizers, hoisting or vertical conveyors, feeder and door control systems as well as large converting operations with constantly changing roll diameter and tension systems require sophisticated positioning, synchronized cam movements and other motion complexities. Add to this the growing need for machines to be more flexible, even to the point of continuous low-volume, even one-off, production and the motion control design and execution challenges grow.

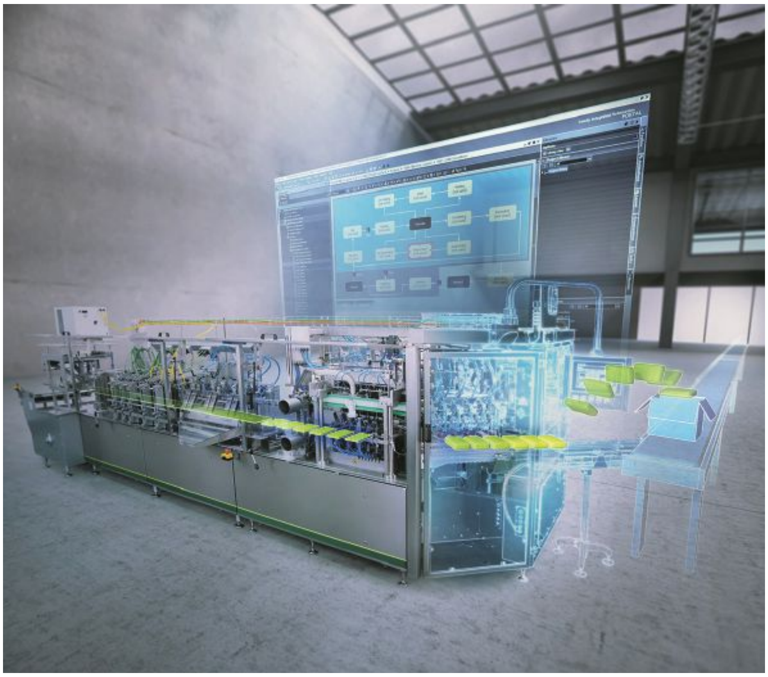
Further, with the impact of digitalization in the modern factory, the need to extract more data, prioritize it and even simulate operations on a machine prior to construction continues to present designers with unprecedented requirements in a time-constrained working environment.

But there are new ways to confront these challenges today. Here is a brief review of the typical motion control needs on today's machines.

Fig. 2 illustrates a variety of cyclic and continuous production requirements. For our purposes in this paper, we define "cyclic" as those in which an object is created stage by stage over a series of workstations, while "continuous" is defined as flow production without interruption, whether additive or subtractive, often in a CNC environment. Thus,

In this paper, the author discusses new paradigms in motion control, which allow machine designers and end users alike the ability to reduce motion design time and training costs, while increasing performance and transparency in the end product.

A brief review of the motor, drives and controller technology is presented, with an emphasis on integrated safety, diagnostics and simulation, as the industry trends towards the digital factory.



To compete in the global market today, machine builders must deliver high-performance machines that are faster, more automated and more flexible, while always meeting customer expectations and keeping design costs under control.

New technologies exist today to enable designers to fashion their motion control schemes with the full integration of the motor, drive and controller devices, while simultaneously integrating safety, diagnostic and operational simulation into the design, all in a virtual environment. The last development has myriad advantages, described in this paper.

Register to download the paper at:
www.usa.siemens.com/anewwayofmotion-wp

SIEMENS
Ingenuity for life

Kevin Wu • wu.kevin@siemens.com • 770-871-3982

Slip Rings for Rotary Index Table Applications

Your place for new products, literature, Apps, Videos, Case Studies and White Papers.

Motion control package for up to 6 axes »

The Festo Motion Control Package (FMCP) is a control system for coordinated motion of up to six axes for pick and place and other high speed, precision Cartesian robotic applications. This prewired and ready-to-install control solution provides the kinematics for H-portal, T-portal, 2-D, and 3-D Festo standard gantry systems. Original equipment manufacturers (OEMs) quickly can configure Cartesian motion applications using function blocks—with no specialized programming knowledge required. FMCP is compatible with all leading control architectures for fast, seamless integration. The FMCP also offers an ideal solution for end-of-arm-tooling. By including an I/O-link connection, the FMCP can control eight external digital inputs and eight digital outputs within the standard function block.

Festo Corp., www.festo.com Input #200 at www.controleng.com/information

« Safety PLC for machine functions

KEB America's Safety programmable logic controller (PLC) is a fail safe over EtherCAT (FSoE) master used in tandem with the machine PLC to execute and monitor the safety functions of the machinery. FSoE uses a black-channel approach and can be used with other bus systems. KEB's Safety PLC connects with other KEB FSoE slave modules. For monitoring safety devices with the Safety PLC, KEB now offers dedicated safe I/O modules. Each FSoE slave device has four safe inputs, two safe outputs, and four OSSD outputs. Because the modules use EtherCAT for fast, real-time communication, they are also ideal for existing systems or installations that require a scalable solution. One FSoE master can control up to 65,535 slave devices.

KEB America, www.kebamerica.com Input #201 at www.controleng.com/information

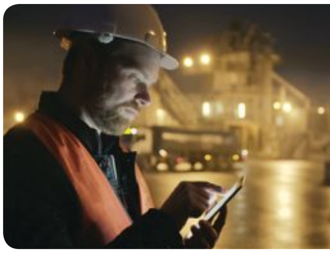
Left-hand shaft worm gearboxes

AutomationDirect's IronHorse worm gearbox line now includes left hand shaft models in four frame sizes and six gear ratios from 5:1 to 60:1. IronHorse cast iron worm gearboxes (worm gear speed reducers) are mechanical power transmission drive components that can drive a load at a reduced fixed ratio of the motor speed. Constructed of cast iron one-piece housings, the worm gearboxes feature a C-flange input. Designed to change drive direction by 90 deg. and to increase torque output, worm gearboxes are used when space is at a premium, such as for conveyors, or to simplify mechanical design. IronHorse gearboxes are mountable in any direction, except motor pointing up.

AutomationDirect
www.automationdirect.com

Input #202 at www.controleng.com/information

Asset performance insight tool for industrial equipment »



The Honeywell Connected Plant allows customers to manage the maintenance and operations of their industrial equipment more effectively. The Honeywell Connected Plant Asset Performance Insight connects the customers' assets and equipment to the cloud, and applies analytical models from Honeywell and its partners, so that customers can avoid unplanned downtime and unnecessary maintenance. Honeywell designed the Asset Performance Insight solution to be deployed rapidly to customers through pre-configured templates. These templates are based on the company's deep industry experience and real-world customer challenges enhanced with advanced analytics. The offering also can be configured and tailored to customers' specific needs.

Honeywell, www.honeywell.com Input #203 at www.controleng.com/information

Rugged touch computer »

Janam Technologies' XT100 rugged touch computer is designed to pack the power and performance of an industrial rugged mobile computer in a slim smartphone design. It is built to survive demanding work environments and can withstand repeated drops to concrete. It is sealed to IP65 standard for protection against water, dust, and extreme temperatures, providing reliable performance in every industry, including retail, field service, hospitality, warehouse, distribution, and direct store delivery. The XT100 addresses the most demanding data capture requirements with integrated 2-D barcode scanning technology, rear- and front-facing cameras, and near field communication (NFC) and radio frequency identification (RFID) reading capabilities.

Janam Technologies LLC, www.janam.com

Input #204 at www.controleng.com/information

PRODUCT & LITERATURE SHOWCASE

Input #109 at controlengineering.hotims.com

Input #110 at controlengineering.hotims.com

Advertising Sales Offices

ContentStream
Patrick Lynch,
Director of Content Marketing Solutions
630-571-4070 x2210
PLynch@CFEMedia.com

AL, FL, GA, MI, TN
Aaron Maassen,
Classified, Product Mart,
Media Showcase
630-571-4070 x2216
AMaassen@CFEMedia.com

AR, IL, IN, IA, KS, KY, LA, MN, MO, MS, NE, ND, OK, OH, SD, TX, WI, Central Canada
Bailey Rice
(630) 571-4070 x2206
BRice@CFEMedia.com

AK, AZ, CA, CO, HI, ID, MT, NV, NM, OR, UT, WA, WY, Western Canada
Iris Seibert
(858) 270-3753
ISeibert@CFEMedia.com

CT, DE, MD, ME, MA, NC, NH, NY, NJ, PA, RI, SC, VA, VT, WV, DC, Eastern Canada
Julie Timbol
(978) 929-9495
JTimbol@CFEMedia.com

Internation (outside U.S., Candada)
Stuart Smith
+44 208 464 5577
stuart.smith@ssm.co.uk

Publication Services

Jim Langhenry, Co-Founder/Publisher, CFE Media
JLanghenry@CFEMedia.com

Steve Rourke, Co-Founder, CFE Media
SRourke@CFEMedia.com

Trudy Kelly, Executive Assistant,
630-571-4070, x2205, TKelly@CFEMedia.com

Elena Moeller-Younger, Marketing Manager
773-815-3795, EMYounger@CFEMedia.com

Kristen Nimmo, Marketing Manager
KNimmo@CFEMedia.com

Brian Gross, Marketing Consultant, Global SI Database
630-571-4070, x2217, BGross@CFEMedia.com

Michael Smith, Creative Director
630-779-8910, MSmith@CFEMedia.com

Paul Brouch, Director of Operations
PBrouch@CFEMedia.com

Michael Rotz, Print Production Manager
717-766-0211 x4207, Fax: 717-506-7238
mike.rotz@frycomm.com

Maria Bartell, Account Director, Infogroup Targeting Solutions
847-378-2275, maria.bartell@infogroup.com

Rick Ellis, Audience Management Director
303-246-1250, REllis@CFEMedia.com

Letters to the editor: Please e-mail us your opinions to MHoske@CFEMedia.com or fax 630-214-4504. Letters should include name, company, and address, and may be edited.

Information: For a Media Kit or Editorial Calendar, email Trudy Kelly at TKelly@CFEMedia.com.

Marketing consultants: See ad index.

Custom reprints, electronic: Marcia Brewer, Wright's Media, 281-419-5725, mbrewer@wrightsmedia.com

CFE Media
Content for Engineers

CONTROL ENGINEERING®
ad index

Company	Page#	RSN	Web
Allied Electronics	C1, 7	5	www.alliedelec.com
AutomationDirect	C2, 16A-16D	1	www.automationdirect.com
B & R Industrial Automation	19	10	www.br-automation.com/ACOPOSmotor
Battery Ventures	56	22	www.battery.com/private-equity
CFE Media's New Products for Engineers Database	47		www.controleng.com/NP4E
Control Engineering Digital Reports	37		www.controleng.com/DigitalReports
Control Engineering Software & Hardware Study	23		www.controleng.com/2018HMIReport
Control Engineering Webcasts	62		www.controleng.com/webcast
Dataforth Corp	9	7	www.dataforth.com
Eaton's Bussmann Business	2	3	www.CUBEFuse.com
Emerson Automation Solutions	57	23	www.emerson.com
Festo Corporation	37	13	www.festo.com
GAMS 2018	33		www.controleng.com/2018-global-automation-manufacturing-summit
Inductive Automation	Bellyband		www.inductiveautomation.com/ignition
Kepware Technologies	1	2	www.kepware.com/CE
Moore Industries - Intl. Inc.	4	4	www.miinet.com
MOTION INDEX DRIVES	59	25	www.motionindexdrives.com
Nidec Industrial Automation USA, LLC	47	16	www.NidecUnidriveM.com
RADWELL INTERNATIONAL, INC	15	9	www.Radwell.com
Sealevel Systems Inc	23	12	www.sealevel.com
SEW-EURODRIVE, Inc.	13, C4	8, 27	www.seweurodrive.com
Siemens	C1, 21, 58	11, 24	www.usa.siemens.com/tia-portal-ce
Steute Industrial Controls, Inc.	8	6	www.switches-sensors.zf.com/us
Subscribe to *Control Engineering*	59		www.controleng.com/subscribe
UNIVERSAL ROBOTS	45	14	www.universal-robots.com
Yaskawa America, Inc.	C3	26	www.yaskawa.com
YRG ROBOTICS	46	15	www.yrginc.com
Inside Machines			
Aerotech Inc	M6	20	www.aerotech.com
Allied Moulded Products, Inc.	M8	21	www.alliedmoulded.com
automatica 2018	M5	19	www.automatica-munich.com
Beckhoff Automation LLC.	M4	18	www.beckhoff.com
WAGO Corp.	M2	17	www.wago.us

REQUEST MORE INFORMATION about products and advertisers in this issue by using the ***http://controleng.com/information*** link and reader service number located near each. If you're reading the digital edition, the link will be live. When you contact a company directly, please let them know you read about them in *Control Engineering.*

Josh Westmoreland, Cross Company

Collaborative robot applications for non-standard businesses

Industries that have never been interested in robotics are finding collaborative technology can help them reap benefits because collaborative robots are easier to program than typical robots—and their impact is growing. Three questions for companies to consider are highlighted.

Collaborative robots have been a disruptive technology in not only the manufacturing industry, but they have also opened the door for automation in other industries as well. Industries that have never been interested in robotics are suddenly finding that with collaborative technology they too can reap the benefits that come from automation. Why can companies outside of manufacturing now look to robotics when it hasn't been an option before?

First, collaborative robots are capable of operating around people without the need for external guarding or safety devices (pending a risk assessment of the total application). This has been a gateway to new industries for robotics. Without the need for a large safety enclosure, robots can now be used in places that wouldn't have been feasible in the past.

Second, collaborative robots are typically much easier to program than traditional industrial robots. Companies no longer need a staff of robotics engineers to program simple applications. When deciding if collaborative robots are a good fit, companies should ask these three questions:

1. Is the task repetitive?

This is possibly the most important question for a quick installation. Robots, whether collaborative or traditional, are programmed to carry out a task over and over again. While there are some methods to allow robots to have flexibility, the simplest and easiest of installations require the robot to carry out the same task over and over. For example, placing hamburger patties onto a grill and flipping them after a predetermined amount of time before removing them from the grill and placing into another location. These types of repetitive tasks lend themselves very well to collaborative robot technology. Wherever a task is performed repeatedly, there is the potential for robotic automation.

2. What are the operating hours?

When it comes to considering robotics, one must consider not only the feasibility of the application but also the return on investment (ROI) to determine if the application makes sense from a business perspective. Oftentimes, this component gets overlooked until many hours have been spent on the engineering side. ROI is variable and has to take not only the application into account but the hours of operation and the burden rate of an employee. With minimum wage on the rise, many companies are starting to realize faster ROI periods for adding collaborative automation.

3. Is the task dirty, dull, dangerous?

Dirty jobs are generally the tasks that employees do not want to perform. They could be smelly, grimy, or even involve the employee needing to take regular breaks to get cleaned up. These can be a morale killer and impact productivity by employees feeling negative about the task they are being asked to perform. Some of these tasks even start falling into the dangerous category. Chemical cleaners, working around hot objects, or working in tightly confined spaces can become dangerous very quickly.

In some robotic applications, the main goal isn't just to increase throughput or reduce costs, but to alleviate the need for the operator to carry out dangerous tasks. However, the two are not mutually exclusive and all of these factors can be considered when evaluating the potential of robotic integration. **ce**

Josh Westmoreland is a robotics specialist at Cross Company. This article originally appeared on Cross Company's blog. Cross Company is a CFE Media content partner. Edited by Chris Vavra, production editor, CFE Media, Control Engineering, *cvavra@cfemedia.com.*

M More INNOVATIONS

KEYWORDS: Collaborative robots

Collaborative robots are designed to work without a safety fence, which allows them to be used in non-traditional applications.

Companies considering collaborative robots need to ask what are the operating hours for the task and whether the task is repetitive, dangerous, or dirty.

GO ONLINE

Read this story online at www.controleng.com for links to additional stories about collaborative robots and their potential for manufacturers and non-manufacturers alike.

CONSIDER THIS

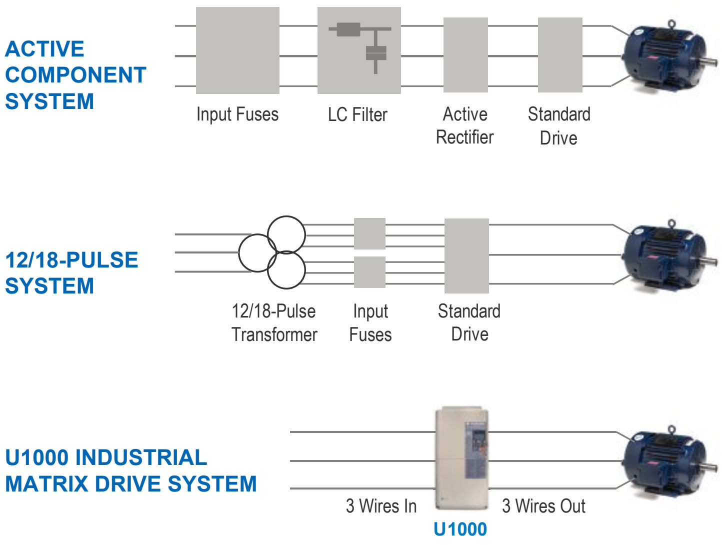
What other considerations should companies have when deciding whether to use a collaborative robot?

YASKAWA

Enter the Matrix

Using complicated systems for low harmonics or power regeneration? Try the efficient way with the U1000 Industrial Matrix Drive.

Our greenest drive ever, the U1000 goes beyond the performance of conventional drives. Enjoy extremely low harmonic distortion and regeneration in a space-saving design, completely without the need for additional components.



ACTIVE COMPONENT SYSTEM

Input Fuses

LC Filter

Active Rectifier

Standard Drive

12/18-PULSE SYSTEM

12/18-Pulse Transformer

Input Fuses

Standard Drive

U1000 INDUSTRIAL MATRIX DRIVE SYSTEM

3 Wires In

3 Wires Out

U1000

Yaskawa America, Inc. Drives & Motion Division 1-800-YASKAWA **yaskawa.com** For more info: http://go.yaskawa-america.com/yai1145

input #26 at www.controleng.com/information