AUGUST 2022

InTech®

OFFICIAL PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

ISA™

www.isa.org/intech

INDUSTRY 4.0 AND THE SMART FACTORY

- Industrial Readiness & Maturity
- Artificial Intelligence & Machine Learning
- Virtualization Technologies (AR/VR)
- Industrial Internet of Things (IIoT)
- Cloud & Edge Computing
- Digital Twin & Simulation
- Industrial Connectivity
- Industrial Cybersecurity

Don't let a simple support call become a costly site visit

StrideLinx

With StrideLinx remote access you can securely connect with remote systems in an instant, troubleshooting and correcting issues without the hassles, delays and costs of traveling.

StrideLinx VPN routers provide 10GB of **FREE** monthly bandwidth to securely monitor, program and/or troubleshoot your remote systems. Optional services are available to maximize your remote access capabilities, including:

- Cloud-based Data Logging - Unlimited cloud data storage for up to 7 years with active subscription
- Cloud Notify/Alarming - provides customized "alarm" email and push notifications when control limits are exceeded on HMI / PLC devices connected to the StrideLinx VPN router
- White Labeling allows users to re-brand the platform, mobile app and hardware

verizon

Research, price, buy at: www.automationdirect.com/stridelinx

Order Today, Ships Fast!

TOP RATED BY CUSTOMERS

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


Monitor machine health
with precise power data
New groov RIO EMU (energy monitoring unit)
• Monitor category III 3-phase AC power up to 600 V in Delta or Wye configurations
• Capture 18 data values per phase—voltage, current, true power, power factor, and frequency—plus 10 3-phase totals
• Measure power and energy at the point of use to detect downtime predictors like high power consumption
• Easily share real-time data with analytics software, databases, and dashboards using the built-in MQTT/Sparkplug client
• Secure the system and data with user accounts, configurable firewall, TLS certificates, HTTPS, and VPN client
• Quickly power for standalone operation with 802.3af PoE Class 0 switches or use 10-32 VDC line power
groov RIO
Visit https://op22.co/rioemu to learn more!
Power Mon
Sparkplug
MQTT
MADE IN THE USA
Made and supported in the U.S.A.
Call us toll-free at 800-321-6786 or visit www.opto22.com
All registered names and trademarks copyright their respective owners.
OPTO 22
Your Edge in Automation.™

InTech
AUGUST 2022 | VOL 69, ISSUE 4

FEATURES

DEPARTMENTS

InTech MAGAZINE

InTech, USPS # 0192-303X, is published bimonthly in Research Triangle Park, NC by the International Society of Automation (ISA), P.O. Box 12277, Research Triangle Park, NC 27709.

ISSN 0192-303X

Volume 69, Issue 4

Editorial and advertising offices are at 3252 S. Miami Boulevard, Suite 102, Durham, NC 27703; phone 919-549-8411; email info@isa.org. *InTech* and the ISA logo are registered trademarks of ISA. *InTech* is indexed in Engineering Index Service and Applied Science & Technology Index and is microfilmed by NA Publishing, Inc., 4750 Venture Drive, Suite 400, P.O. Box 998, Ann Arbor, MI 48106.

To order reprints of *InTech* print or digital articles, contact Nathan Swailes at reprints@mossbergco.com or 800-428-3340.

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

Subscriptions: ISA Members receive *InTech* as part of their annual membership. Become an ISA Member at: http://www.isa.org/join. Other subscribers: 175 USD in North America; 235 USD outside North America. Single copy and back issues: 20 USD + shipping.

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

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

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

www.isa.org/InTech

Setting the Standard for Automation™

FEATURES

www.isa.org/InTech

ISA Members Contribute to the Action of Automation

By Renee Bassett, *InTech* Chief Editor

It all started in Mumbai in October 2015. In a conversation with then ISA President Jim Keaveney, ISA member Sujata Tilak described how industrial automation and control systems played a vital role in the burgeoning field of the Industrial Internet of Things (IIoT). "They are the foundation for IIoT, and, conversely, all major areas of automation are impacted by IIoT," she said.

Keaveney agreed that ISA should look at these areas, but it wasn't until soon-to-be-president Carlos Mandolesi came forward in 2017 to work with Tilak that formation of a new ISA division happened. After two and a half years of planning, the Smart Manufacturing and IIoT (SMIIoT) Division was reality. Said Tilak at the time, "We hope to catch all the action happening in the smart manufacturing and IIoT space via our diverse membership and contribute to this action."

Contribute they have. The hundreds of ISA volunteers around the globe who are associated with ISA's newest division are active and passionate about how the technologies they focus on are essential to the success of industrial companies and the professionals who work for and with them.

Since 2020, SMIIoT members have published 37 articles on the ISA Interchange blog (https://blog.isa.org) that answered questions like, "'What does an HMI look like in the age of Industry 4.0?" or "What is IIoT?" They helped launch ISA's virtual events program with the debut of the IIoT & Smart Manufacturing Virtual Conference in October 2020. Now, the SMIIoT Division has taken over this special edition of *InTech* magazine.

Division Director Jeff Winter envisioned an entire publication devoted to the eight key topics within Industry 4.0, which correspond to the eight SMIIoT technical committees. The technical committee chairs wrote or co-wrote the bulk of what you see in this issue with the support and encouragement of the other division leaders listed on page 8. The result is a guide to some of the most important cutting-edge innovations in industrial automation today.

All ISA divisions (https://connect.isa.org/community/divisionlist)—and there are 16 covering various technology areas or vertical industries—help members grow professionally and technically by developing technical content and approaches to solving critical problems. Future *InTech* special editions will let those members shine a light on their corner of the automation space. In the meantime, ISA volunteers around the world continue to develop standards, organize discussions, produce webinars, present at conferences, write articles, and otherwise contribute their actions toward making the world a better place through automation. ■

Carlos Mandolesi and Sujata Tilak in 2019 celebrating the approval of the SMIIoT Division.

InTech

OFFICIAL PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

EDITORIAL

CHIEF EDITOR

Renee Bassett, rbassett@isa.org

CONTRIBUTING EDITORS

Bill Lydon, blydon@isa.org

Charley Robinson, crobinson@isa.org

Jack Smith, jsmith@isa.org

STAFF WRITERS

Melissa Landon, Lynn DeRocco

ART & PRODUCTION

Lynne Franke, Production Editor

Bonnie Walker, Art Director

Jamie McLendon, Graphic Designer

Colleen Casper, Digital Designer

ADVERTISING & SPONSORSHIP

PUBLISHER

Rick Zabel, rzabel@isa.org

ACCOUNT EXECUTIVES

Richard T. Simpson, richard@isa.org

Chris Nelson, chris@isa.org

Gina DiFrancesco, gina@isa.org

MEDIA KIT

https://tinyurl.com/InTechAcom2022mediakit

ISA MEMBER LEADERS

ISA PRESIDENT

Carlos Mandolesi

PUBLICATIONS VICE PRESIDENT

Joao Miguel Bassa

PUBLICATIONS VICE PRESIDENT-ELECT

Nicholas Sands

INTECH EDITORIAL ADVISORY BOARD

Joao Miguel Bassa

Nicholas Sands

Patrick Bouwman

Vitor Finkel

Tom McAvinew

Michael Murray

Russ Rhinehart

Steve Valdez

100%

of **Reference Standards traceable** to Nationally Recognized Standards.

Ensure compliance and increase process uptime with optimized services

- Lab and field accredited calibrations (A2LA) and verification capabilities for flow, pressure and temperature instruments
- Patented, industry-expert methods to optimize your calibration plan
- We are a leading manufacturer of process instrumentation – uniquely qualified to verify and calibrate
- Our global, harmonized calibration standards provide consistent service quality

Do you want to learn more?
www.us.endress.com/calibration-usa

Endress+Hauser
People for Process Automation

Smart Manufacturing and Industrial IoT Shine Bright

Along with most of the automation community, ISA knows that the future of manufacturing is more than just being automated—it is a digital, smart, and integrated set of cyber-physical systems enabling greater performance in terms of agility, efficiency, safety, security, and sustainability. The fourth industrial revolution introduced a paradigm shift. This is why, in 2020, ISA created the Smart Manufacturing and IIoT (SMIIoT) Division. Today, more than 3,000 ISA members want to be a part of it.

ISA divisions help members professionally and technically by focusing on specific vertical industries or technology clusters. They develop technical content and standardized approaches to solving critical problems and provide a forum for networking and collaboration.

SMIIoT Division members do this work through one of eight technical committees that each represent key topics within the Industry 4.0 framework. SMIIoT Division activities are directed by the 2022 division leaders shown on this page. Activities include:

- creating and collecting technical resources such as articles, whitepapers, webinars, and case studies
- supporting ISA's Smart Manufacturing & IIoT Conference
- collaborating with ISA Districts and Sections to promote and disseminate relevant information
- expanding volunteer opportunities for further collaboration and networking
- publishing a quarterly newsletter for awareness of SMIIoT Division activities
- developing a network of smart manufacturing and IIoT partner organizations as resources to members.

Join the SMIIoT Division if you want to learn, contribute, and network around one or more of its topics, and help division members and ISA create a better world through automation. Use the QR code on the cover of this publication, visit isa.org/SMIIoT, or contact any of the division leaders shown here. ■

2022 Division Leadership

Division Director
Jeff Winter, Microsoft

Membership Chair
Shridhar Kulkarni

Board Member
Dharmender Singhal

Division Director-Elect
David Schultz, G5 Consulting

Marketing Chair
Jessica Morell

Awards Chair
Karam Rehani

Program Co-Chair
Mike Nager, Festo

Past Director
Sujata Tilak, ascent intellimation

Newsletter/ Webmaster
Ryan Kershaw, Litmus

Program Co-Chair
Lalit Bangera, Siemens

Board Member
Victor Venâncio, IHM

Section-Division Liaison
Yogeswaran Supramaniam

Secretary
Dattatray Sawant, NIMMS

Board Member
John Whitten, Projects of Things

2022 Technical Committee Chairs

Industrial Connectivity
Andy Piatek, Novus Technical Services

Virtualization Technologies (AR & VR)
Mario Ishikawa, PackIOT

Industrial Cyber Security
Jacob Chapman, Nozomi Networks

Artificial Intelligence & Machine Learning
Ines Mechkane

Digital Twin & Simulation
JP Zeballos Raczy

Industrial Internet of Things (IIoT)
Shiv Kataria, Siemens

Cloud & Edge Computing
Ryan Treece, Telit

Industry Maturity & Readiness
Brian Romano, AGR


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

The Birth of Industry 4.0 and Smart Manufacturing

Industry 4.0 and smart manufacturing. What do these terms mean? Can they be used interchangeably or not?

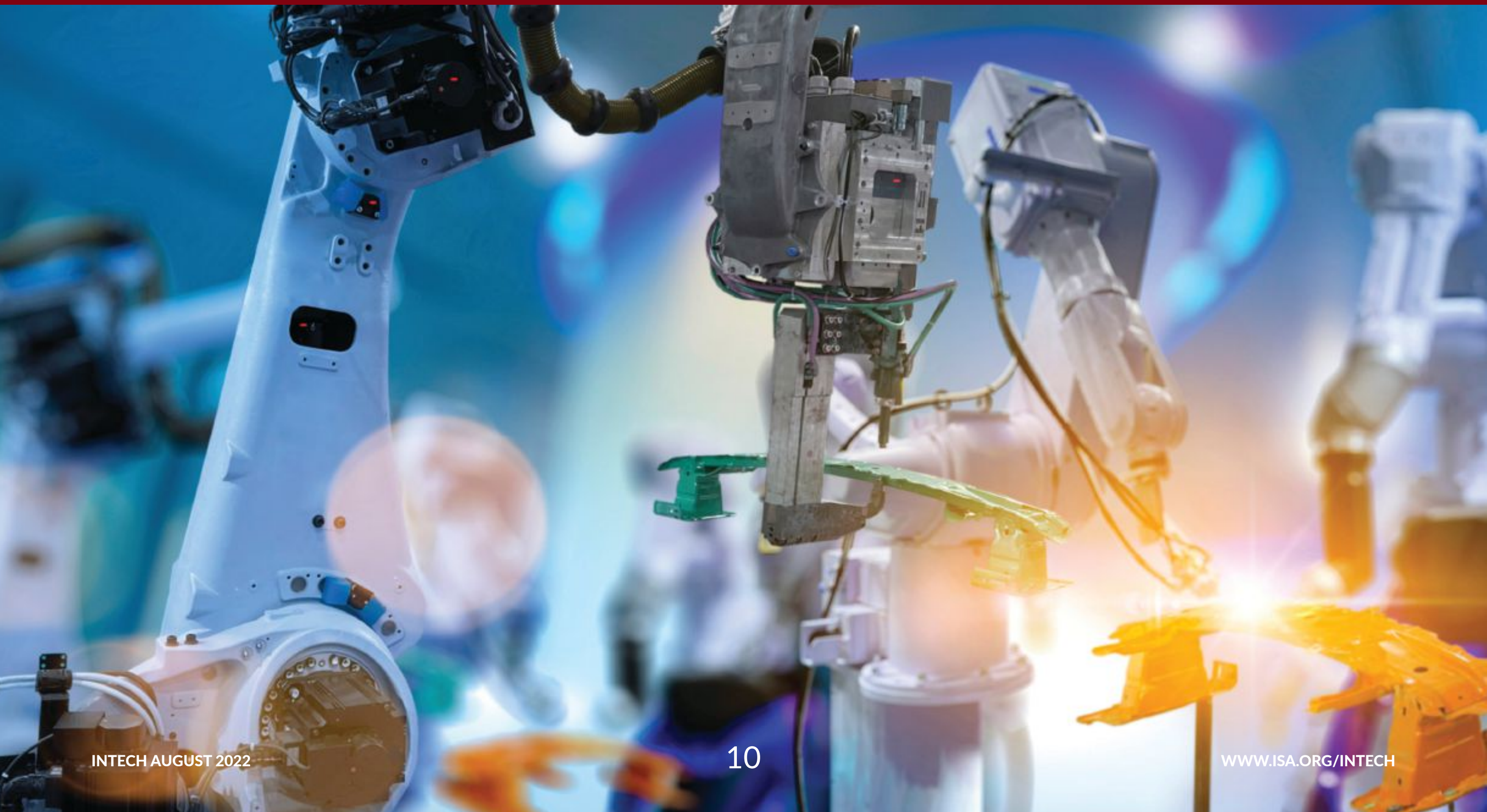
Industry 4.0 is a paradigm shift in organizing and managing industrial businesses.

By Jeff Winter

It is nearly impossible to be in the manufacturing or the industrial automation industry and not have heard these buzzwords used in one form or another. They seem to be everywhere, actively discussed by thought leaders, industry experts, strategists, and company executives. They are written in mission statements and are even part of annual goals for a lot of companies, which gives the impression that everyone knows exactly what they are. But if you start asking people what the terms mean, they will either be honest and say, “I have an idea, but I don’t really know,” or they will give you an answer that is totally different from the next person’s.

And if that is the case, it would make using or achieving anything related to these concepts difficult, wouldn’t it?

The purpose of this special edition of *InTech* magazine is to help clarify these concepts by defining them, identifying the technology components, and explaining their relationship to one another and to your organization. Most



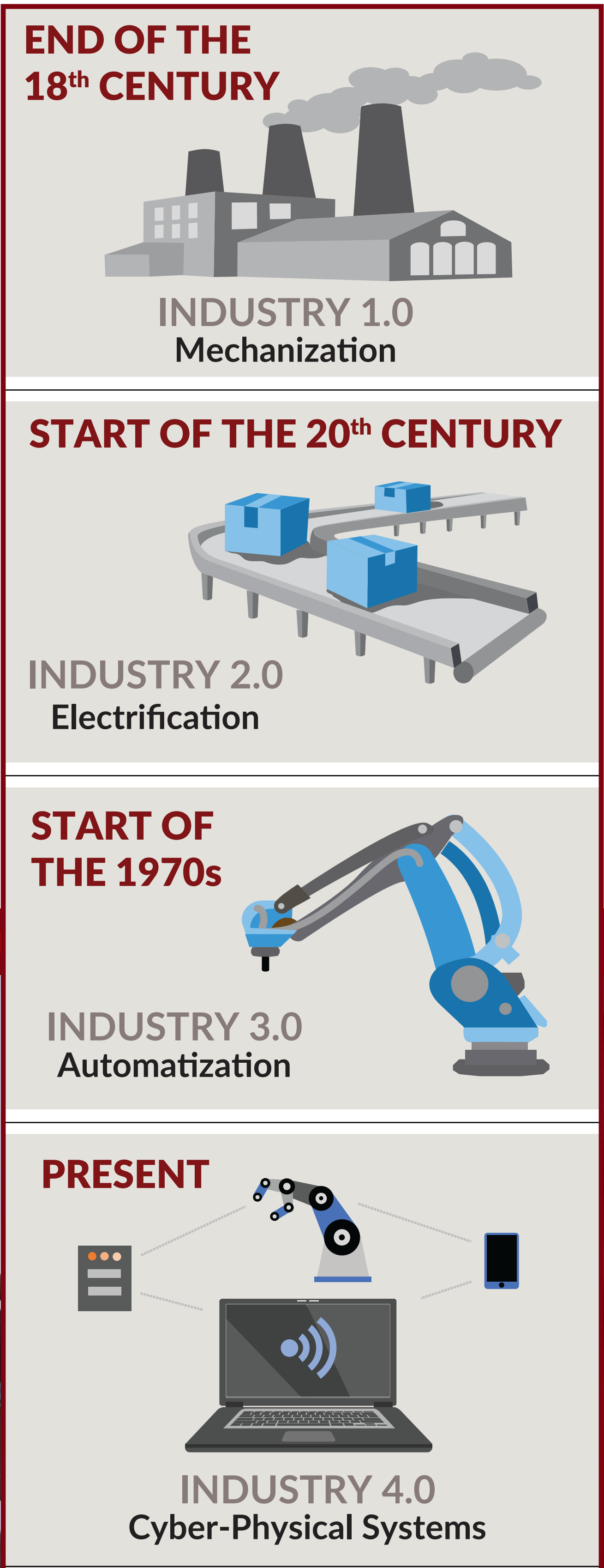
importantly, we will answer the question: Why are these concepts such a big deal right now?

The birth of Industry 4.0

Industry 4.0 (known as “Industrie 4.0” in Europe) was brought to life as a term and a concept in 2011 at Hannover MESSE, where Bosch described the widespread integration of information and communication technology in industrial production. The entire manufacturing industry, along with the German government, took interest in this idea.

After Industry 4.0 was introduced, the idea turned into the “High-Tech Strategy 2020” action plan in 2012 by the German government. This idea took hold, and soon dozens of other governments developed their own initiatives, all similar in purpose, but different in execution and scope.

China developed “Made in China 2025” to fully modernize the country’s manufacturing industry. The United Kingdom introduced its “Future of Manufacturing” in 2013; the European Union developed its “Factories of the future” in 2014; Singapore came out with its “RIE2020” plan; and yes, the U.S., in 2014, launched the “Manufacturing USA” initiative that created a network of 16 member institutes. Each of the institutes focuses on a specific advanced manufacturing technology. They each pull together private-sector companies, academic institutions, and other stakeholders to pursue collaborative research and development, test applications, train workers, and reduce the risks associated with deploying new technologies.



To understand the fourth industrial revolution, it helps to know the names and timeline of the first three.

A working group on Industry 4.0 was formed, led by Bosch executive Siegfried Dais and Henning Kagermann, the former chairman and CEO of SAP and president of the German National Academy of Science and Engineering (https://en.acatech.de). In 2013, this working group presented a set of Industry 4.0 implementation recommendations to the German federal government. From that moment forward, the fourth industrial revolution had begun, and the working group members were recognized as the founding fathers and driving force behind Industry 4.0.

An 85-page paper developed by the Industry 4.0 working group starts off by explaining how we are entering the fourth industrial revolution—hence the reference to "4" in "Industry 4.0." To understand the fourth industrial revolution, it helps to remember the first three, and how we got to this point (figure). At the end of the 18th century, the first industrial revolution involved mechanization—using water and steam to increase production beyond that of manual labor. It can be represented by the introduction of the first mechanical loom in 1784. The second industrial revolution saw the development of assembly lines powered by electricity. Electrification typified Industry 2.0, which continued through the start of the 20th century.

Industry 3.0 introduced electronics and computers to replace manual processes. The dawning of this era of "automatization," according to the Industry 4.0 working group paper, could be represented by the introduction of the first programmable logic controller, the Modicon 084.

Our present era, Industry 4.0, is known as the era of cyber-physical systems—the convergence of physical, digital, and virtual systems and the rise of the Internet of Things (IoT). Industrial IoT (IIoT) emphasizes manufacturing IoT as distinct from retail/consumer, medical, or other IoT devices or architectures. Industry 3.0 is about automation—the reduction of human intervention in processes. Industry 4.0 is about cognition or the process of acquiring knowledge and understanding. These two are separated by the ability to properly capture and harness the power of data.

Trying to define Industry 4.0

Industry 4.0 is not merely a matter of connecting machines and products through the Internet. It encompasses a wide range of advanced technologies, such as digital twins, artificial intelligence, high-speed wireless networks, deterministic wired networks, cloud and edge computing, and virtualization technologies like augmented reality. It is also a paradigm shift in how we organize, manage, and approach business to make the most of cyber-physical systems.

The working group characterized Industry 4.0 as a concept that is focused on creating smart products, smart procedures and processes, and smart factories. But that statement is so grandiose and vague that it is almost no help. With all that visionary talk, we can easily get excited and energized, but we still do not have a definition. The Industry 4.0 working group did not really provide one.

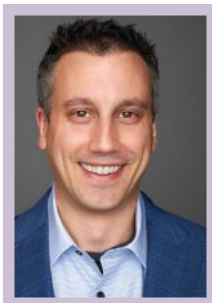
Over the past nine years, people have latched onto the concept of Industry 4.0. Each country attempted to define it in its context as it saw fit, which of course meant different ideas everywhere. Several years after the working group convened, two of the largest standards bodies, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), got together and formed a joint working group called JWG21. Its main intent was defining the concept of Industry 4.0. In the middle of 2021, the JWG21 finally established a definition. For myriad reasons, the term "smart manufacturing" was selected instead of "Industry 4.0." The group felt it better represented a global viewpoint.

Here is the current formal definition of smart manufacturing:

Manufacturing that improves its performance aspects with integrated and intelligent use of processes and resources in cyber, physical, and human spheres to create and deliver products and services, which also collaborates with other domains within enterprises' value chains.

- *Note 1: Performance aspects include agility, efficiency, safety, security, sustainability, or any other performance indicators identified by the enterprise.*
- *Note 2: In addition to manufacturing, other enterprise domains can include engineering, logistics, marketing, procurement, sales, or any other domains identified by the enterprise.*

As a society, we are starting to feel the impacts of Industry 4.0 already. Not only are companies investing, but governments around the world are pouring a lot of money into this idea as the way of the future. Smart manufacturing promises improved performance through the digital transformation of manual and mechanical systems, and the further integration of automated systems with business systems and advanced technologies. We all are in the midst of this paradigm shift and are being compelled to move our companies forward. The birth of Industry 4.0 is giving way to growth and change, asking us to help move our companies toward whatever the next revolution might bring. ■



ABOUT THE AUTHOR

Jeff Winter (www.linkedin.com/in/Jeffreyrwinter) is the 2022 director of ISA's Smart Manufacturing and IIoT (SMIIoT) Division. He is also part of the International Board of Directors for Manufacturing Enterprise Solutions Association (MESA), a U.S. registered expert for IEC as a member of TC 65, a Global AI Ambassador for SwissCognitive, and on the Smart Manufacturing Advisory Board for Purdue University. Winter is currently an industry executive for manufacturing with Microsoft, where he helps U.S. manufacturers digitally transform their businesses at scale.

Walking the Path of Digital Transformation

Ready for Industry 4.0? Evaluate people, processes, and then technology.

By Brian Romano

Academic research expresses readiness as the state of being psychologically and behaviorally prepared. By extension, smart manufacturing industry readiness is how businesses can leverage Industry 4.0 technologies and be psychologically and behaviorally prepared as an organization.

Although different organizations may be similar by having products in a vertical industry, each is unique with its own culture, size, management team, and other traits. Moreover, each organization will have a unique ability to adapt Industry 4.0 principles and practices. Specialized companies now provide a level of uniformity and guidance, but also customizable features, to aid organizations in what has become known as the "digital transformation" toward the adoption of Industry 4.0, with a goal of organizational transformation in efficiencies and effectiveness.

Industry 4.0 readiness models (https://www.mdpi.com/2078-2489/11/7/364) are mostly designed with two unique angles, one of finding practice applicability and the other of finding users for the respective readiness definitions. Recent studies of literature related to small to medium-sized enterprises (SMEs) found they have some weaknesses and gaps in the maturity models identified. The areas identified showed that the models are technology focused and, therefore, can overlook management or cultural dimensions. They also may not consider company size, vertical industry, or the complexity of the product being made.

Several other models have been published by both industrial and academic organizations to help guide companies starting the digital journey and transforming their businesses to adopt Industry 4.0 technologies and practices. One of the studies (https://doi.org/10.3390/s22031185) summarized a company's readiness into three high-level silos: smart process planning, infrastructure, and organization and human resources.

Why digital transformation is important now

Between the pandemic, the supply chain shortage, the workforce shortage, and the related skills gap, it is becoming increasingly essential for organizations to begin a digital transformation to stay competitive on the world stage. The digital transformation, part of which is the implementation of Industry 4.0 practices, encompasses the entire enterprise, including the upstream and downstream connections in the value chain. Because the transformation is all encompassing, it requires commitment, organizational maturity, and a company with the physical, structural, and cultural resources to adopt digital technologies.

A company's ability to implement new technologies takes a commitment from the entire enterprise. Without the support of the company's management and ownership, consisting of financial and organizational commitment, the effort to implement any significant initiative is doomed to fail. The same is also true when implementing Industry 4.0, smart factory, and Industrial Internet of Things principles and practices. Recent studies have identified what management is looking

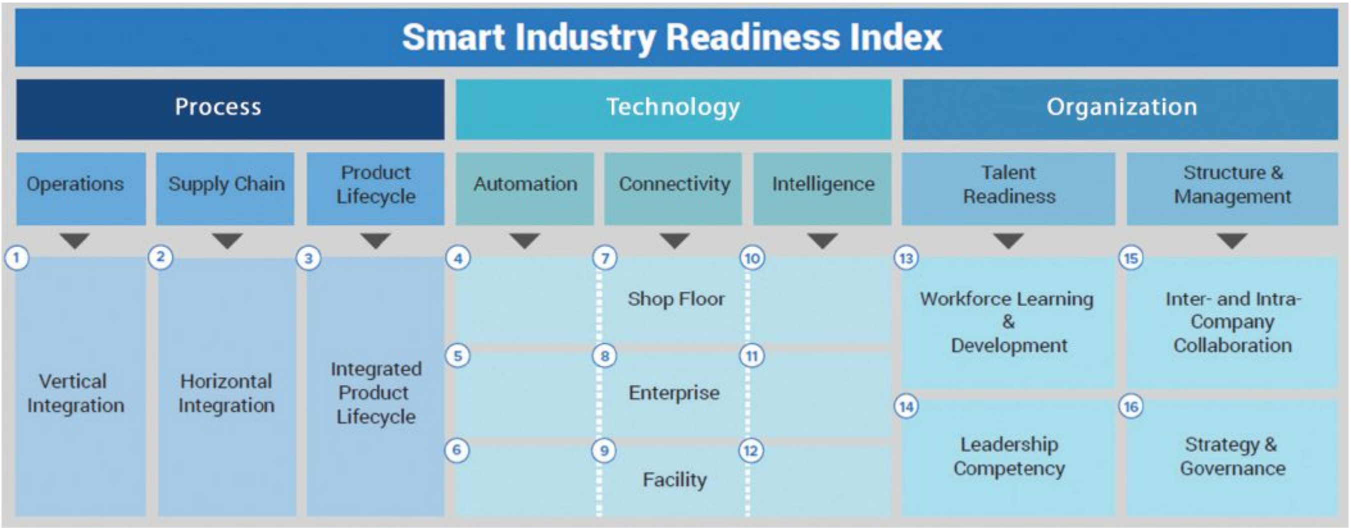


Figure 1. The 16 points of the "Smart Industry Readiness Index (SIRI)" framework are considered in a SIRI assessment.

for from the adoption of Industry 4.0. The top two motivations are expected increases in productivity and product quality; one of the top five goals is a return on investment.

Industry 4.0 readiness needs to be viewed from wall to wall within an organization. Because all the aspects of implementing a smart manufacturing program can be overwhelming, having an organized methodology and strategy to assist in planning is paramount to success. Adherence to such a plan can help keep the program aligned with industry best practices and prevent a company from going down a path that is not desired or that will not yield a positive outcome.

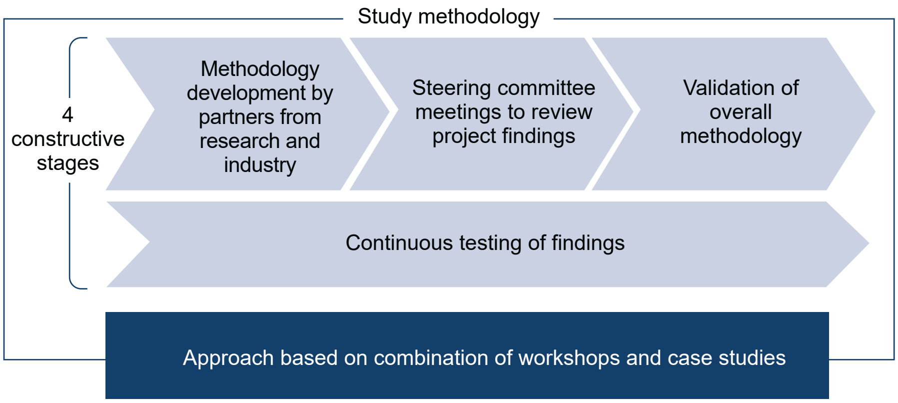


Figure 2. Stages of development, testing, and validation accomplished during workshops and case studies selected by a steering committee within the organization.

Models, maps, and other trends

Maturity and readiness models for industrial transformation existed as early as 2006, but most were published within the last three to four years. Most of the readiness models listed in the literature are academia based, with only 30 percent being industry-driven models.

One of the more prominent industry models (http://www.edb.gov.sg) was created by the Singapore Economic Development Board in conjunction with many leading technology companies and industry experts worldwide. The Smart Industry

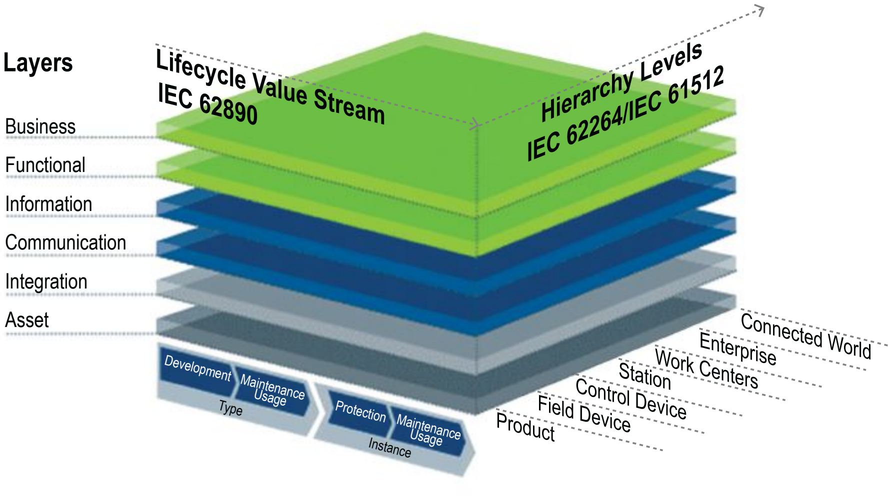


Figure 3. Three-dimensional aspect of the RAMI model, which can help guide companies to deploy Industry 4.0 in an organized and structured way.

Readiness Index (SIRI) (https://siri.incit.org/frameworks-tools) comprises a suite of frameworks and assessment tools meant to provide the initial, scaling, and sustaining guidance companies need for digital transformation.

Figure 1 depicts the 16 elements considered within a SIRI assessment. Like what is described in the academic research, the SIRI index is similarly based on the three pillars of process, technology, and organization, while also considering an organization's current capabilities from infrastructure, technology, culture, and management perspectives.

The assessment and adoption processes are iterative within the SIRI, as well as within many other academic and industrial-driven assessments and frameworks. Companies need to anticipate an ongoing and evolving process, much like any continuous improvement or Lean initiative. Like any Deming-related cycle of plan-do-check-act, the assessment frameworks consider learning, evaluation, planning, and implementation stages. The assessment methodology associated with the German National Academy of Science and Engineering (acatech) Industrie 4.0 Maturity Index demonstrates a cycle of development and testing along the path of readiness and maturity discovery (figure 2).

A recent augmentation of the readiness infrastructure is the introduction and inclusion of a three-dimensional map named the Reference Architecture Model for Industrie 4.0 (RAMI 4.0), which depicts an industry 4.0 implementation that incorporates all aspects of a company (figure 3). This map integrates the life cycle value stream described in the IEC 62890 standard with the hierarchical levels described in the IEC 62264 and IEC 61512 standards.

In the RAMI 4.0 model, the hierarchy level axis accounts for the information technology and control systems. The life cycle value stream accounts for the life cycle of the organization's products and manufacturing facilities, and the layers show the makeup of a machine into its component structures.

How this topic supports a smart factory

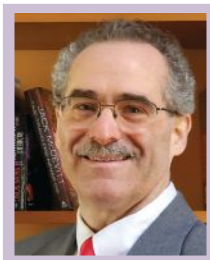
The goal of the complete digital transformation and deployment of Industry 4.0 is an integrated smart factory. A smart factory exists when the organization has a sufficiently high level of integration to allow the production processes to be better organized and optimized to achieve a higher level of automatic sustainability. Connecting the production indicators with the results of a maturity index, such as what is accomplished with the acatech Industrie 4.0 Maturity Index, generates outcomes of assessment versus implementation, which can be cast with actual and definitive outcomes and figures.

Based on these fundamentals, it should be strongly noted that the digital transformation journey to Industry 4.0 readiness is not simply a technology application. Although many of the pillars of Industry 4.0 are technology-laden, a company's maturity and readiness for implementation do not and cannot rest solely on the technology that will be applied. As depicted in the three high-level silos mentioned previously, it is the culmination of the organizational planning, the technology infrastructure, and the human resources both within the organization and throughout the entire value chain that comprise readiness and maturity.

The technology aspect is used to expose and collect the information that is then also used for analysis, which provides a means for understanding that information. The final results from the collected and evaluated data are then left as an element of how the organization will use the information and analysis.

Looking ahead

For a company considering an Industry 4.0 implementation that is willing to start digital transformation, it is paramount to assess readiness and maturity. With the large undertaking and commitment that such a journey will require, assessing a company's infrastructure, culture, and commitment is a needed first step. ■



ABOUT THE AUTHOR

Brian Romano (Brian.Romano@arthurgrussell.com) is chair of ISA's Industry Readiness and Maturity committee, which provides expertise and guidance on assessment methods for implementing smart manufacturing programs. Focused on gathering industry best practices, the committee plans to generate guides and assistance documents to help assess readiness and implement smart manufacturing. Romano is the director of technology development at The Arthur G. Russell Co. and has been in the process and automation control systems industry for 40 years. After serving as president of an automated machine builder division, he owned a systems integration company. Romano is an industrial advisory board member for two technology and engineering universities, holds an AS, BS, MS, and MBA, and is working on his PhD in technology and innovation.

RESOURCES

The following resources and links will help anyone looking to make the first steps down the Industry 4.0 and digital transformation pathway.

The SIRI Framework
https://siri.incit.org/frameworks-tools

Industry 4.0 Readiness Online Self-Check for Businesses
https://www.industrie40-readiness.de/?lang=en

Using the Industrie 4.0 Maturity Index in Industry
https://en.acatech.de/publication/using-the-industrie-4-0-maturity-index-in-

The Smart Industry Readiness Index: Catalysing the transformation of manufacturing
https://siri.incit.org

"RAMI 4.0 Reference Architectural Model for Industrie 4.0"
https://www.isa.org/intech-home/2019/march-april/features/rami-4-0-reference-architectural-model-for-industr

Transmitting Data at 5G Speeds

By Andy Piatek and Ron Blow

Modern industrial and process automation systems consist of many subsystems and components, including CNC machines, robots, controllers, interfaces, sensors, actuators, and other production assets. To fulfill the manufacturing or processing requirements, these devices must communicate their state and exchange data. That is the function of industrial networks.

Industrial-grade private wireless networks join wired solutions to support advanced applications.

Early industrial networks did not have the need to carry large volumes of data and instead relied on arrays of relays and switches to communicate with motors and other load devices. Over time, the production and processing systems became more advanced and drove the development of complex communication protocols. Today, it is common to see a combination of various transmission methods, including serial, Ethernet, and wireless protocols.

In serial communication, data is transmitted sequentially bit by bit, which translates to very slow transmission speeds; the point-to-point RS-232 standard defined the rate at 1.492 Kbps for up to 15 m (50 ft). The improvement to RS-232 is the multipoint RS-485 standard, which provides communication for fieldbus protocols such as Modbus or Profibus. It delivers 10 Mbps and can support a cable length of up to 1,200 m (4,000 ft).

Ethernet, defined in IEEE 802.3, is commonly used for connecting devices in a wired local area network (LAN) and wide area network (WAN). It is the de facto standard for enterprise networks. Multiple Ethernet specifications define different cable options and speeds, but they all share the same data link format, allowing integration of nodes running different "flavors" of Ethernet.

The implementation of Ethernet for industrial automation is slightly different from what one typically sees in the enterprise space. Here are some of the differences:

- utilization of ruggedized switches, routers, and cables with special connectors to allow the network to function in harsh environments and operating conditions
- typical speeds range from 10 Mbps to 1 Gbps, with 100 Mbps being the most popular
- adaptation of a ring topology for redundancy and quick service restoration; star topology is mostly deployed on the office networks
- implementation of industrial Ethernet protocols, such as EtherNet/IP, Profinet, Modbus TCP/IP, and EtherCAT, to achieve deterministic performance for real-time, critical communication.

Ethernet allows for an integration of operational technology (OT) and information technology (IT) systems and can be a key enabler for innovative use cases such as the Industrial Internet of Things (IIoT).

Wireless technologies

Running traditional field wiring through an industrial facility can be expensive. It is not even possible in some cases. Wireless technology has multiple benefits over wired connections, including cost savings, quick and flexible deployment, and mobility for applications used by plant operators. Several wireless technologies, each suited to certain applications, can be found on the increasingly smart factory floor (figure). Wireless technologies deployed for industrial operations can be divided into three categories based on their role:

- for connecting sensors and field devices, e.g., LR-WPAN, BLE, LPWAN
- for connecting distant parts of the plant, e.g., Wi-Fi, LTE/5G
- for mobility applications used by field personnel, e.g., Wi-Fi, LTE/5G.

Low-Rate Wireless Personal Area Network (LR-WPAN), IEEE 802.15.4, is typically used for low-data-rate monitoring and control applications on devices with low power requirements. Examples of LR-WPANs are ISA-100.11a, WirelessHART, ZigBee, 6LoWPAN, and Thread. Each has advantages, with some offering self-organizing and self-healing mesh architecture and Advanced Encryption Standard (AES) data encryption.

Bluetooth Low Energy (BLE) operates at 2.4 GHz. It is mainly used for low-cost, short-range connectivity for battery-operated devices that do not require high bandwidth. BLE is well suited for connecting remote controls, handheld devices, locks, and smart sensors. Additional benefits of BLE are a near-real-time location tracking and 128-bit AES encryptions.

Low Power Wide Area Network (LPWAN) provides long-range communication at low data rates with very low power consumption (battery life is up to 10 years). It is well suited for machine-to-machine (M2M) communication. Typical applications include smart meters, pipeline monitoring, and various IoT-based solutions for smart agriculture and smart cities.

Wi-Fi, as defined by the IEEE 802.11 family of standards, is widely used by computers, mobile devices, and other devices to connect to the local area network and to the Internet through a wireless router. Wi-Fi operates at either the 2.4- or 5-GHz spectrum, and at 6 GHz for the newest Wi-Fi 6 standard. It offers high data rates up to 600 Mbps for 802.11n, 3.6 Gbps for 802.11ac, and 9.6 Gbps for 802.11ax. Those data rates are the theoretical rates. The real rates are about 50 percent less, but they are still very high for a wireless technology. Wi-Fi was not meant for battery-operated devices, and it is typically used for machine monitoring and connecting the plant floor to enterprise systems.

Both 4G/LTE and 5G have been standardized by the 3rd Generation Partnership Project (3GPP), which unites seven telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC). These standards cover cellular telecommunications technologies, including radio access, core network, and service capabilities, which provide a complete system description for mobile telecommunications. The 3GPP specifications also provide hooks for nonradio access to the core network, and for interworking with non-3GPP networks.

Why industrial connectivity is important now

Plant operators are looking for ways to improve operational efficiency, reduce costs, and increase overall equipment effectiveness through various Industry 4.0 initiatives. Industrial connectivity is the foundation for Industrial IoT solutions. It enables operators to get insights into their production assets to better understand their performance, improve efficiency, and avoid costly downtime. Asset-intensive industries are moving quickly to take advantage of these technologies.

Industrial-grade private wireless networks meet the demands of industry's mission- and business-critical operational

	Wi-Fi	ZigBee	Bluetooth LE	Z-Wave	LoRa	Sigfox	NB-IoT	LTE Cat M1
Frequency	2.4/5 GHz	2.4 GHz	2.4 GHz	900 MHz	sub-1 GHz	sub-1 GHz	GSM/ LTE bands	LTE bands
Data Rate*	up to 10 Gbps	250 Kbps	2 Mbps	100 Kbps	50 Kbps	600 bps	200 Kbps	1 Mbps
Range*	100 m	100 m	100 m	100 m	10 km	50 km	10 km	10 km
Power	High	Low	Low	Low	Low	Low	Low	Low

**optimal conditions*

Several wireless technologies, each suited to certain applications, enable industrial communications.

applications. Critical communications solutions based on industrial-grade private wireless offer many possibilities to power Industry 4.0 use cases in industrial sites, plants, campuses, and wide area networks. Use cases range from machine remote control to cloud robotics, process automation, predictive asset maintenance, assisted/autonomous vehicles, CCTV monitoring, and mission-critical push-to-talk and push-to-video, all on a single network infrastructure.

Trends in industrial connectivity

Recent research from Nokia and ABI Research reports that 74 percent of manufacturing decision makers surveyed plan to upgrade communications and control networks in the next two years to advance digital transformation and Industry 4.0. More than 90 percent are investigating the use of 4G/5G for their operations, and 84 percent of those considering 4G/5G will deploy their own local private wireless network in their manufacturing operations. Additional insights can be found in technology developments. Here are few examples:

Single-pair Ethernet (SPE). SPE offers faster and cheaper Ethernet connectivity with power over data lines (PoDL) to remotely power field devices. The IEEE P802.3cg 10BASE-T1L standard specifies full-duplex transmission over a single pair of conductors at 10 Mbps for up to 1000 m. SPE is much faster than fieldbus and can use the existing single twisted pair fieldbus cable runs—a huge savings.

IEEE 802.3ch supports up to 10 Gbps with a cable length of up to 15 m. SPE meets the requirements of the industrial Ethernet and will be able to support EtherNet/IP, HART-IP, OPC UA, Profinet, and other higher-level network protocols.

Time Sensitive Networking (TSN). The traditional IEEE 802 Ethernet standard is based on the best-effort principle and does not provide the level of determinism required by industrial systems. The transport of critical and time-sensitive control data requires reliable transmission with a defined latency. TSN is a collection of IEEE 802.1 standards developed to address the shortcomings of Ethernet; its main focus is on time synchronization, bounded low latency, reliability, and resource management. TSN allows time-sensitive, critical data to be transported together with best-effort traffic on the same network infrastructure without any concern that critical data gets delayed. Network convergence is possible due to time synchronization and prioritization of data streams implemented by TSN.

Emerging protocols. IoT Analytics cites five trends pushing industrial connectivity forward, and an important one is the development of communications protocols. "IO-Link, OPC UA and MQTT are emerging as the fastest growing I/O, OT and IT protocols, respectively, as vendors and end users alike look to capture richer industrial datasets more efficiently," they say. "A key barrier preventing more widespread adoption of the OPC UA and MQTT protocols is the lack of widely adopted data structure standards." Despite the challenges, industrial connectivity vendors have products that natively support these protocols.

Private LTE/5G. The need to constantly reinvent operations to optimize safety, sustainability, and efficiency has made a compelling case for digitalization and automation in the mining and oil and gas industries and elsewhere. Wi-Fi, WiMAX, and others were not designed for frequently changing environments that need permanent, pervasive, and predictable network coverage. They do not provide the necessary coverage, reliability, mobility, precision, or service prioritization.

Delivering the advanced applications of Industry 4.0 in today's industrial spaces is really only possible with today's 4G/LTE, 4.9G/LTE, and 5G cellular industrial wireless networks. More than 85 percent of digital applications can already run on 4.9 G today. Once the industrial ecosystem has fully developed, the upgrade to 5G will be straightforward.

Release 16 and Release 17 of 5G are bringing critical machine connectivity features, such as ultra-low latency and TSN, which are necessary for Industry 4.0 applications. 5G will bring significant benefits for private wireless, enabling most of the remaining 15 percent of applications not yet possible on private 4.9 G today: applications that need more bandwidth (ultra-high-definition video services) or ultra-low latency for real-time tele-remote control of robots and drones. The 5G release 18 standard, which is due in 2023, should bring the final piece of the puzzle with massive IoT connectivity—the successor to LTE-M and NB-IoT.

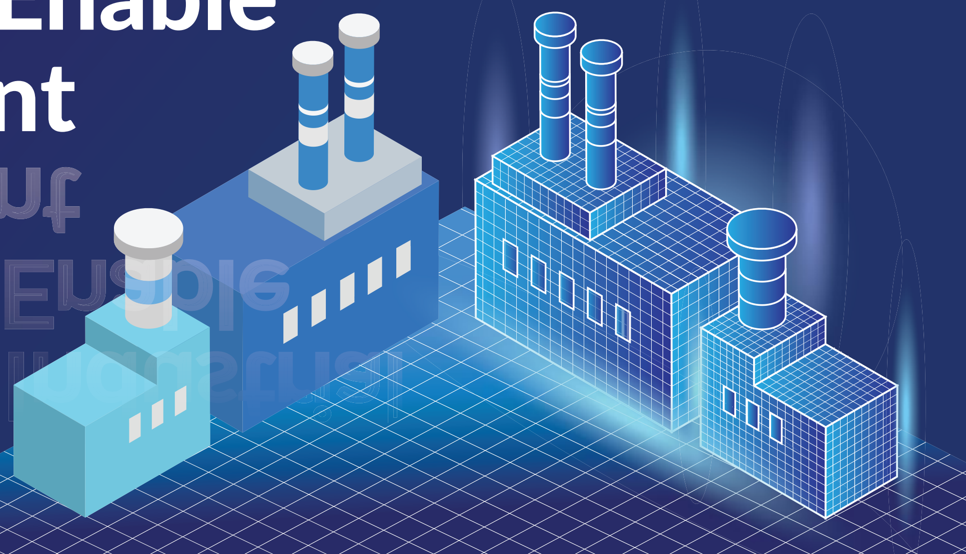
Industrial connectivity supports every Industry 4.0 advanced application and all aspects of the smart plant and smart factory. A private 5G network in particular is a critical enabler of IIoT technologies; it promises reliable, low latency connectivity with better performance, privacy, and levels of security. A private 5G network is the nervous system of any digital factory campus, and it is already showing how it enables machine-to-machine (M2M) communications, smart asset management, facility security, digital twins, and augmented worker applications. Transmitting data at 5G speeds is just the beginning. ■

ABOUT THE AUTHORS

Andy Piatek (andy.piatek@novustechserv.com), is a chair of the Industrial Connectivity committee of ISA's SMIIoT Division, whose aim is to identify emerging technologies in network connectivity and develop guidelines applicable to industrial operations. Based in Canada, Piatek is a digital solutions director at Novus Technical Services. He has a BS in computer science and multiple industry credentials, including CCIE No. 12778, JNCIE No. 523, and CISSP.

Ron Blow (ron.blow@nokia.com) is private wireless regional sales manager – Canada for Nokia. Previously, he worked with enterprise clients in North America designing and optimizing MPLS networks, data centers, and cloud solutions.

Replicating Industrial Systems to Enable Improvement



Digital models, digital shadows, and digital twins help transform and optimize industrial and business operations.

By Juan-Pablo Zeballos Raczy

Digital twins are currently being used in several industries and organizations to design and operate complex products and processes. This technology adoption is massively accelerating process development and optimizing operations, and its success comes from enabling enhanced decision making. In terms of business outcomes, the main results companies pursue through digital twins are increased efficiency, reduced costs, better product design, and boosted innovation.

Before we get to the applications, let's look at some definitions. The International Organization for Standardization (ISO) has developed a digital twin framework for manufacturing where the concept of digital twins is defined as: "A fit-for-purpose digital representation of an observable manufacturing element with a means to enable convergence between the element and its digital representation at an appropriate rate of synchronisation."

This means that a digital twin is a virtual replica of a physical component, product, system, or process within a manufacturing setting. Its function is to reflect the state or performance of the physical object in real time—not to enable further capabilities, such us simulation, orchestration, or prediction—and ultimately support operational decision making.

The digital twin concept comprises three main elements: the physical product, the digital product, and data connecting the two. Depending on the level of data integration, digital twins can be categorized into three subcategories (figure 1):

- A digital model is a digital representation of a physical object without any automated data exchange between the physical object and the digital object. This means that a change in the physical object is not reflected automatically into the digital object and vice versa.
- A digital shadow is a digital representation where an automated one-way data exchange exists, which means that a change in the physical object is reflected automatically into the digital object, but not vice versa.
- A digital twin is a digital representation where

data is fully integrated and flows automatically in both directions between the physical object and the digital object.

A digital twin should not be thought of as a technology but as a composition of different technologies that develop a way of linking the physical and digital worlds. Digital twins can span the entire product lifecycle, from design through simulation, manufacturing, assembly, service, and support.

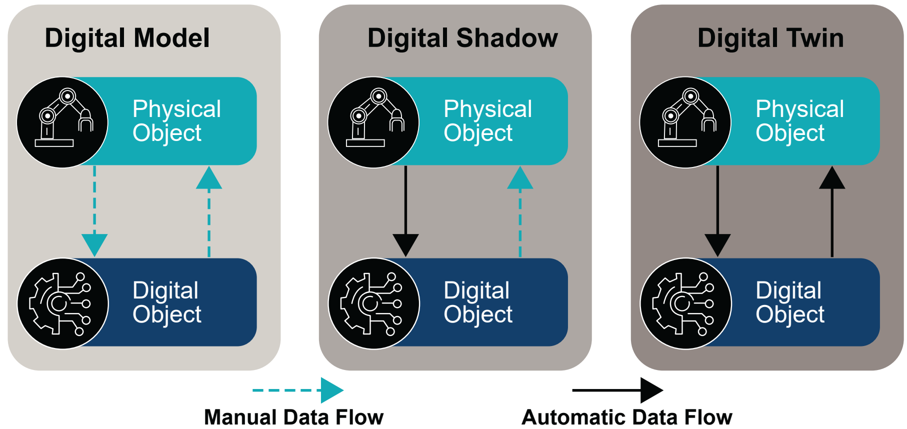


Figure 1. Each type of digital twin involves a different relationship between the physical and digital worlds, and different data flows. *Source: Jeff Winter*

Because digital twins are designed to model complex assets or processes that interact with several components, environments, and unpredictable variables, manufacturers need to have a range of capabilities already in place to deploy them. These include computer-aided design modeling, connectivity, cloud computing, Industrial Internet of Things (IIoT), a variety of different software platforms, augmented reality (AR) and virtual reality (VR) hardware, artificial intelligence (AI) and machine learning (ML), and systems integration.

The challenges associated with digital twin development include data growth, cybersecurity, the extent of digital skills required, and change management. Despite the challenges, the digital twin is quickly becoming a relevant technology, and manufacturers should start thinking of piloting new projects.

Why digital twins are important now

During the past decade, digital twin capabilities have been evolving rapidly because of a series of technology enablers and drivers:

- Access to larger volumes of data and machine learning make it possible to create more detailed simulations with enhanced depth and usefulness of insights.
- Better asset monitoring technologies and new sources of data enable continuous real-time simulations.
- Enhanced industry standards for communications between sensors and operational hardware and diverse platforms have improved interoperability.
- Better data visualization technology (e.g., 3D, VR, AR, AI-enabled visualizations) can handle greater volumes of data.
- Instrumentation is becoming smaller, more accurate, more powerful, and cheaper.
- Compute power, network, and storage are becoming more powerful and cheaper.

It is worth mentioning that a few other key enabling technologies are becoming cost effective and are being adopted: AI, ML, IoT, high-performance computing, cloud computing, and more are what allow digital twins to be so powerful today as opposed to five years ago. Technology companies are significantly investing in improving these digital enablers. Some of these investments are supporting the development of specific digital twin use cases.

Technology vendors have been shifting their attention to developing strong digital twin offerings. In the past few years, several—including IBM, Oracle, SAP, Microsoft, Amazon AWS, Rockwell, Siemens, and GE—have developed and launched digital twin offerings. Some also have made acquisitions to strengthen and build advanced digital twin capabilities.

Digital twin trends and smart factories

Digital twins are being used alongside other Industry 4.0 and smart factory applications in a variety of industries. A growing number of organizations in asset-heavy industries, such as aerospace, automotive, industrial products, and oil and gas, are implementing digital twins to transform their operations. Nonheavy and nonmanufacturing industries in sectors such as consumer goods, retail operations, facility management, health care, and smart cities also are piloting and starting to adopt digital twins.

Other companies are increasing the scale of digital twin deployment, because it provides real business value: It helps companies transform and future proof their businesses to deal with uncertainties and stringent competition. According to Deloitte, digital twin technology can deliver specific business value in the following areas:

- improve quality of product and processes and help predict and detect quality defects quicker
- improve customer service by enabling a better understanding of equipment and determining warranty costs and claim issues more accurately
- reduce operating costs by improving product design, equipment performance, and by streamlining operations and reducing process variability
- create record retention of serialized parts and raw materials to support tracking and quality investigation
- reduce time to market and cost to produce a new product

- by reducing lead times of components and optimizing supply chain performance
- create new revenue growth opportunities by helping to identify new products and improving efficiency and cost to service.

To help understand where digital twins can be used within a smart factory, a framework created by IoT Analytics breaks down the cases and capabilities, using three dominant dimensions: the hierarchical level of a digital twin (six levels), the lifecycle phase in which the digital twin is applied (six levels), and the use or capability of the digital twin (seven levels). An additional fourth dimension can be added that specifies the data type used by the digital twin; this can be real-time, historical, or test data (figure 2). Therefore, according to this framework, there are at least 250 combinations or types of digital twins (6×6×7=252).

One of the best examples of how to implement digital twins in manufacturing to support smart factory initiatives is Unilever. In 2019, Gartner named the consumer goods giant one of the industry's best-performing supply chain leaders.

Unilever implemented digital twins of its manufacturing production line process to increase productivity, reduce waste, and make better operational decisions. Its digital twins are a type described by the IoT Analytics framework as process × operate × orchestrate.

According to a 2019 article in the *Wall Street Journal*, devices send real-time information on physical variables, such as temperatures and motor speeds, into the cloud. Advanced analytics process this data and simulate conditions to ultimately map out the best operational conditions to control and adjust the production process. This results in better quality and productivity. Unilever worked with Microsoft to implement digital twins of dozens of its 300 global plants, and each twin reportedly was implemented in three or four weeks.

Another interesting example is digital twins in the field of maintenance prediction. Using the digital twin, a company can develop predictive maintenance strategies based on the digital replica of a machine or group of machines.

With this technology, maintenance specialists can simulate future operations of the machine, create failure profiles, calculate the remaining useful life of the machine, and plan maintenance activities based on the simulation results. All of this happens without the machine being stopped. The digital twin collects machine data from the machine controller and external sensors; this data is fed into a simulation model that uses algorithms and data analysis technologies to predict the health status of the asset. According to the IoT Analytics framework, this type of digital twin is a product × maintain × predict digital twin.

Digital models, digital shadows, and digital twins are helping transform and optimize industrial and business operations today. Manufacturers that have not started down this path should begin thinking of pilot projects and what is needed to implement the technology. ■

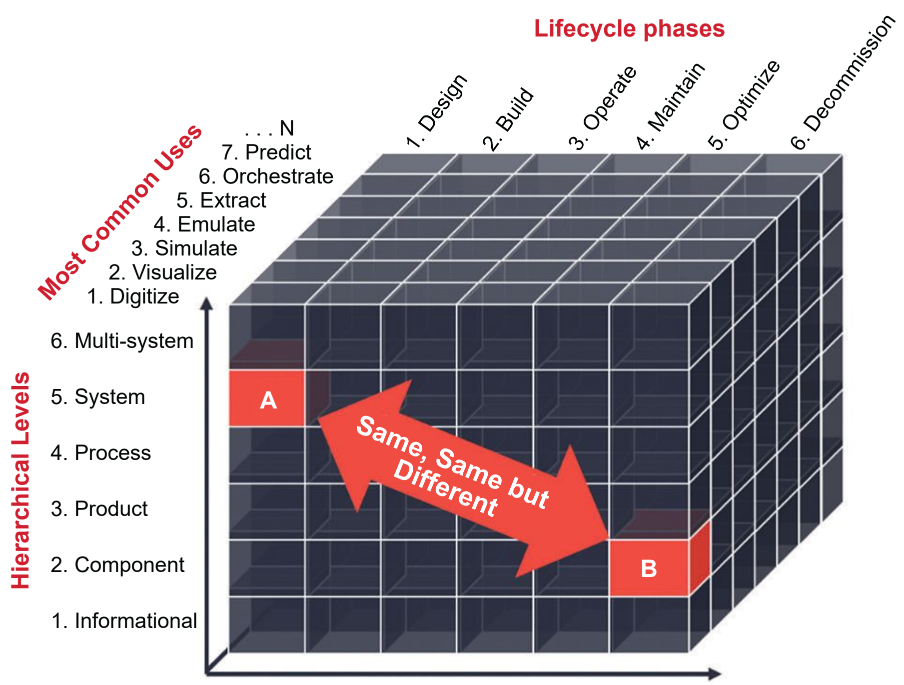
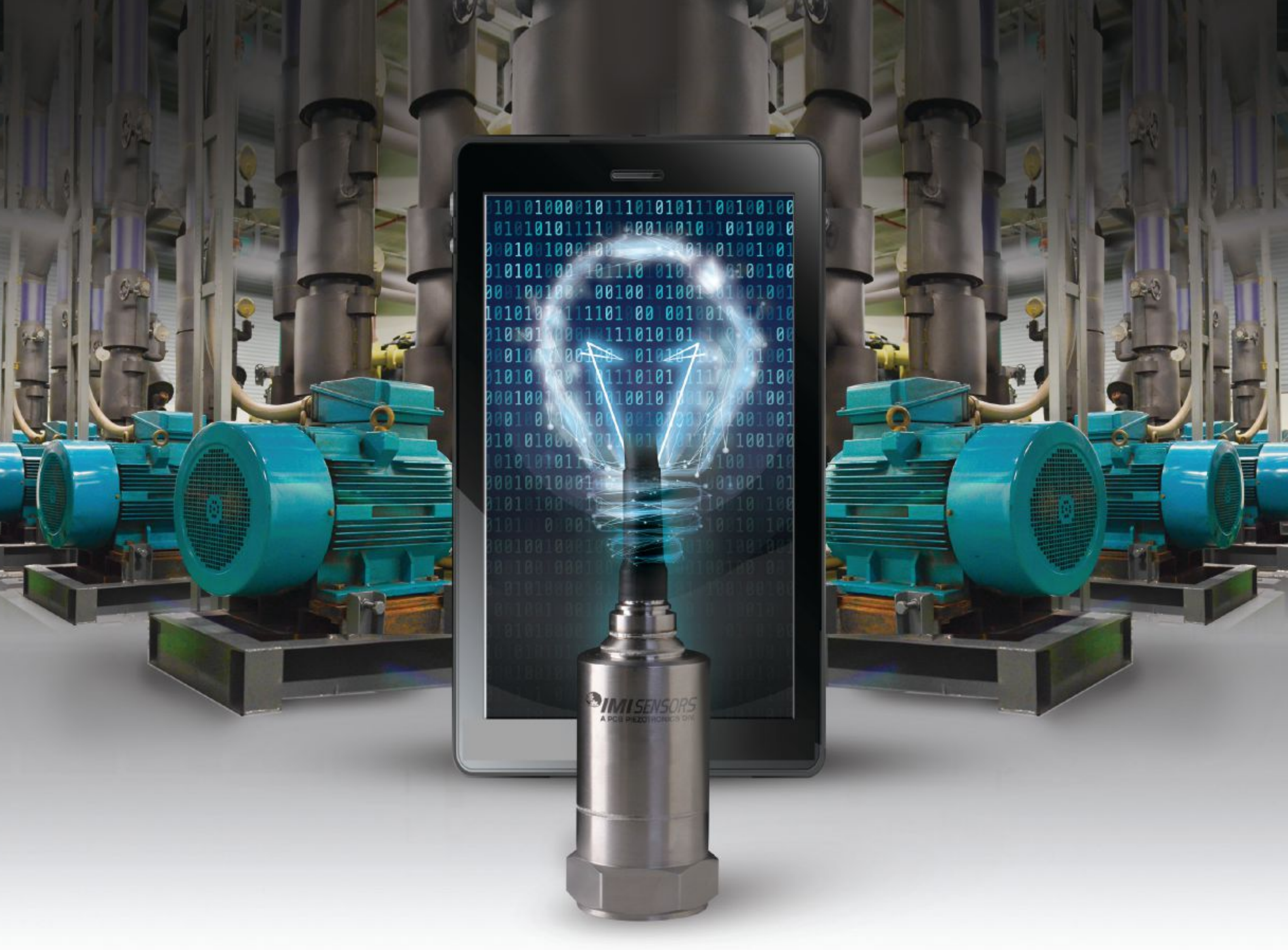


Figure 2. Digital twin classification framework
Source: IoT Analytics research

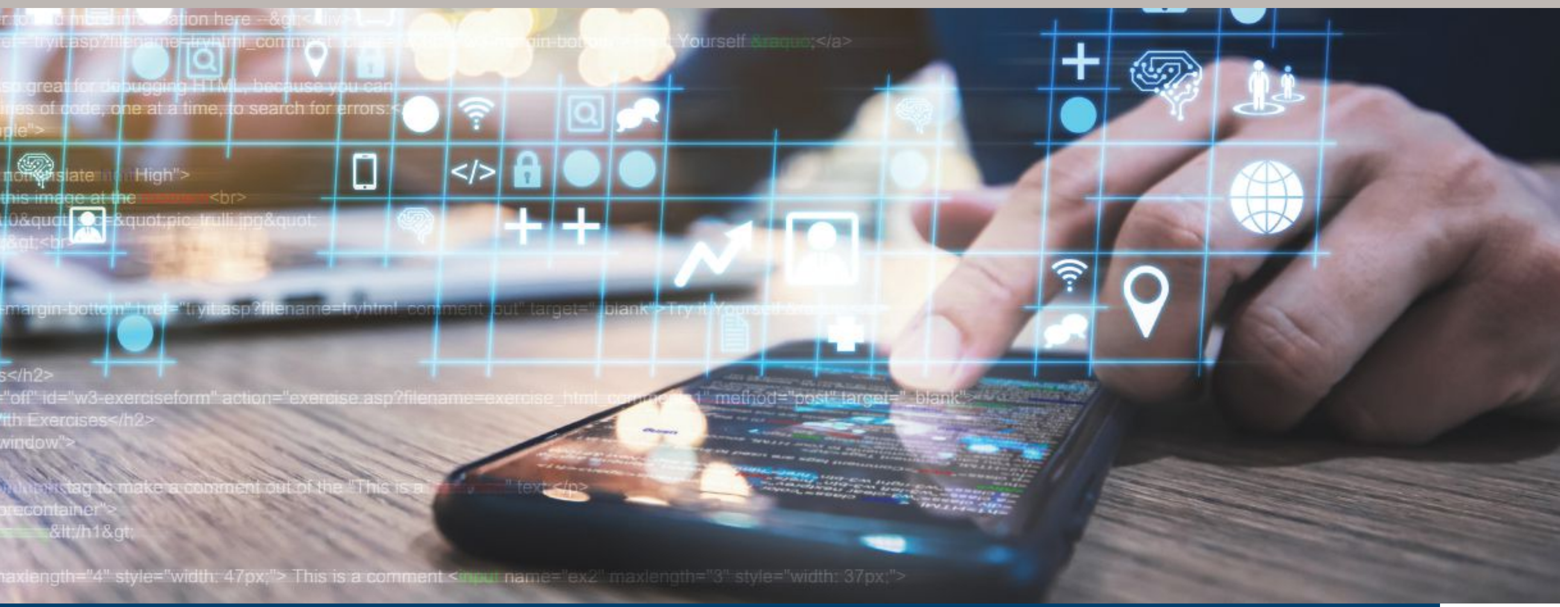
ABOUT THE AUTHOR

Juan-Pablo Zeballos Raczy (jpzeballosr@gmail.com) is chair of the ISA Digital Twin and Simulation committee within the SMIIoT Division. The committee provides expertise and guidance to implement digital twins as part of smart manufacturing programs. Its main focus is on building strong digital twin knowledge with a vision to start developing strategic material to help committee members navigate a digital twin journey: strategy formulation, piloting, implementation, and roll out at scale.

Zeballos Raczy is a senior consultant specializing in digital transformation of manufacturing and supply chain operations leveraging Industry 4.0 technologies. Before transitioning to consulting, he worked for eight years in world-class consumer goods and mining organizations in Latin America. He holds a degree in electronic engineering and an MBA.


IMI SENSORS

Transforming Operations with Data Communications



The smartness of a factory lies in its ability to make optimal and timely decisions.

By Shiv Kataria

The Internet of Things (IoT) is a recent concept that originated out of the advancement and penetration of Internet services. The term IoT was first used by Kevin Ashton in 1999 to promote radio frequency identification (RFID) technology. It means smart devices with some computational capability are connected to the Internet and support sharing data in formats that can be used for further analysis. Day-to-day consumer examples of IoT devices include Alexa smart speakers, connected cars, and smart wearables.

When the application of IoT is extended to industrial use cases, it is called IIoT. It is also sometimes referred to as "industrial Internet" or "Industry 4.0." IIoT originated out of the commercial concept of the Internet of Things and the advancement and penetration of Internet services within industrial environments. The term "industrial Internet" reportedly was coined by GE for the convergence of critical assets, advanced predictive and prescriptive analytics, and modern industrial workers.

IIoT is a network of smart sensors, actuators, and systems using communication technologies that help in the real-time analysis and communication of data produced by the devices in the factories or field. The ability to gather real-time data enables monitoring, exchange, and analysis of the data for meaningful insights. These insights are harbingers of smarter and faster business decision making for manufacturing organizations.

In general, an IIoT ecosystem consists of the following (figure 1):

- connected smart devices that gather and communicate over a network
- a public or private communications infrastructure
- processes that analyze the data gathered by smart devices and produce business use information
- data storage that houses data in a central location
- people that consume the information to make informed decisions.

IIoT enables the true convergence of information technology (IT) and operational technology (OT). The smart edge devices in the field or factories communicate the captured data intelligently over the communication infrastructure. The data is consumed to drive actionable information and trend analysis for machinery. The analyzed information supports informed decision making for predictive maintenance, safety, security, and business optimization.

An IIoT system with IT-OT convergence can be seen as a layered modular architecture of digital technology (figure 2). It can be divided into four technology layers:

- Content layer: People-interface devices like computer screens, tablets, smart glasses, and smart surfaces
- Service layer: Applications and software to analyze data and transform it into actionable, insightful information
- Network layer: Communication infrastructure such as Wi-Fi, Bluetooth, LoRa, 4G/5G cellular, and other methods that send and receive the data
- Device layer: Smart edge devices, cyber-physical systems, sensors, actuators, and machines.

Trends and standards

The growing adoption and multitude of players in the IIoT space has necessitated the development of standards. In 2020, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) jointly released three IoT standards:

- ISO/IEC 21823-2 specifies a framework for transport interoperability to enable information exchange within and between IoT systems.
- ISO/IEC TR 30164 describes the concepts, characteristics, and technologies of edge computing for IoT systems applications.
- ISO/IEC TR 30166 applies to IIoT systems and landscapes.

In addition, the Industrial IoT Consortium has developed several volumes of architecture and specifications for IIoT. Sixteen consortia and associations and 17 standards development organizations are helping to define and standardize the IIoT environment.

An abundance of communication standards frameworks also exist. These include: MQTT, a bidirectional TCP/IP–based publish-subscribe communication protocol; REST, a scalable Hypertext Transfer protocol used for edge-to-cloud communication; NodeRED, an open-source platform developed by IBM to connect APIs, hardware, and online services; OPC, a series of standards developed by the OPC Foundation for industrial communication to connect controllers with computers and the cloud; Chatty Things, an open framework being developed by XMPP Standards Foundation for scalable IIoT infrastructure; Cognitive IoT, a framework being developed by IBM that combines IoT with machine intelligence, contextual information, and learning using natural language processing; and Mindsphere, a cloud-based platform developed by Siemens to integrate IoT edge devices, applications, and services in one place.

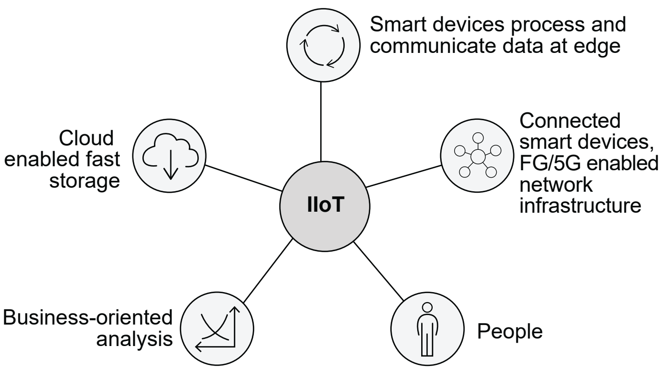


Figure 1. Industrial Internet of Things

These standards and frameworks are shaping the IIoT landscape, as are Industry 4.0 reference architectures being developed around the world. Industrial Internet Reference Architecture (IIRA), the German Industrie 4.0, and the RAMI model are all independent efforts to create a defined standard for IIoT-enabled facilities.

Why IIoT is important now

IIoT has affected the industrial sector significantly and brought many benefits to digital manufacturing. The advancement in IoT technologies and the availability of the Internet has helped other advanced technologies, such as cloud computing, big data analytics, and artificial intelligence/machine learning, penetrate the industry. This has comprehensively contributed to a robust infrastructure for cyber-physical systems. The traditional industrial systems like supervisory control and data acquisition and distributed control systems have improved in monitoring, performance, productivity, and, more importantly, in efficiency with the advent of IIoT, contributing to the profitability of organizations.

The convergence of the physical devices over network infrastructures with smart edge devices, real-time analysis of data from the production process, visibility into process parameters, control of processes, and data exchange have all improved significantly. Overall, IIoT has enabled data-driven decision making and positively affected the accuracy and predictability of these decisions in industrial environments.

Trends and benefits enabled by IIoT

Digitalization enabled by IIoT has been increasing rapidly during the past decade. According to a survey conducted by statista (https:\www.statista.com\statistics\611004\global-industrial-internet-of-things-market-size) in 2020, the global market for IIoT was more than 263 billion USD. The market is expected to grow to some 1.11 trillion USD by 2028.

During the COVID pandemic, the adoption of IIoT-enabled technologies increased significantly. The remote work requirements were a push factor of this adoption. The focus of IIoT implementation in recent years has been workforce management initiatives, automation, and customer experience improvements.

The advanced applications brought about by the proliferation of IIoT technology is the most significant trend associated with IIoT. This list was compiled by ATS (https://www.advancedtech.com/blog/iiot-trends):

- Remote monitoring and operation: The advantage of sensor-based data analytics is to access data and devices on demand.
- Edge sensor advances: The edge capability and penetration of 4G/5G communications have enabled faster communication and robust sensors.
- Predictive analysis: Data-driven trend analysis has improved on-time maintenance, reducing downtime and increasing production.
- Digital twins: Smart sensor data feeds into digital twin models and makes remote monitoring and management more reliable and efficient.
- Health and safety: IIoT-driven technologies contributed to health and safety, especially during the pandemic time in 2020–21. Employee locations on the facility floor, tracking of close contacts, and temperature recording all contributed to safe and healthy work environments.
- Agile and flexible infrastructures: IIoT advances provide unprecedented flexibility in areas such as supply chain, so manufacturers can be agile in supplier selection, ordering and procurement strategy, and inventory management.
- Smart factory: Increased penetration and use of 5G wireless communications within factories is taking digital manufacturing in new directions. Smart factories are a reality in 2022.
- Data analysis at the source: The abundance of data generated by the smart edge devices makes it important to analyze the data at the source in a timely manner. Factories are changing their technical architecture, bringing data analysis and artificial intelligence (AI) technology out to the "edge" to take full advantage of the IIoT ecosystem.

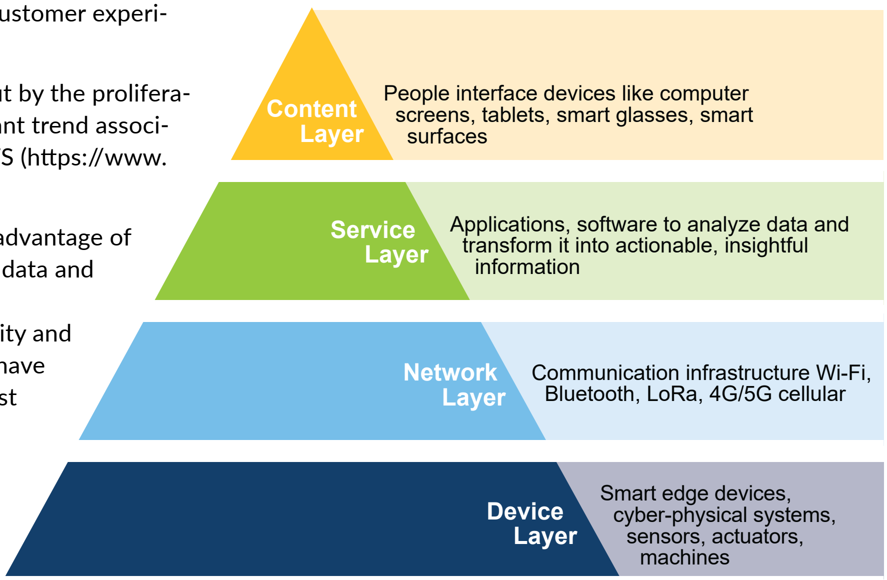


Figure 2. A layered modular architecture of digital technology

The integration of IT and OT, increased speeds of Internet and communication technologies, and fast data analysis have supported the conversion of digital factories into smart factories. IIoT platforms integrate IT functions with OT functions and transform factory floor operations. The legacy machines and sensors are being integrated with the IT systems, and edge intelligence has been introduced. Lately, 5G penetration has accelerated this transformation by eliminating cabling and enabling ultrareliable, mission-critical wireless communications.

The smartness of a factory lies in its ability to make optimal and timely decisions. Humans may or may not be part of such decisions. IIoT makes highly advanced technologies possible. For example, companies are adopting robotics and unmanned autonomous vehicles at deeper levels to augment or replace human workloads. Machine learning and artificial intelligence is being used to analyze data gathered by sensors and monitoring devices to make real-time decisions and improve the efficiency of production.

The huge operational advantages of smart factories are beginning to be realized as the pace of AI-driven process intelligence, blockchain-enabled supply chain management, and crypto-enabled edge security picks up. In the next few years, we will see the true transformation of factories as technologies like digital twins, the industrial metaverse, token-based economies, and algorithmic trust are enabled by lightweight edge computing. IIoT enables all that and more. ■

ABOUT THE AUTHOR

Shiv Kataria (shiv.kataria@siemens.com) has been associated with ISA since 2019 and currently leads the IIoT committee within ISA's SMIIoT Division. One of the focuses of this committee is to document best practices and frameworks and share the knowledge throughout the automation community. The use cases shared by the committee are from professionals working in IIoT areas who have been implementing IIoT for the digitalization of factories. Kataria is a research professional with Siemens Cybersecurity and Trust Research India. He has been working in and with industrial security, digital factories, and critical information infrastructures for 15 years. A large part of his career was with the government of India. He is an electronics and communication graduate and holds certifications including CISSP, ISA/IEC 62443 Cybersecurity Expert, CEH, and ISMS 27001.

Making Best Use of Computing Resources Wherever They Are

By Ryan Treece

Manufacturing processes have become extremely complex. One manufacturing line can generate hundreds of thousands of data points from various sensors, programmable logic controllers, motors, motion drives, and other devices. The data points for each device are often only used once for a small task within a larger process, with the data overwritten during each machine's cycle. Communicating across hundreds of different proprietary protocols over wired networks to access and send that data to a centralized system for filtering and analyzing has been a challenge.

Enter the Internet of Things (IoT) and cloud and edge computing. These information technology (IT) concepts enable distributed network architectures by moving data and computing tasks normally processed in a centralized location to the cloud or to the edge of the network. IoT edge technology decentralizes data processing and storage by performing various functions at the edge of a network, closer to individual devices and machines.

Supported by wireless communication including 5G, cloud and edge computing bring IT expertise to the smart factory.

Edge computing brings the advantages and power of cloud computing closer to where data is created and acted upon to improve efficiency, security, or compliance. Edge devices and sensors are where data is generated and collected, but they do not always have the compute and storage resources needed to perform advanced analytics.

Edge computing is used on premise in facilities to handle real-time data processing for important smart factory applications like predictive maintenance. Cloud computing, on the other hand, is done in a remote environment hosted by public cloud companies like Microsoft, Amazon, or IBM to support more data-intensive and less time-critical processes.

According to *Forbes*, public cloud providers are increasingly focusing on a hybrid cloud model. Hybrid cloud computing allows manufacturers to store and analyze their proprietary internal process information locally on their own servers, while offloading resource-intensive applications like machine learning to a public cloud to take advantage of scale and cost efficiencies.

Combining edge computing with 5G will allow more flexibility in on-premise deployments by extending the range and reach of data collection to assets normally unreachable through wired deployments or bandwidth constraints.

Private cloud architectures exist too, in which an industrial company's IT department handles its own cloud storage for data like production recipes, customer information, or even process knowledge of each product being manufactured. Public clouds are most effective in terms of cost per compute and long-term storage. They may be used for applications like storage of machine schematics, computer-aided design drawings of parts or machines, and other information that is not critical or time sensitive.

Why edge and cloud are important now

According to IoT Analytics, the number of connected IoT devices is expected to reach 14.4 billion by the end of 2022. Allied Market Research states that the global value of IoT in manufacturing products was $198.25 billion in 2020, with predictive maintenance applications commanding the largest share. Thanks in large part to advancements in smart sensors and virtual and augmented reality, the demand for real-time asset monitoring will boost the overall value to $1,495.65 billion by 2030, at a compound annual growth rate of 22.6 percent from 2021.

With exponentially more IoT devices collecting, analyzing, and processing more data and information, the need for edge computing can only increase in an effort to reduce latency and increase speed. With the edge orchestrating, aggregating, and trimming data on the fly, companies will rely upon the cloud for long-term storage and cost-efficient compute. The toughest decision corporations will face is choosing which data points are worth real-time analysis on premise, which need long-term storage and analysis in the cloud, and, most importantly, which data needs no analysis at all.

Private 5G networks and other trends

Many experts believe enterprises will deploy edge platforms and 5G wireless communications together in the coming years. A recent article from The Enterprisers Project indicates that the "next big thing" will be private 5G networks. 5G adds ultrareliable, low-latency communication (URLLC) that has previously only been offered on Class-C Ethernet technology.

With the increased data transfer speeds, decreased latency, and higher capacity of 5G technology, factories will be able to scale without relying on proprietary Industrial Ethernet protocols via standard wired network infrastructures. Combining edge computing with 5G will allow more flexibility in on-premise deployments by extending the range and reach of data collection to assets normally unreachable through wired deployments or bandwidth constraints.

Another trend is the need for faster and more agile cloud deployments. The Gartner Research (https://www.gartner.com/en/doc/753853-2022-planning-guide-for-cloud-and-edge-computing) *2022 Planning Guide for Cloud and Edge Computing* stresses the importance of "cloud teams" that play an important role in supporting CIO- and executive-driven initiatives to accelerate cloud deployments. Speed of deployments through business agility and ability are the cornerstones of deploying effective cloud solutions.

Cloud teams must have more than architecture and technical ability; they need to understand the overall business and business challenges they are addressing. If teams are too slow to adopt, they may never catch the moving target of digital transformation. If teams do not understand the core challenges or reasons behind the digitization of a project, their solution may not be adaptive enough in future improvements and require more nonrecoverable engineering costs.

Cloud and edge support for OEE

Factories deploying edge platforms experience faster network speeds and low latency, which contribute significantly to better decision making and production optimization. This ultimately improves return on investment. Using edge and cloud computing, manufacturers are improving productivity and identifying revenue opportunities from the efficiencies and capabilities of smart systems. In particular, real-time overall equipment effectiveness (OEE) visualization tools provide full visibility into every aspect of a factory's efficiency.

OEE was invented in the 1960s by Seiichi Nakajima, the founder of the Total Productive Maintenance (TPM) system. OEE is a key performance indicator calculated to measure machine and overall manufacturing performance. It is not a static, individual measurement of success, failure, or mediocrity, but rather a living metrics combination that points operational technologists to the levers they must pull to improve business performance.

The first and most common challenge for an effective OEE implementation is data collection. Good data analytics start with good data availability. For manufacturing environments that use hundreds of types of machines and gather data from multiple industrial protocols, real-time data collection from machines it critical. Advanced industrial IoT data management edge platforms provide this. Most offer core capabilities that include:

- real-time access to operational data
- data rationalization to identify relevant points
- data transformation into usable formats
- speedy delivery for ingestion by cloud and middleware OT and IT systems.

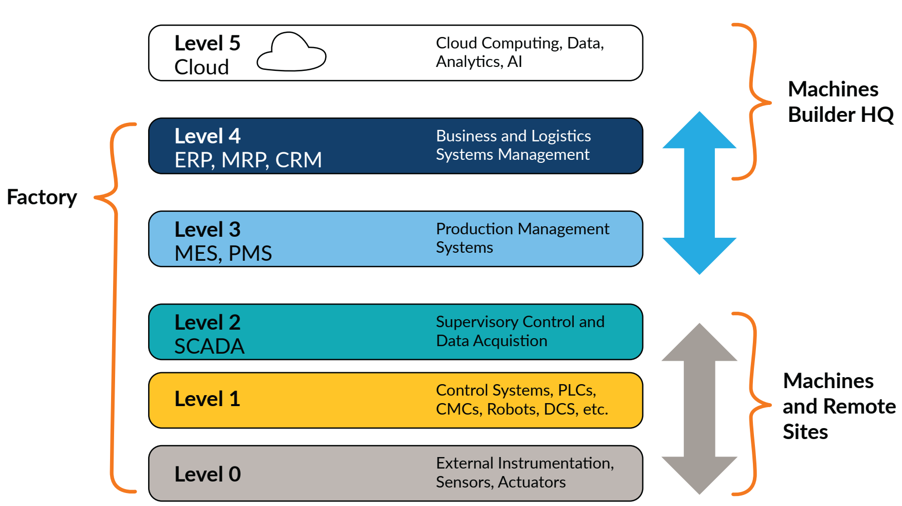
Inherently, edge computing is done at or near devices and offers more security, lower latency, and more bandwidth capacity and reliability than cloud services. The most efficient IIoT edge platforms for data management include a large library of protocol converters enabling machine data collection using open and private protocols such as OPC UA and OPC DA, Modbus, MTConnect, BACnet, and Siemens. For networked machines, the edge makes data collection a simple process, particularly for choosing the driver and appointing it to the IP address. All the tags are auto-enumerated.

For machines requiring analog or digital I/O data collection or external instrumentation, edge platforms can collect data from sensors or from a hardware adaptor for legacy machines.

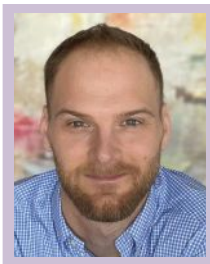
With the machines connected, algorithms can be set up by mapping the variables to a trigger. The logic was previously written in traditional programming languages, however newer platforms provide a low- or no-code environment for a visual logic workflow to facilitate application creation, maintenance, and calculations. OEE calculations can be done machine by machine and consolidated by line, shift, and plant level to improve management visibility. Alarm functions for monitoring specific machine and process conditions can be added and customized to automated actions.

With robust OT/IT edge integration software, it is possible to automate machine setup and reduce setup time, as the software's low latency is critical to avoid hidden downtime in the machine. With improved process visibility, managers have better information for planned stops and can calculate the machine OEE and schedule maintenance based on machine information.

Every manufacturer knows that unscheduled downtime is expensive. If one machine component fails, it can halt the entire production system, resulting in the loss of production time, raw materials, and more. Edge platforms can be deployed to learn expected machine behavior and fully automate preventive maintenance with triggers identifying anomalies in the production cycle, such as power consumption, vibration and noise, and temperature. Given that the most common challenge for smart factories is usually interoperability with infrastructure implementation, it is well worth prioritizing IIoT architecture that uses edge intelligence to integrate legacy machines and sensors into IT systems. ■



Edge computing brings the advantages and power of cloud computing closer to where data is created and acted upon.



ABOUT THE AUTHOR

Ryan Treece (Ryan.Treece@telit.com) is chair of the Edge & Cloud committee within the SMIIoT Division of ISA. The committee's goal is to combine members' skills and expertise to educate others to improve manufacturing processes, automate predictive maintenance, and leverage embedded IIoT sensors to tackle large problems. Ryan is currently business development manager for industrial IoT at Telit, within its Platforms division. He works with senior leadership at global manufacturers to identify opportunities, and leads teams to deliver Industry 4.0 solutions.

The Marriage of Digital Factories and Cybersecurity

By Jacob Chapman and Danielle Jablanski

Cybersecurity for OT and IoT is a field of study and practice to prevent the unauthorized access, manipulation, and disruption of operational technologies (OT) and industrial and consumer Internet of Things (IoT) devices and platforms. New emphasis is now being placed on reducing incident severity across sectors that deploy these technologies, tapping into the strong safety culture throughout industrial environments.

Monitoring smart systems and managing risk become more essential as connected systems proliferate.

The ISA/IEC 62443 series of standards—which focuses exclusively on industrial automation and control systems—succinctly defines the term security as the "condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss."

There has been an increase in cybersecurity incidents, both those that are financially motivated and those primed to cause physical disruption, using both OT- and IoT-specific vectors and malware. Strategies for securing OT and IoT have traditionally deployed defense-in-depth approaches. Defense in depth is a strategy with various methods for introducing stop gaps for security across an organization, layering controls in a way that crosscuts people, technology, and processes and relies on tools and policies that ensure robust and redundant protection. Tools and policies may include endpoint security, access controls, segmentation, network monitoring, anomaly detection, patch management and allow listing, and additional cybersecurity solutions depending on the type and complexity of an organization, its assets, and its networks.

Admittedly, cybersecurity is a large, complicated—and intimidating—subject that is further complicated by its many interactions with adjacent subjects. Visualizations of what the subject includes take many forms. One particularly popular mind map was developed by Henry Jiang (https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang) and improved over four years. Another popular graphic from Momentum Cyber (https://momentumcyber.com/docs/CYBERscape.pdf) categorizes the hundreds of tools that target various security needs and specialties, such as data, endpoint or application security, risk and compliance, and incident response. Interestingly, only a fraction of those tools—probably less than 10 percent—focus on OT and industrial control systems today.

At its roots, OT and IoT cybersecurity is an accidental by-product of Industry 4.0. The fourth industrial revolution, characterized by the real-time optimization benefits that connected systems provide to a business, has driven IT/OT convergence and exposed vulnerable OT and IoT systems. As technologies that help businesses realize the benefits of connectivity mature, so does the increase in risk. Put another way, the more important digital factories become, the more important OT and IoT cybersecurity becomes; the two are married.

In fact, cyber risk has been increasing so quickly that the federal government, insurers, cybersecurity professionals, and asset owners alike are struggling to keep up. On 7 May 2021 the U.S. suffered the largest attack to date on its critical infrastructure: the Colonial Pipeline ransomware attack, which shut down its pipeline system for five days—the first time it had done so in its 57-year history. The very day operations resumed, President Biden issued an executive order specifically referencing operational technology security, elevating the topic's attention internationally.

Threat actors are doing their homework and learning more about the purpose-built nature of OT and industrial IoT operations, meaning that unauthorized access is more dangerous than ever.

From a legal perspective, courts are evaluating responsibility for cybersecurity incident liabilities. When Merck was affected by the 2017 malware attack known as NotPetya—which was deployed by Russia with Ukrainian companies as its primary target—Merck's insurers famously declined the insurance claim by citing a policy exclusion for acts of war. However, in January 2022, a New Jersey Superior Court judge ruled that the exclusion cannot be used. This ruling will certainly cause actuarial calculations to change, further accelerating the already increasing premiums for cybersecurity insurance policies.

The Colonial Pipeline attack and major shifts in legal and liability rulings are just two examples showing that there has never been a moment of more rapid change within the OT and IoT cybersecurity space than today. And from an asset owner's perspective, the business risks associated with OT and IoT cybersecurity have never been higher.

In OT and IoT, different systems are responsible for performing functions, controlling functions, monitoring functions, and analyzing functions, traditionally designed with mission state and continuity in mind. The evolution of the technologies we care about in OT began with on-premise connectivity between systems, often using Ethernet, to connecting multiple sites and often remote locations, to the expansion of supervisory control and data acquisition architectures. They are increasingly adopting cloud technologies. These systems are deployed and configured without visibility into the communications and data patterns that power their operating status, resulting in limited information to investigate and understand the root cause of a cybersecurity incident or data management accident.

The Industry 4.0 push for intelligence and the crunching of more data has led to the development of IoT solutions that require massive amounts of asset intelligence and data that few spend the resources to understand and maintain from a security perspective. With this landscape, the continued overlap of IT and OT, and the rapid expansion of smart devices for industrial and consumer use, asset owners are often left in the dark about how to address security concerns and mitigate risks.

It is clear that the technology available and the activities required to secure computer systems are enormous, but what may not be clear is how OT and IoT cybersecurity relates to cybersecurity generally. Is OT and IoT cybersecurity a subset of a broader cybersecurity space as some suggest, or is it entirely different?

The answer: OT and IoT cybersecurity is the practice of cybersecurity applied to OT and IoT systems. In some areas, securing OT and IoT systems is the same as traditional IT systems. Identical tools and processes can be leveraged. In other areas, they are entirely different, requiring specialized tools, protocol expertise, and tailored methodologies.

Trends in OT and IoT cybersecurity

On 24 February 2022, Russia began its invasion of Ukraine, which has affected international markets, foreign policy, and cybersecurity. The Cybersecurity & Infrastructure Security Agency (CISA) issued a "Shields Up" advisory as a direct response to the increased cyber risk. New strains of destructive malware (https://www.cisa.gov/uscert/ncas/alerts/aa22-057a)—which leave devices permanently destroyed with no means to recover—have been detected in Ukraine, including WhisperGate, HermeticWiper, IsaacWiper, HermeticWizard, and CaddyWiper. Worse, it has been reported that the malware has been detected on U.S. building automation system networks, a clear example of the risks to third-party OT/IoT asset owners when distant warring nations engage in cyberattacks.

There has been a full realization that operations that tolerate little to no physical downtime are lucrative targets. Threat actors are doing their homework and learning more about the purpose-built nature of OT and industrial IoT operations, meaning that unauthorized access is more dangerous than ever. Recent attacks have focused on three relevant trends:

- targeting centralized control and management capabilities as a single point of failure
- achieving longer dwell times, i.e., doing extra work to go undetected for longer periods
- increased understanding of OT and IoT operations to disguise manipulations as legitimate activity.

Within the technology space, OT-specific security tools continue to grow and gain popularity. OT cybersecurity pundit Dale Peterson recently posted a blog article stating that "the first OT security product segment to have a company, actually multiple companies, valued over $1 billion is OT detection."

History demonstrates that the cybersecurity vendor market is extremely dynamic; over the past year, FireEye (products) and Mandiant (services) split, followed by an acquisition of Mandiant by Google for $5.4 billion. Such major merger and acquisition activity is part of a larger trend in surging merger and acquisition volume. We can expect this to continue, with OT and IoT cybersecurity software tools changing corporate ownership and growing in complexity and company valuation.

From a technical perspective, providers and asset owners are increasingly adopting cloud hosting as a part of their strategies. Nozomi Networks, for example, released Vantage, a cloud-based software as a service platform for OT and IoT security monitoring in 2020. Other tools, including Armis, MediGate, and many IT-oriented cybersecurity tools, also use a cloud-centric platform for security monitoring. As asset owners demand greater scalability and advanced analytics of enterprise-wide security data for insights, cloud platforms will continue to gain in popularity across all OT and IoT verticals.

Securing smart factories

Factories are historically data-rich but information-poor ecosystems. As the benefits of a smart factory drive more and more connectivity and intelligence drives innovation, the reality is that cybersecurity risks will grow. All smart factory initiatives must include a strategy for appropriately managing the risk to the business to a tolerable level, plain and simple.

To do this, organizations are increasingly investing in a security operations center (SOC) that monitors logs and events within their IT environments and OT environments in one location. Security information and event management (SIEM) and security orchestration, automation, and response (SOAR) tools are typically used to do this.

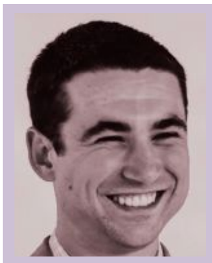
In effect, logs and events are aggregated from OT, IoT, and IT security tools into a single location, where analysts can continually monitor for suspicious activity. Or, after an incident has occurred, logs can be correlated, and a narrative can be built to understand how the incident occurred.

In the case of a SOAR, the tool may be enabled to automatically take preventive action when certain logs and events are seen. In some cases, additional software platforms are included in the mix, such as threat intelligence platforms to keep the team informed of the latest threat signatures and malicious activity occurring throughout the world.

Unfortunately, the investment required to deploy an SOC is massive. It is further complicated by the shortage of cybersecurity talent globally as well as by the realization that a security operation center alone is not sufficient. Instead, asset owners small and large are turning to managed security service providers (MSSPs) that integrate tools deployed within the asset owner's environment into the MSSP's SOC. In fact, Forbes published that the MSSP market is expected to reach $40.97 billion this year, based on Allied Market Research's 10-year report. The trend toward SOCs, and outsourcing to MSSPs, is here to say.

Beyond traditional security monitoring, the OT and IoT environment is unique in that the underlying control systems are controlling a physical process. OT monitoring tools take advantage of this by not only alerting on known malicious signatures, but also by monitoring the process variables themselves and alerting on anomalies.

Stay tuned for how this marriage between smart factories and cybersecurity responses continue to evolve. ■



ABOUT THE AUTHORS

Jacob Chapman (jacob.d.chapman@icloud.com) is the Cybersecurity committee chair of ISA's Smart Manufacturing & IIoT Division, whose focus is OT cybersecurity as a part of smart manufacturing, leveraging ISA99 and the Global Cybersecurity Alliance (GCA). He is a registered U.S. expert to TC65 of the IEC, member of Manufacturing Enterprise Solutions Association's Cybersecurity Workgroup, and a member of the ISA99 standards development committee. He is also solutions architect, BD and Alliances, for Nozomi Networks.

Danielle Jablanski is president of the North Texas Section of ISA, OT cybersecurity strategist for Nozomi Networks, and a nonresident fellow at the Cyber Statecraft Initiative of the Atlantic Council's Scowcroft Center for Strategy and Security. She serves as a staff and advisory board member of the nonprofit organization Building Cyber Security. She holds a master's degree in international security from the Josef Korbel School of International Studies at the University of Denver and a bachelor's degree in political science from the University of Missouri – Columbia.

Enhancing Human Effort with Intelligent Systems

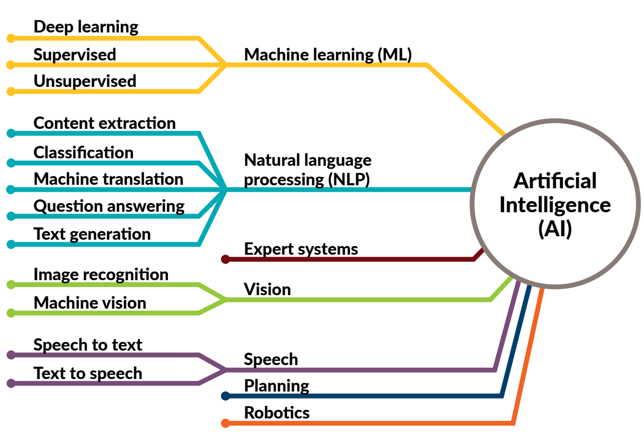
Artificial intelligence has come a long way since scientists first wondered if machines could think.

By Ines Mechkane, Manav Mehra, Adissa Laurent, and Eric Ross

In the 20th century, the world became familiar with artificial intelligence (AI) as sci-fi robots who could think and act like humans. By the 1950s, British scientist and philosopher Alan Turing posed the question "Can machines think?" in his seminal work on computing machinery and intelligence, where he discussed creating machines that can think and make decisions the same way humans do (reference 1). Although Turing's ideas set the stage for future AI research, his ideas were ridiculed at the time. It took several decades and an immense amount of work from mathematicians and scientists to develop the field of artificial intelligence, which is formally defined as "the understanding that machines can interpret, mine, and learn from external data in a way that imitates human cognitive practices" (reference 2).

Even though scientists were becoming more accustomed to the idea of AI, data accessibility and expensive computing power hindered its growth. Only when these challenges were mitigated after several "AI winters" (with limited advances in the field) did the AI field experience exponential growth. There are now more than a dozen types of AI being advanced (figure).

Due to the accelerated popularity of AI in the 2010s, venture capital funding flooded into a large number of startups focused on machine learning (ML). This technology centers on continuously learning algorithms that make decisions or identify



Areas within AI (reference 3)

patterns. For example, the YouTube algorithm may recommend less relevant videos at first, but over time it learns to recommend better targeted videos based on the user's previously watched videos.

The three main types of ML are supervised, unsupervised, and reinforcement learning. Supervised learning refers to an algorithm finding the relationship between a set of input variables and known labeled output variable(s), so it can make predictions about new input data. Unsupervised learning refers to the task of intelligently identifying patterns and categories from unlabeled data and organizing it in a way that makes it easier to discover insights. Lastly, reinforcement learning refers to intelligent agents that take actions in a defined environment based on a certain set of reward functions.

Deep learning, a subset of ML, had numerous groundbreaking advances throughout the 2010s. Similar to the connections between the nervous system cells in the brain, neural networks consist of several thousand to a million hidden nodes and connections. Each node acts as a mathematical function, which, when combined, can solve extremely complex problems like image classification, translation, and text generation.

Impact of artificial intelligence

Human lifestyle and productivity have drastically improved with the advances in artificial intelligence. Health care, for example, has seen immense AI adoption with robotic surgeries, vaccine development, genome sequencing, etc. (reference 5). So far, the adoption in manufacturing and agriculture has been slow, but these industries have immense untapped AI possibilities (reference 6). According to a recent article published by Deloitte, the manufacturing industry has high hopes for AI because the annual data generated in this industry is thought to be around 1,800 petabytes (reference 7).

This proliferation in data, if properly managed, essentially acts as a "fuel" that drives advanced analytical solutions that can be used for the following (reference 8):

- becoming more agile and disruptive by learning trends about customers and the industry ahead of competitors
- saving costs through process automation
- improving efficiency by identifying processes' bottlenecks
- enhancing customer experience by analyzing human behavior
- making informed business decisions, such as targeted advertising and communication (reference 9).

Ultimately, AI and advanced analytics can augment humans to help mitigate repetitive and sometimes even dangerous tasks while increasing focus on endeavors that drive high value. AI is not a far-fetched concept; it is already here, and it is having a substantial impact in a wide range of industries. Finance, national security, health care, criminal justice, transportation, and smart cities are examples of this.

AI adoption has been steadily increasing. Companies are reporting 56 percent adoption in 2021, an uptick of 6 percent compared to 2020 (reference 10). With the technology becoming more mainstream, the trends of achieving solutions that emphasize "explainability," accessibility, data quality, and privacy are amplified.

"Explainability" drives trust. To keep up with the continuous demand of more accurate AI models, hard-to-explain (black-box) models are used. Not being able to explain these models makes it difficult to achieve user trust and to pinpoint problems (bias, parameters, etc.), which can result in unreliable models that are difficult to scale. Due to these concerns, the industry is adopting more explainable artificial intelligence (XAI).

According to IBM, XAI is a set of processes and methods that allows human users to comprehend and trust the ML algorithm's outputs (reference 11). Additionally, explainability can increase accountability and governance.

Increasing AI accessibility. The "productization" of cloud computing for ML has taken the large compute resources and models, once reserved only for big tech companies, and put them in the hands of individual consumers and smaller organizations. This drastic shift in accessibility has fueled further innovation in the field. Now, consumers and enterprises of all sizes can reap the benefits of:

- pretrained models (GPT3, YOLO, CoCa [finetuned])
- building models that are no-code/low-code solutions (Azure's ML Studio)
- serverless architecture (hosting company manages the server upkeep)
- instantly spinning up more memory or compute power when needed
- improved elasticity and scalability.

Data mindset shift. Historically, model-centric ML development, i.e., "keeping the data fixed and iterating over the model and its parameters to improve performances" (reference 12), has been the typical approach. Unfortunately, the performance of a model is only as good as the data used to train it. Although there is no scarcity of data, high-performing models require accurate, properly labeled, and representative datasets. This concept has shifted the mindset from model-centric development toward data-centric development—"when you systematically change or enhance your datasets to improve the performance of the model" (reference 12).

An example of how to improve data quality is to create descriptive labeling guidelines to mitigate recall bias when using data labeling companies like AWS' Mechanical Turk. Additionally, responsible AI frameworks should be in place to ensure data governance, security and privacy, fairness, and inclusiveness.

Data privacy through federated learning. The importance of data privacy has not only forged the path to new laws (e.g., GDPR and CCPA), but also new technologies. Federated learning enables ML models to be trained using decentralized datasets without exchanging the training data. Personal data remains in local sites, reducing the possibility of personal data breaches.

Additionally, the raw data does not need to be transferred, which helps make predictions in real time. For example "Google uses federated learning to improve on-device machine learning models like 'Hey Google' in Google Assistant, which allows users to issue voice commands" (reference 13).

AI in smart factories

Maintenance, demand forecasting, and quality control are processes that can be optimized through the use of artificial intelligence. To achieve these use cases, data is ingested from smart interconnected devices and/or systems such as SCADA, MES, ERP, QMS, and CMMS. This data is brought into machine learning algorithms on the cloud or on the edge to deliver actionable insights. According to IoT Analytics (reference 14), the top AI applications are:

- predictive maintenance (22.2 percent)
- quality inspection and assurance (19.7 percent)
- manufacturing process optimization (13 percent)
- supply chain optimization (11.5 percent)
- AI-driven cybersecurity and privacy (6.6 percent)
- automated physical security (6.5 percent)
- resource optimization (4.8 percent)
- autonomous resource exploration (3.8 percent)
- automated data management (2.9 percent)
- AI-driven research and development (2.1 percent)
- smart assistant (1.6 percent)
- other (5.2 percent).

Vision-based AI systems and robotics have helped develop automated inspection solutions for machines. These automated systems have not only been proven to save human lives but have radically reduced inspection times. There have been significant examples where AI has outperformed humans, and it is a safe bet to conclude that several AI applications enable humans to make informed and quick decisions (reference 15).

Given the myriad additional AI applications in manufacturing, we cannot cover them all. But a good example to delve deeper into is predictive maintenance, because it has such a large effect on industry.

Generally, maintenance follows one of four approaches: reactive, or fix what is broken; planned, or scheduled maintenance activities; proactive, or defect elimination to improve performance; and predictive, which uses advanced analytics and sensing data to predict machine reliability.

REFERENCES

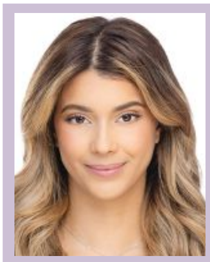
View the digital edition of this issue for the full citation and links to these resources.

Visit www.isa.org/intech to view the digital edition.

Predictive maintenance can help flag anomalies, anticipate remaining useful life, and provide mitigations or maintenance (reference 17). Compared to the simple corrective or condition-based nature of the first three maintenance approaches, predictive maintenance is preventive and takes into account more complex, dynamic patterns. It can also adapt its predictions over time as the environment changes. Once accurate failure models are built, companies can build mathematical models to reduce costs and choose the best maintenance schedules based on production timelines, team bandwidth, replacement piece availability, and other factors.

Bombardier, an aircraft manufacturer, has adopted AI techniques to predict the demand of its aircraft parts based on input features (i.e., flight activity) to optimize its inventory management (reference 18).

This example and others show how advances in AI depend on advances associated with other Industry 4.0 technologies, including cloud and edge computing, advanced sensing and data gathering, and wired and wireless networking. ■



ABOUT THE AUTHORS

Ines Mechkane is currently the AI Technical committee chair of ISA. She is a senior technical consultant with IBM, where she helps companies reach their full potential through AI and IoT. She has a background in petroleum engineering and international experience in artificial intelligence, product management, and project management. Passionate about making a difference through AI, Mechkane takes pride in her ability to bridge the gap between the technical and business worlds.

Manav Mehra is a data scientist with the Intelligent Connected Operations team at IBM Canada focusing on researching and developing machine learning models. He has a wide variety of experience developing ML models and pipelines for the aerospace, agriculture, transportation, and health care industries. Mehra has a master's degree in mathematics and computer science from the University of Waterloo, Canada, where he worked on a novel AI-based time-series challenge to prevent people from drowning in swimming pools. Mehra is active in the Python community and has recently been working on the fairness and explainability aspect of deep neural networks.

Adissa Laurent is AI delivery lead within LGS, an IBM company. Her team maintains AI solutions running in production. For many years, Laurent has been building AI solutions for the retail, transport, and banking industries. Her areas of expertise are time series prediction, computer vision, and MLOps.

Eric Ross is a senior technical product manager at ODAIA, where he works closely with engineers and data science teams to translate pharmaceutical customer pain points into AI products that drive engagement with health care professionals. After spending five years working internationally in the oil and gas industry, Ross completed his master of management in artificial intelligence. Ross then joined the life sciences industry to own the product development of a customer data platform infused with AI and BI.

Visualizing Data to Improve Operations

Augmented reality (AR) and virtual reality (VR) technologies are conduits of information to the plant floor. They are answers to the questions, "What do I do with all this data I've collected?" and "How do I attract and train new workers at a much faster rate than in the past?"

AR and VR use similar technology but are very different. Both have been popularized by gaming culture, and both are focused on changing what is visually presented to the user, but their industrial use cases are completely different.

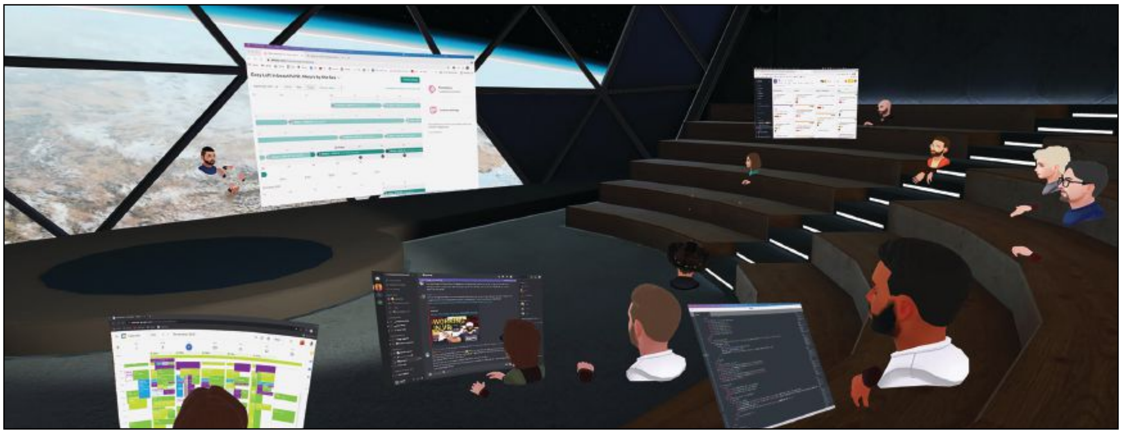
Augmented reality, which uses devices such as smart eyeglasses, smartphones, or tablets, changes what a user sees in his or her real environment. AR is very popular with games and entertainment applications, of which perhaps the most famous example is Pokémon Go. This mobile game lets users see Pokémon creatures in their own real-world environment when looking at their phone screens. Combined with global positioning system technology, the game allows players to find Pokémon associated with a specific real location.

Augmented reality is the most popular term to refer to such technology, but it is also called "mixed reality" or "computer-mediated reality." The devices that have helped it become popular are Google Glass and Microsoft Hololens smart glasses. Although Google Glass had a short life, it helped other companies, such as Vuzix, create their own products using the Android operating system for smart devices.

Artificial and virtual reality help manufacturers digitally transform and train new workers.

By Mario Gonsales Ishikawa and Dave Griffith

Smart glasses use AR to help operators get machine and system information that would usually require them to access another interface, such as a human-machine interface (HMI). Wearing smart glasses, operators can just look at an asset like a machine and get its entire real-time context—its current status, speed, last downtime event, current job, and so on. And this is just one of the possible industrial use cases.



VR: Real people collaborate in a virtual room, sharing screens and a whiteboard.

Source: Immersed

Virtual reality is also referred to as "alternate reality." Unlike AR, which mixes reality with computer-assisted information presented to the user's eyes, VR immerses the user in a completely virtual environment. Although it can be experienced on devices such as a laptop or a phone, the most popular and useful way to use VR is with virtual reality glasses or goggles. While using a VR device, the user has no vision of the real world, and his or her view range can reach only what is being shown by the VR lenses.

As with AR, games and other entertainment applications are helping to take VR mainstream. Meta (Facebook's parent company) Oculus Quest 2 is one of the most popular VR devices. It was created to provide a complete experience for the user without requiring a connection to a computer or powerful video game console, which was a big breakthrough.

So, while it makes sense to wear AR smart glasses to take a walk through the shop floor, the same cannot be said for VR, as they take complete vision and attention. The use cases are different, such as for training new employees on facilities and equipment they have never been exposed to before, or even to allow colleagues to join in a virtual environment and collaborate by sharing computer screens and whiteboards, which is possible with an immersed app.

Why are AR and VR so important right now?

AR and VR have been in the market for quite a long time. According to Wikipedia, the U.S. military started the first AR tests in the early 1990s, while VR with immersive devices was introduced in 1979 at NASA. During the 1980s, several companies, including ATARI, started substantial investment in research and development. In the 1990s, many gaming VR headsets were available from companies like SEGA and Nintendo.

The fact is that the technology at that time was not robust or cost effective enough to allow people to really feel immersed in a world-like environment. Just like handheld devices for business and daily tasks became ubiquitous only after the first iPhone was introduced, the same can be said for AR and VR devices.

As little as five years ago, the best VR devices required an expensive computer or a video game console. Today, devices like Oculus Quest 2 are available at a viable price point and comfortably deliver lifelike simulated worlds: If a colleague calls to you from behind, you hear the voice as if the person was right at your back. The headset comes with its own processing unit and graphical processing unit (GPU), and you can use it hands free. And the battery, always an issue, now lasts for four hours.

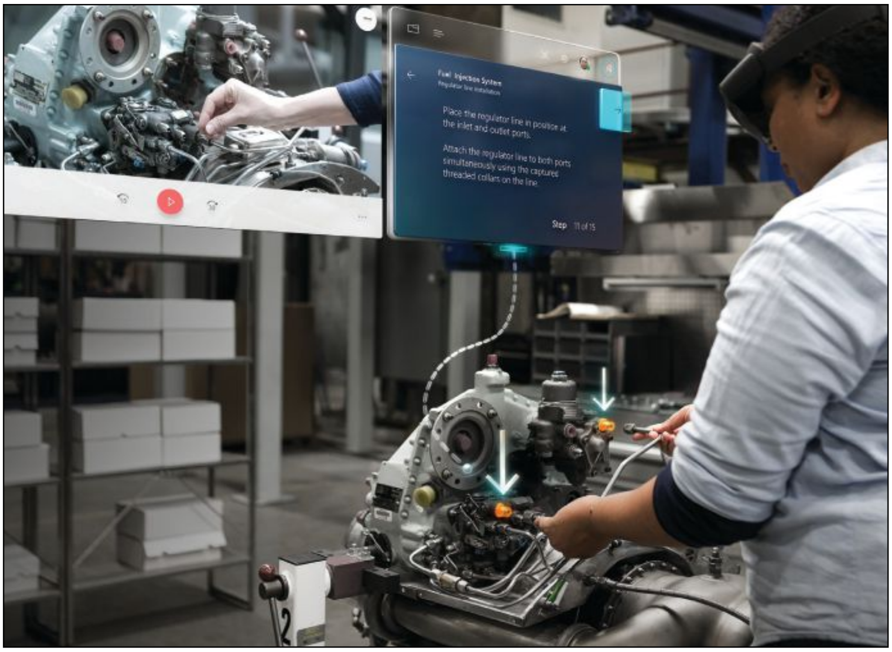
Now that these gadgets are being taken more seriously, and not just for games, there are many possibilities for applications on both AR and VR in business, especially manufacturing. Manufacturers need to digitally transform, and AR and VR can help them in this process in a cost-effective way.

Current trends related to AR and VR bode well for its adoption by industrial companies. Devices are getting cheaper and more physically robust. In addition to Google Glass and Microsoft Hololens, dozens of new devices have been launched at various prices, notably RealWear, Vuzix, Hololens 2, and new versions from Google and Apple. In a major shift, most of the AR/VR platforms can run on the Android operating system now. Manufacturers can hand people inexpensive tablets or leverage the phones in their pockets.

Applications abound

With so much data available on the shop floor, AR glasses help contextualize the processes for operators by providing information that layers over the assets. This information might be something as simple as an andon could show, or something that would require visiting spreadsheets, PDF project documents, and other HMIs. With a well-customized system on the back end, the smart glasses do not only present the information from these various systems, but they also present it in a processed and contextualized way.

Here is an example: By looking at an enterprise resource planning system HMI, operators can see which work order is next and then look at a PDF document to check the correct tool. With AR, they can look at the machine and immediately receive the information that the current job is done and the next work order is ready to start, with a list of the required



AR: On-the-job guidance provided with Microsoft Hololens.

Source: Microsoft

We are seeing fully processed 3D facility models that remote executives can walk around in.

tools. Microsoft presented a Hololens use case at Toyota in which inspection time was reduced by 20 percent (https://www.microsoft.com/en-us/hololens/industry-manufacturing). The time for manual and repetitive jobs can also be reduced by allowing the user to check for next steps right from the glasses, without having to look in paper documents.

VR can be used to train for dangerous situations that might never happen but require operators to be ready for corrective operations. AR could be very important in situations where the technician cannot go into the field for maintenance and is working remotely. In such a case, an operator in the field with smart glasses can give the remote technician the same visualization while both are in a call, so instructions can be placed.

One thing holds true for new pieces of technology: People find innovative ways to use them. Some of the initial applications for AR and VR technology included maintenance information, the creation of workflows, quality checks, and QR-code access to cloud-stored information. But give this technology to smart people with a need, and the applications become endless.

How can AR and VR help in a smart factory?

Today, we are seeing virtual training applications where people can practice spraying coatings without causing issues in production. We are seeing underground nuclear facilities with secure data and hands-free workflows. There are fully processed 3D models that allow executive board members to walk around their facility without going into the field. Tomorrow's applications will only be limited by the demands and our imaginations.

Companies are being forced to adopt technologies at a fever pitch. The lack of skilled resources is forcing companies to leverage technology to complete their work and attract new talent. The ability to upskill and train employees in a mock environment has never been more important, and younger employees want interesting technology to learn and grow with over the course of their careers. AR and VR are two of those technologies with extremely low costs of entry.

This is now a reality. AR/VR is the path to putting the correct information in the hands (or should we say, eyes) of workers when they need it. ■

ABOUT THE AUTHORS

Mario Gonsales Ishikawa (mario@packiot.com), is the chair of the Virtualization Technologies (AR & VR) technical committee of ISA's SMIIoT Division, which is focused on bringing awareness of the benefits of these technologies, and accelerating their adoption to improve manufacturing efficiency and working conditions. Ishikawa has worked with industrial software such as SCADA, historians, MES, and SPC for 24 years and currently is the chief technology officer of PackIOT. He leads technical product development and architects custom IIoT solutions for large corporations.

Dave Griffith (www.linkedin.com/in/davegriffith23), is a member of ISA's SMIIoT Division. He runs a weekly multimedia show called Manufacturing Hub, where the manufacturing community from around the world gathers to discuss ideas. Currently, he is working at the intersection of technology and operational excellence for his company, Capelin Solutions.

Cybersecurity for Electric Energy Infrastructure

The U.S. Department of Energy (DOE), global equipment suppliers, and other stakeholders announced the establishment of the *Electric Energy OT Security Profile* working group hosted by the ISA99 standards committee. The *Electric Energy OT Security Profile* will be a cybersecurity work product using the ISA/IEC 62443 series of standards. The final product will be a formal ISA/IEC 62443 application guide, recognized globally as the consensus work product for securing various control systems used in electric energy generation, transmission, and distribution operations.

The ISA/IEC 62443 series of standards is designated as a horizontal standard, applicable to many industry sectors and applications. Industry groups use the ISA/IEC 62443 standard series as the basis for securing industrial control systems. DOE's Securing Energy Infrastructure Executive Task Force (SEI ETF) evaluated available industry standards and recommended the electric energy operational technology (OT) applications be formalized as ISA/IEC 62443-5 security profile applications—gaining international energy sector consensus on applying ISA/IEC 62443 to electric energy OT applications.

The working group is seeking participation from industry groups, including the Institute of Electrical and Electronics Engineers (IEEE), the International Electrotechnical Commission (IEC), the International Council on Large Electric Systems (CIGRE), and other industry stakeholders, to ensure consideration of and alignment with other cybersecurity work product development efforts. The initiative will use the DOE SEI ETF's *Reference Architecture and Profiles for Electric Energy OT* as a foundation.

"The Securing Energy Infrastructure Executive Task Force developed an OT-specific reference architecture for electricity systems to provide a common language for control system environments that can be used to design and assess security applications," said Puesh Kumar, director, DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER). "The ISA working group represents an opportunity to validate these profiles and put them into practice for the energy industry. CESER is excited to see energy sector stakeholders carrying forward the task force's reference architecture work."

Eric Cosman, co-chair of the ISA99 Standards Committee, noted that, "Global standards and supporting specifications provide efficiencies for end users, product suppliers, and system integrators that design, deliver, and support products and systems all around the world. One specification and one globally recognized certification provides needed transparency and reduces the regulatory burden on manufacturers."

Companies and individuals interested in participating in the Electric Energy OT Security Profile working group should contact Eliana Brazda at ebrazda@isa.org to be added to the roster. ■ *—By Steven Aliano*

EnQuest Wins ISA100 Wireless Excellence Award

The ISA100 Wireless Compliance Institute presented its ISA100 Wireless Excellence in Automation Award for 2021 to EnQuest, an oil and gas production and development company with operations in the U.K. North Sea and in Malaysia. Managing director Andre Ristaino presented the award at the ARC Forum conference in Orlando in June.

ISA100 Wireless, also known as international standard IEC 62734, is an open, universal IPv6 wireless network protocol that establishes the Industrial Internet of Things. IPv6 addressability makes ISA100 Wireless the only industrial network protocol compatible with the Internet of Things. The ISA100 Wireless Excellence award is presented each year to an end-user company that has demonstrated outstanding leadership and innovation in the use of ISA100 Wireless technology.

The 2021 award was presented to EnQuest for its Sullom Voe Terminal in Scotland and its novel application of ISA100 Wireless technology for new approaches to gas detection and achieving a safe and secure gas detection system upgrade on a vast scale. Cybersecurity and reliability were key considerations in the gas detection system upgrade.

EnQuest's Sullom Voe Terminal is located at the northern end of the largest of the Shetland Islands and is one of the largest oil terminals in Europe. It handles production from many oil fields in the east and west Shetland Basin in the North Sea. Fourteen different companies have ownership interests in the terminal, which receives production through the Brent and Ninian 36-in pipeline systems.

Previous award recipients include Fuji Oil Company (2020), ILBOC (2019), BACPO (2018), ALCOA (2017), Phillips 66 (2016), Petronas (2015), Nippon Steel (2014), and RasGas (2013).

Find out more through the ISA100 Wireless Interest Group on LinkedIn at https://www.linkedin.com/groups/4840835. ■

Updated Schedule for ISA Fall Hybrid Events

New virtual events with in-person components provide convenient attendance and live networking opportunities. The live components of the events are supported by ISA sections and/or regional partners. The locations shown indicate the time zones during which the virtual events will take place. Find out more and register online (https://www.isa.org/events-and-conferences).

- Digital Transformation – North America, 25 August, 9 a.m.–5 p.m. ET. In-person location: Houston, Texas. Local partner: ISA Houston Section.
- Digital Transformation – India, 20 September, 9 a.m.–5 p.m. GMT+5:30. In-person location: Faridabad, Haryana, India. Local partner: National Power Training Institute (NPTI) and Central Electricity Authority (CEA).
- Digital Transformation – Malaysia, 5 October, 8 a.m.–5 p.m. GMT+8. In-person location: Kuala Lumpur, Malaysia. Local partner: Petronas.
- Cybersecurity Standards Implementation – North America, 26 October, 9 a.m.–5 p.m. ET. In-person location: Houston, Texas. Local Partner: ISA Houston Section.
- ISA Automation, Leadership and Technical Education – North America, 7–9 November, 8 a.m.–5 p.m. ET. In-person location: Galveston, Texas.
- Cybersecurity Standards Implementation – Middle East, 6 December, 9 a.m.–5 p.m. GMT+3. In-person location: Saudi Arabia. Local Partner: Saudi ARAMCO. ■

AD INDEX

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

ISA Automation & Leadership Conference: In Texas and Online in November

A new event that combines ISA's annual leadership conference with two days of technical presentations will welcome attendees both online and in-person in Galveston, Texas, in November. The three-day event, 7–9 November, will be held at the Galveston Island Convention Center. It combines workshops and association meetings with presentations on important industry topics like digital transformation, cybersecurity, Industrial Internet of Things, smart manufacturing, and process automation.

Planned sessions for the multi-track event include a cybersecurity hackathon. Speakers include subject matter experts from the U.S., Middle East, Brazil, Malaysia, Spain, and India. The event also includes an exhibition area where the latest automation and cybersecurity products and technology will be on display, as well as the ISA Honors and Awards gala. Information and registration are online at https://www.isa.org/events-and-conferences/alc. ■

Collaboration is Key to an Automation Professional's Role in the Digital Revolution

By Bill Lydon

Lydon (blydon@isa.org) is an *InTech* contributing editor with more than 25 years of industry experience. He regularly provides news reports, observations, and insights here and on Automation.com.

Automation professionals have an important role as manufacturing and production are being integrated into the real-time digital business architectures of manufacturers and other industrial companies. A real-time digital business architecture integrates information from sensors to business systems and cloud applications to maximize customer responsiveness, increase profits, and achieve sustainability goals. It also ends the isolation of manufacturing, closing information loops in real time to achieve internal and external manufacturing efficiency and responsiveness.

Industrial automation professionals are helping their employers become leaders in their industries. To do this, the best need a forward-looking mindset that understands and embraces the difference between significant transformational change and continuous improvements that leverage new technology only for incremental gains. Significant transformational change requires system analysis to integrate information technology (IT), operational technology (OT), automation, and controls to achieve efficient and responsive synchronized production.

This integration is now possible given the significant advances in technology, communications, and software. Automation professionals have the knowledge and know-how to end the isolation of manufacturing as a siloed part of the business separate from other business disciplines.

Automation professionals can positively impact their companies by helping everyone understand the possibilities, showing how to make them a reality, gaining organizational support, and convincing management to invest in true digital transformation. This requires taking the initiative to collaborate with manufacturing groups, creating transformative manufacturing processes and applying advanced technologies such as collaborative robots, machine learning, artificial intelligence, and virtual/augmented reality. Good examples of such groups include:

Industry 4.0. Started in Germany more than 10 years ago (see p.10), a working group developed an 85-page paper that has since become a major focal point for defining and standardizing the digital manufacturing business architectures being adopted by companies and countries throughout the world. Companies are each trying to gain a competitive advantage from the development of Industry 4.0 cyber-physical systems, and the RAMI 4.0 Reference Architecture (https://www.zvei.org) is a great starting point.

The OPC Foundation. This organization's standards are becoming the industrial digitalization semantic information models. They facilitate smart data messaging from sensors and controllers by providing inherently usable information rather than cryptic messaging. Semantic data is structured to add context and meaning that is immediately usable by applications—streamlining communications, improving quality, and ensuring data consistency. OPC UA (https://opcfoundation.org) and companion specifications are an example of semantic data models that implicitly define how the information relates to real-world applications. Significant collaborations include VDMA Companion Specifications (www.vdma.org), and CESMII OPC UA Cloud Library (https://www.cesmii.org) global OPC UA Cloud Library.

ISA's SMIIoT Division. This newest division of ISA (see p. 8) focuses on smart manufacturing, Industry 4.0, and Industrial Internet of Things (IIoT) and related technologies, providing members with a forum for networking and collaboration so they can positively impact their companies and the global manufacturing community at large.

Significant transformational change requires system analysis to integrate IT, OT, automation, and controls to achieve efficient and responsive synchronized production.

Automation professionals are an integral part of the efforts to rethink fundamental processes and architectures, to learn from and collaborate with others, and to achieve real-time integration of entire businesses. Industry is experiencing transformational changes. Automation professionals who rise to the challenge will be leading the way to greater manufacturing productivity, efficiency, sustainability, and energy efficiency. ■


WE'VE GOT
YOU COVERED
• Process Automation
• DCS Modernization
• Systems Integration
• Startup & Commissioning
• Field Service
• 24/7/365 Support
Let's Talk About Your
Control System Performance.
MAVERICK
TECHNOLOGIES
A Rockwell Automation Company
mavtechglobal.com
info@mavtechglobal.com 888.917.9109
READ THE
CASE STUDY
GOOSE
DUG UP!
mavtechglobal.com/goose-intech
GOOSE

Ignition 8.1

by inductive automation

Built For The Plant Floor

Build Mobile-Responsive HTML5 Applications That Run Natively on Any Screen

8.1

Try Ignition 8.1 For Free Today at
www.*inductiveautomation.com*

Built For Everyone

Unlimited Licensing Model
Add unlimited clients, screens, tags, connections & devices.

Cross-Platform Compatibility
Ignition works with any major operating system, even iOS and Android.

Instant Installs and Updates
Install on a server in just 3 minutes, push updates to clients everywhere, instantly.