Smart industry
TECHNOLOGY REPORT

One Year Smarter, Yet Much to Learn: Our 2019 Digital Transformation Crystal Ball

With each passing year, our collective digital transformations mature. We're further down the digital road, we know more about the pitfalls and possibilities than we did just a few years ago. Our systems are, perhaps, smarter. Our temples are, perhaps, grayer. But we're still early in this process—there is much to learn. And pondering the near future is a healthy place to start as we enter the new year.

Smart industry

TECHNOLOGY REPORT

CONTENTS

Smart gets cheaper & four other predictions for global manufacturing 3

Finding the balance between human and machine in 2019 5

Smarter systems, smarter bad guys…securing industry in the coming year 7

A natural user experience in the smart space 10

More predictions on our digital transformation 12

Smart gets cheaper & four other predictions for global manufacturing

By Dr. Simon Kampa, CEO and co-founder of Senseye

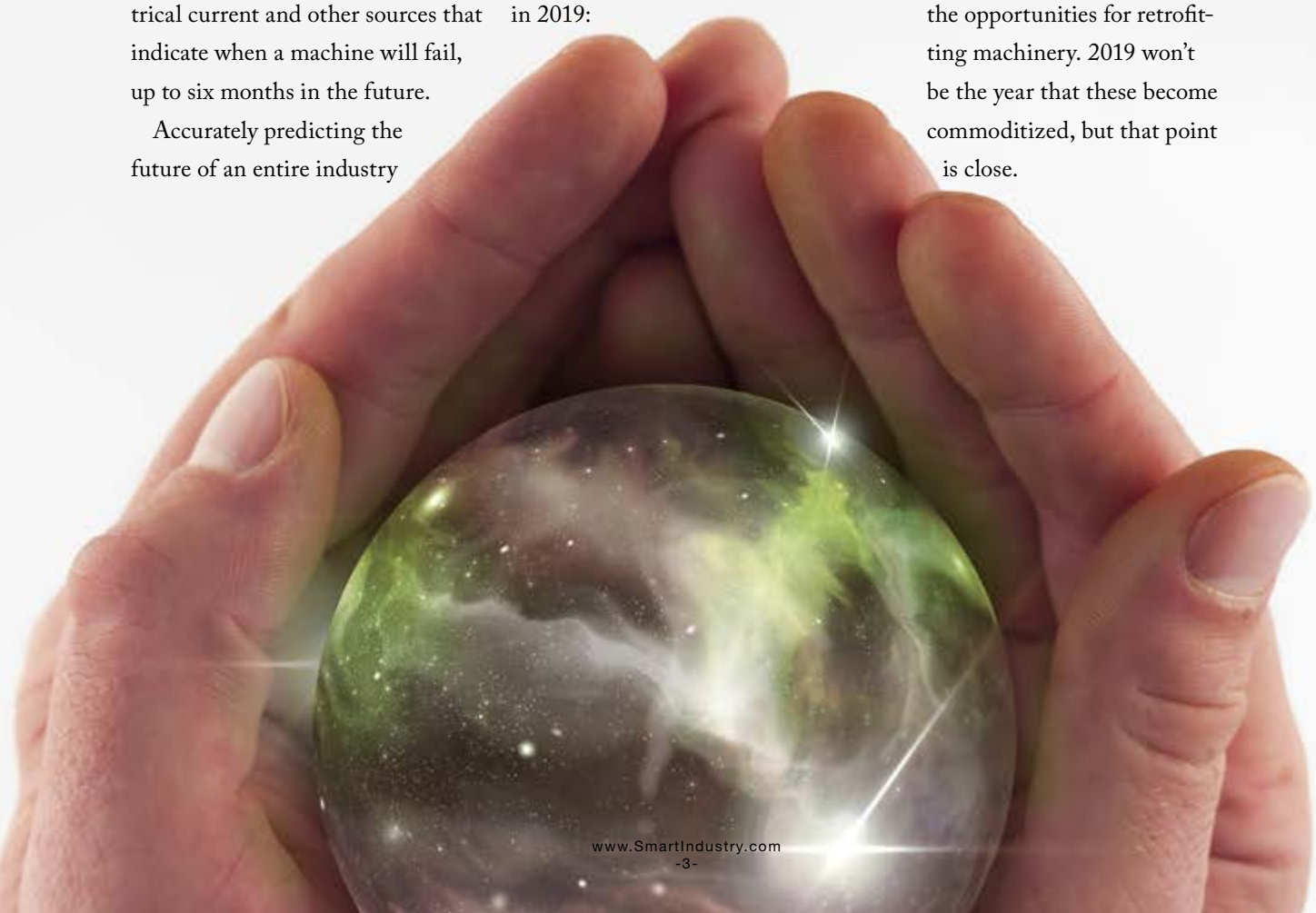
2019 marks an inflection point in the maturity of Industry 4.0 and the application of real-world predictive maintenance as companies move from pilots to real deployments—with significant ROI.

We use machine learning to monitor the condition of industrial machinery and spot the small but significant variations in vibration, pressure, temperature, torque, electrical current and other sources that indicate when a machine will fail, up to six months in the future.

Accurately predicting the future of an entire industry such as manufacturing is much more difficult—the variables are many more than you'd find on a typical piece of industrial equipment. We do, however, come into contact with hundreds of manufacturers around the world every year, which gives us some idea about where the industry is heading.

Here are our top five predictions for the global manufacturing sector in 2019:

1. The cost of smart sensing solutions to connect legacy machinery and enable Industry 4.0 will continue to decline. Manufacturers want data from older machines, but have been forced to bolt together their own systems due to a lack of off-the-shelf products. There will be a land grab from systems vendors that have recognized the opportunities for retrofitting machinery. 2019 won't be the year that these become commoditized, but that point is close.



The food & ag industry is increasingly under pressure to produce products with better quality and safety, while reducing waste. AI's ability to improve reliability across the value chain—while optimizing energy, raw materials and cycle times—is why it should be on every food & ag plant's priority list for 2019.

Humera Malik, CEO of Canvass Analytics

2. Building upon the availability of inexpensive data, 2019 is going to be all about the value-add that it brings; using data to monitor machinery, predict problems before they impact production, and optimize the efficiency and throughput of manufacturing environments. Manufacturers will increasingly turn to *holistic* cloud platforms (such as Siemens Mindsphere) and use the data they contain at a greater scale—and ease—than ever before. This focus on data provides an opportunity for IT to move beyond problem-solving and deliver huge amounts of value to the organizations they serve.
3. Automated machine-learning-driven predictive maintenance will become mainstream. Predictive maintenance has been used in regulated industries such as aerospace for years, relying on humans to collect and analyze the data for signs of problems. Advances in this area and the ubiquity of cloud computing, together with the ability to gather machine data, means we can now automate condition monitoring and prognostics at a scale and cost that gives an ROI of less than three months in most cases. There have been many trials for this nascent technology in recent years, and we'll see lots of these expanded, factory-wide, in 2019.
4. While engineers will make greater use of data, we won't see them spending more time at their desks. Engineers will be mobilized to spend more time on the factory floor, armed with rugged mobile devices and a range of industrial apps. These will make jobs such as monitoring machine health incredibly easy, performed by a computer in the cloud, with the critical bits of information served directly to engineers on the factory floor. 2019 will see real-world case studies emerge, as companies build the confidence to share this information with the world.
5. 2019 will be the year machine manufacturers recognize the opportunity presented by servitization. More OEMs will move to selling capacity and uptime rather than simply a production asset, and this change will require more visibility into how machines perform. It will also require greater data-sharing between users of those machines and the OEMs.

Of these five predictions, I am most excited about servitization. It will represent the biggest step-change for the industrial sector since the introduction of Industry 4.0.

The software industry has demonstrated that a scalable As-A-Service model can be effectively integrated into all levels of modern business. Providing the business function of a machine is really no different, though it does require far more complex data-processing and interpretation. ◻

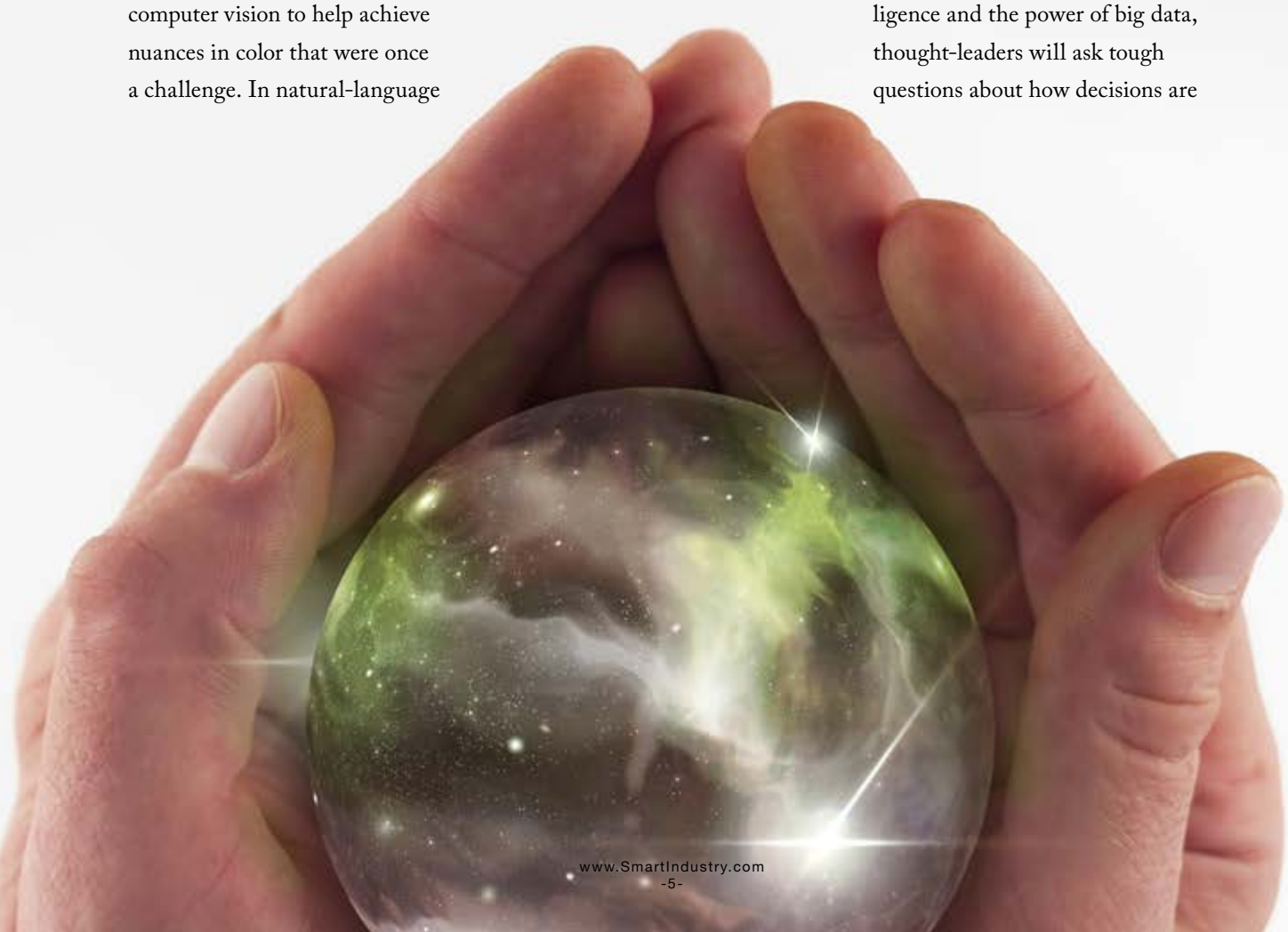
Finding the balance between human and machine in 2019

By Marcia E. Walker, principal industry consultant in the industry practice of SAS

Artificial intelligence can conjure images of soulless robots repetitively managing machines, but that's an outdated view. AI is not just mechanical in nature; it can also affect the manufacturing industry in more artistic areas like computer vision and natural-language processing. For example, a paint manufacturer might use computer vision to help achieve nuances in color that were once a challenge. In natural-language processing, a manufacturer can turn to unstructured written data sources like equipment maintenance logs, shipping manifests, and customer call-center records to reveal new insights.

AI will help manufacturers solve old problems, innovate new products and create new business models.

Man v. machine. Finding the balance between human and machine will become more pronounced in 2019. Recent news about things like genetically engineered babies has many wondering about the balance of ethics and technological advancement. As mainstream consumers become more familiar with artificial intelligence and the power of big data, thought-leaders will ask tough questions about how decisions are



We are seeing the global mega-trends moving toward the use of the IIoT in the manufacturing industry, such as Industry 4.0 in Europe, the Industrial Internet Consortium in the US, intelligent manufacturing in China and others. All of these share a common goal: the creation of smart factories in which everything is connected, data is used to the fullest, and optimized manufacturing takes place autonomously. In order to create smart factories, essential issues include gathering real-time information from production processes, processing it, and then transmitting it seamlessly to IT systems. Toward that end, one crucial need when making the most of production-site data is a network capable of high-speed, stable-control communication as well as large-volume information transmission to IT systems. In other words, it is important to combine industrial networks at production sites with IT system networks. To that end the CC-Link Partner Association (CLPA) has created a new industrial open network specification: CC-Link IE TSN.

John Wozniak, manager—CLPA-Americas

made, how to bake ethical principles into mechanical processes, and how to consider the unintended consequences of automating tasks previously reserved for humans.

The myth and reality of IIoT. The hype surrounding IIoT platforms has been tempered as producers and users recognize the complexity of knitting together disparate systems and monetizing offerings. IoT platforms will still make a strong play in the market even as their adoption has been more complicated than anticipated. Commercialization of those platforms is progressing at a slower rate than expected because vendors and customers are presently more focused on testing, security and other important foundational aspects of IoT technology.

Increased literacy about big data and analytics. A disappointment in 2018 was that many companies claimed to offer AI or machine-learning capabilities when, in fact, they offered only simple dashboards and entry-level statistics. As data continues to permeate daily life and digital-literacy grows, an understanding of analytics will naturally grow, too. In coming years, more non-tech personnel will be able to speak competently and evaluate solutions that include AI features like neural networks, deep learning, computer vision and natural-language processing. ◻

Smarter systems, smarter bad guys…securing industry in the coming year

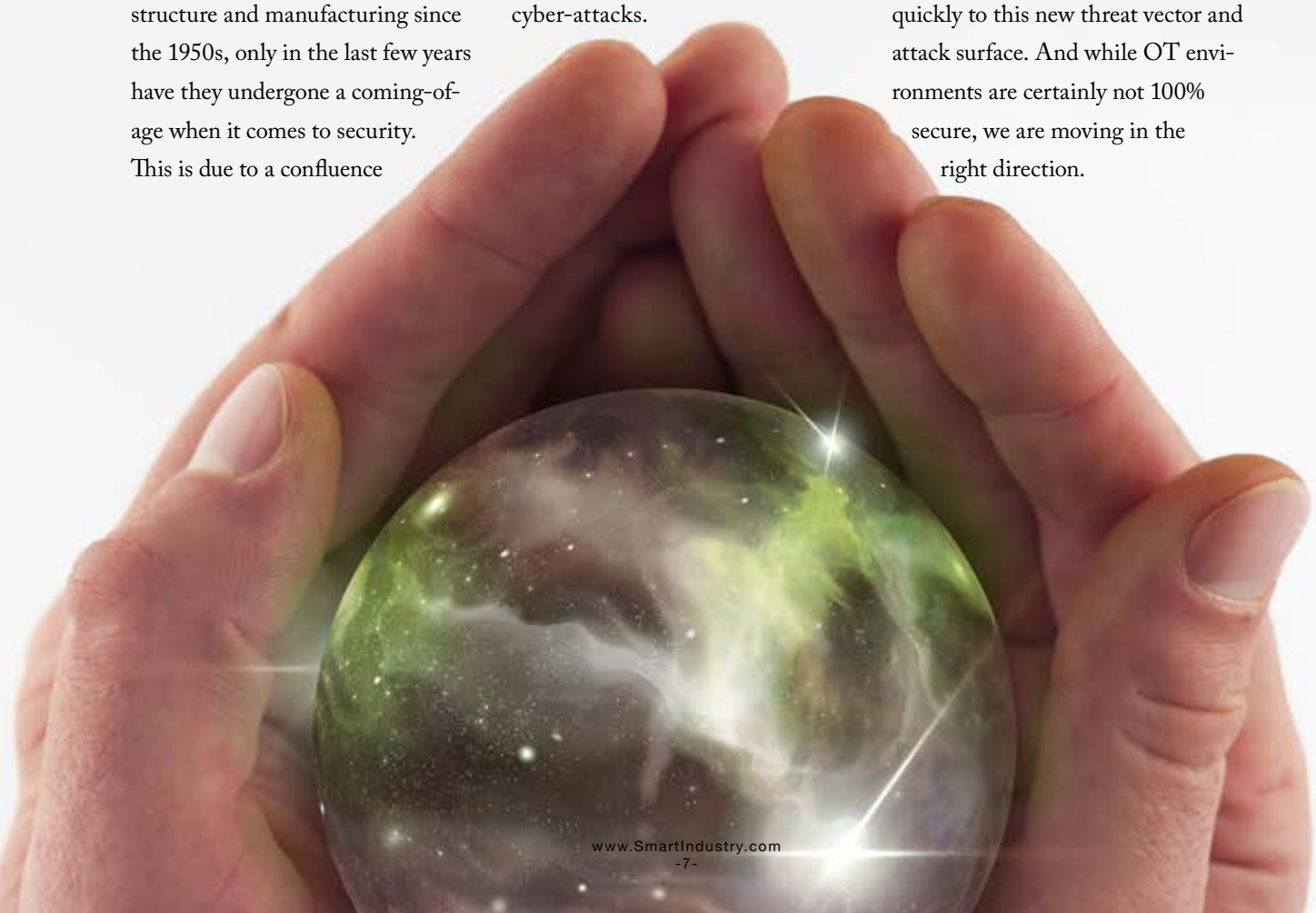
By Mille Gandelsman, Indegy CTO

In many ways, 2018 represented the coming of age for industrial cybersecurity. The old adage that operational-technology networks were isolated from threats by an air gap was recognized for what it is—a fallacy in an era of interconnectedness and IIoT technologies.

Many pundits believe that even though industrial-control systems have been running critical infrastructure and manufacturing since the 1950s, only in the last few years have they undergone a coming-of-age when it comes to security. This is due to a confluence of events that have propelled OT threats to the C-Suite risk agenda. Namely, the adoption of IIoT, the convergence of IT and OT environments, and the increased targeting of these mission-critical systems by known and unknown rogue parties.

What used to be isolated, air-gapped "set and forget" OT networks have become ground zero for potentially debilitating cyber-attacks.

It is not all doom and gloom, however. Progressive industrial organizations are well down the path of ensuring the full visibility, security and control of their environments. If fact, many organizations that must meet a minimum-security compliance level (NERC, NIST, NIS) have progressed beyond these basic directives. The markets have reacted quickly to this new threat vector and attack surface. And while OT environments are certainly not 100% secure, we are moving in the right direction.



As 2019 ramps up, the obvious question is: What can we expect this year? Based on our daily interactions with professionals working to secure their industrial control systems, we have pulled together the following predictions about the 2019 industrial-security landscape.

ICS SECURITY WILL BECOME MORE MAINSTREAM

As noted earlier, many large industrial and critical-infrastructure organizations have already made investments to secure their OT infrastructure to the same (or higher) degree than their IT infrastructure. We expect this trend to continue in 2019. In addition, we predict it will extend beyond large organizations to midsize and smaller companies. Given the clear and present threat, Industrial Control Systems (ICS) security is no longer an early adopter segment; it will become a mainstream requirement for every industrial organization, regardless of size or vertical.

HACKING TOOLS FOR CRITICAL INFRASTRUCTURE WILL BE MORE ACCESSIBLE

And that brings me to the adversaries responsible for ICS attacks. There is no question that many past attacks have been conducted by nation states, rogue factions and insiders. Going forward, we will likely see lone wolves and non-nation actors also launching attacks. The barriers to entry are lower, and with a little know-how, OT-based attacks can be carried out by the general hacking community rather than being relegated to state-sponsored cyber-warfare initiatives.

OF COURSE, ATTACKS WILL CONTINUE TO GROW MORE SOPHISTICATED

In general, most of the attacks that we have seen to date were aimed at a single target or country. Attacks will continue to grow in sophistication and become multi-pronged, targeting multiple locations and sites simultaneously or in close succession. Organizations will need to consider this possibility and (once

We've used apps on our smartphones and tablets for years. Most companies that provide a service to consumers have an app. But most of these apps are coming from companies that are business-to-consumer. In 2019, we will start to see business-to-business companies provide apps to their customers. With apps for their enterprise systems, manufacturers can quickly access important product and enterprise data on the fly, in a format that is easy for them to understand. Products with sensors that feed information from the field can be connected to apps that enable stakeholders to quickly and easily view real-time information. And with AR apps, global teams can quickly review designs or prototypes concurrently. The possibilities of enterprise apps are endless. They will enable users to rapidly launch systems that have traditionally been tethered to a desktop.

Kevin Wrenn, divisional general manager of PLM with PTC

again) evolve their security posture accordingly.

ACTIVE DETECTION WILL BE TOO VALUABLE TO IGNORE

The previous prediction will not only push organizations to act, but also force them to address new threats in a more proactive way. Passive or "listening only" monitoring merely looks at network traffic. It will no longer be sufficient. Rather, Active Threat Hunting through safe-device querying will become essential to gain the visibility, security and control necessary to protect against a new generation of threats. "Active" covers the 50% of threats that can't be detected with network-only monitoring. Many OT security vendors are only now adding rudimentary active capabilities.

MORE COLLABORATION/ SHARING OF OT THREAT INTELLIGENCE

In the area of threat-hunting, several other capabilities will be required to better identify, mitigate and report on new ICS threats. In the coming year we are likely to see a maturation of ICS threat intelligence. This includes the use of external security-data feeds as well as integrating OT-security technologies with SIEMs, next-generation firewalls, etc. There will also be more sharing of information across communities such as OISF, which has been a mainstream practice for years in IT. It will be embraced by the OT community as a key way to quickly identify threats and protect against new attacks that can impact ICS environments.

REAL STANDARDS FOR ICS SECURITY WILL EMERGE

Finally, we will see new the publishing and adoption of ICS-specific standards, guidelines and best practices for assessing and hardening the security of ICS environments.

Looking at 2019 and beyond, ICS threats will continue to escalate and evolve, but we predict the solutions to combat these threats will effectively address whatever emerges. In planning your strategy, look for ICS-security vendors that are experts in what they do and can help chart the course that is right for your organization, both now and into the future. ◻

Amazon Web Services was launched in 2006, with Google and Microsoft announcing their own services two years later (Google Cloud and Azure). That's all by 2008 if you're counting at home. In 2018, with Siemens Mindsphere v3 availability and GE Predix, well, we're not sure what's going to happen, what with GE spinning out their software business. But 10 years into the public cloud-services market, it finally feels likely to see in this space manufacturing companies (or the manufacturing side of manufacturing companies, as many IT departments have already shifted IT and application workloads to the cloud). But for OT departments…not so much. Looking ahead to 2019, the offerings feel mature enough to be ready for broad adoption for manufacturing use cases and workloads. It took a decade, but we're there.

Michael Risse, CMO/VP with Seeq Corp.

A natural user experience in the smart space

By Itai Dadon, director of smart cities and IoT at Itron

The success criteria for use of technology is often defined by the user experience. In fact, the more transparent the technology, the more natural the experience will be. Most end-to-end solutions affecting smart spaces will include the following four components:

Devices: Industrial IoT devices are starting to benefit from tremendous growth of the consumer-IoT market in recent years. Rapid democratization of high-computing and low-power platforms has enabled huge innovation in the areas of edge computing and sensor performance, including gathering more accurate information at higher frequencies, prompting action on this data close to its source. Devices are increasingly capable of executing advanced use cases in near real time.

Connectivity: Many standards exist for networking devices in the field, but different technologies will apply to different markets and use cases. The rapid proliferation of connected devices, generating more and more data, will require the transmission of this information in a secure, reliable and efficient way. Scale and longevity are also essential criteria for the selection of the right technology. Consider a smart city, in which millions of meters and smart devices work together seamlessly, creating a positive experience for the consumer and a winning business case for the utilities and cities operating them.

Data platform: Collecting all the data and managing it according to the most rigorous standards of security is essential. Understanding how important it is for such a platform to enable an open (but controlled) use of the data, in addition to data from

other sources, is the key to unlocking the true transformation of smart spaces. In fact, many cities are adopting a policy of providing open access to data by default. This shared access across multiple interoperable systems enables the complex interaction between heterogeneous devices operating in the smart space. As an example, parkingspace sensors are only useful if the information is available in real-time to drivers in an accessible and actionable way. Providing automatic guidance to that parking spot from within your car-navigation system or the navigation system in your phone helps deliver the specific outcome consumers expect (faster access to parking). One of the biggest challenges we see today is how to ensure all these systems speak the same language and understand the data being shared without extra integration or translation efforts.

Outcomes: What do we do with the information available to us? What is the objective of the smart space to begin with? Good questions. We see a great deal of use of technology for the sake of technology. A careful understanding of the pain points we are trying to remedy and a meticulous study of the business case of the proposed solution guarantees a real outcome to create continuous and repeatable benefits for all parties in the smart space. Cities and utilities that own these critical-infrastructure assets can leverage their open platforms to enable more outcome-oriented solutions. With more mature device ecosystems powered by open standards-based platforms, developing an end-to-end solution is faster and easier than ever. We expect to see cities and utilities utilize these tools to accelerate innovation to deliver the outcomes that consumers demand.

In 2019 we expect to see great progress across these four pillars. As deployment for systems begins, we expect them to deliver valuable data, which creates new opportunities. Currently, solutions at work deliver mostly independent and siloed solutions (e.g. parking sensors, air-quality monitors, waste-bin sensors, etc.).

This current phase will enable important improvements in each one of those applications separately. However, the real transformation of our smart spaces will only happen after we are able to learn how to fuse the data from all these sensors together. ◻

Got your own prediction?
Join the discussion on Twitter using #DTCrystalBall

More predictions on our digital transformation

"Is geolocation our friend or foe? The day when we know the location of every item (or person) is not far away. Most of us already have smartphones that allow apps to present content based on the device's (and presumably the user's) location. Increasingly, our cars are also connected, enabling the owner to go online and see where it is parked, which is a particularly helpful capability for parents of teenagers! Think about other uncertainties in daily life—Where is my package? How far away is the service tech I'm expecting? Where has my doggone dog gone? While it may sound "Big Brotherish" to many, and while ominous potential may exist, there is great opportunity in reducing anxiety-causing, back-and-forth communication. I can't help but be excited about the quality-of-life enhancements enabled by this technology."

— **Joseph H. Schwartz**, president, Braas Motion Industries Automation Solutions Group

"What I'm most excited to see in 2019 is not the growth of any one type of technology in particular, but the emergence of a new role because of technology. In 2019 we'll see an influx of individuals with the titles workplace strategist and workplace technologist. These individuals will fill a role that crosses over IT, HR and facilities management—all driven by the ever-evolving work environment. Today's employees demand easy-to-use, connected technology at their desks and in their conference rooms. Workplaces that fail to deliver this run the risk of losing top talent. That's where the overlap between IT, HR and facilities comes in—companies need someone who can help identify what employees want, help design a facility that fits that need, and understand the technology that must be deployed to do so. The workplace strategist will take into consideration the technology individuals are using in their personal lives (like voice control) and help deploy it in an office environment with the goal of creating a better experience for employees."

— **Dan Jackson**, director of enterprise technology at Crestron

"The future of automation is in combining real-time control with edge computing, so your data comes directly from the source and can be securely processed and sent where you need it. Existing systems are complex, costly and difficult to maintain, but a new kind of technology solves those problems. This new technology is not a PLC, a PAC or a PC, but is EPIC—an Edge Programmable Industrial Controller.

- **Edge—Collect, process, view, and exchange data where it's produced…at the edge of your network.**
- **Programmable—Choose your programming options: IEC 61131-3, field-proven flowcharting, C/C++, Python, Node-RED and more.**
- **Industrial—Place an industrially hardened EPIC just about anywhere, from plant floors to remote sites.**
- **Controller—Gain real-time control, communications, data management and visualization in one unit, with an integral high-resolution color touchscreen."**

— **Benson Hougland**, vice president of marketing and product strategy with Opto 22

"As the makeup of the grid changes, so too will the way we transport electricity. Alternating current (AC) has largely been the dominant method of shipping power over long distances, however, DC can transfer up to three times as much energy over longer distances far more efficiently. Because of that, one technology that I'm really excited about for 2019 is HVDC (high-voltage direct current). With HVDC, we'll be able to move more power over even longer distances, from where it is produced to where it is most needed. And there are other benefits: connecting HVDC combined with the right controls can support and stabilize the system, provide ancillary services to make possible a clean, cost-effective energy future. As the adoption of HVDC continues, we'll gradually shift toward a hybrid grid that combines local decentralized systems with large transmission grids connecting countries and continents. I can even imagine a future system enabling exchanges of electricity all the way from the border of North Africa (with its solar energy resources) to the North Sea (with its growing offshore wind parks)."

— **Vera Silva**, GE grid solutions CTO