HOW CONNECTED TECHNOLOGIES ARE IMPACTING INDUSTRY TODAY

2019
EDITION

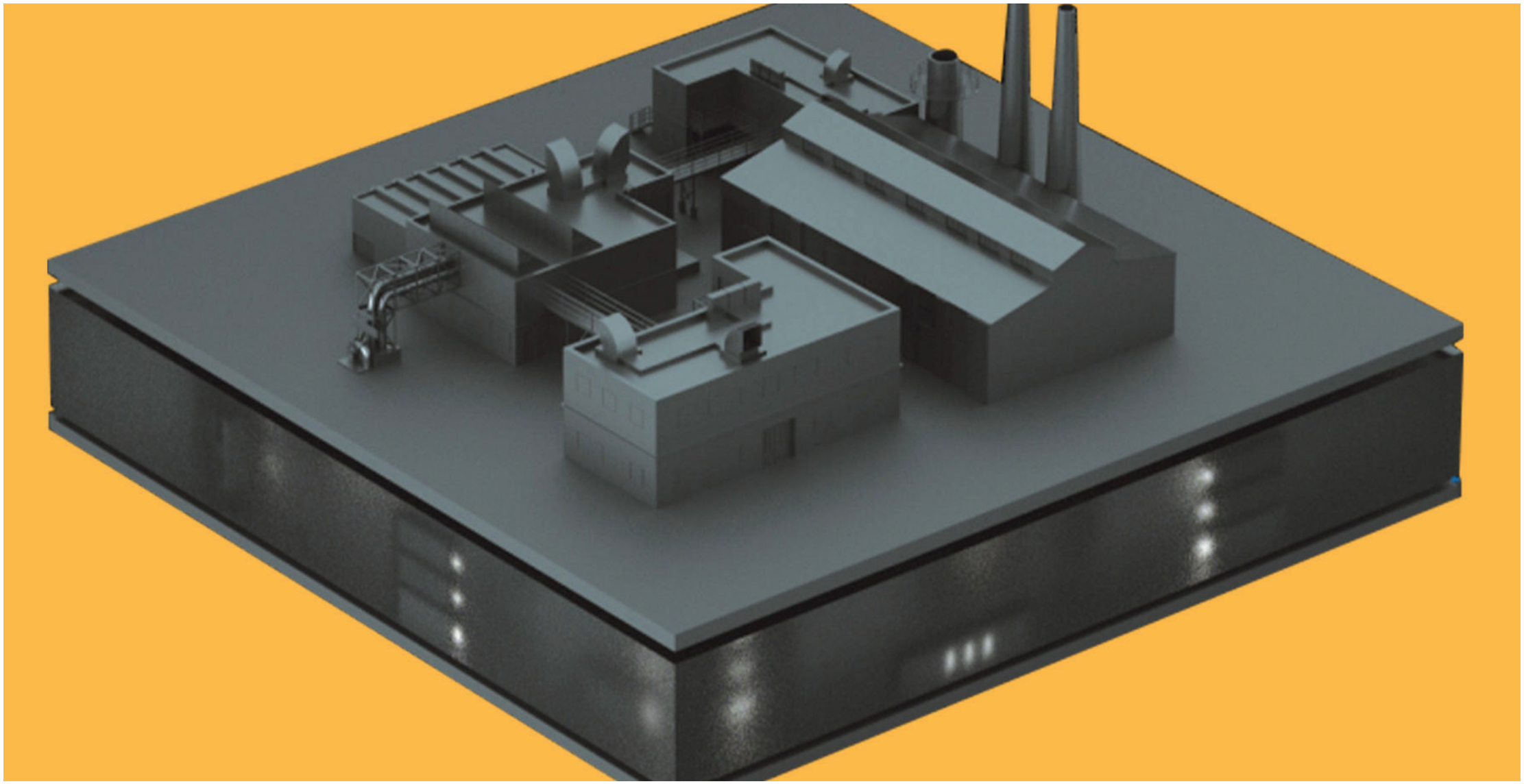
Discover the future of Industrial Internet of Things and Industry 4.0 in today's manufacturing and processing industries.

AutomationWorld®

Battle for Cybersecurity Spreads to Sensors

Even the lowest level of the Purdue model has become a target for hackers who want to attack manufacturing facilities. Automation vendors are scrambling to help users defend sensors and other intelligent devices.

James R. Koelsch , Contributing Writer



The Industrial Internet of Things (IIoT) is proving to be a double-edged sword for sensors. Sure, the connectivity that it brings is simplifying their installation and streamlining the distribution of collected data. But the IIoT has also made it easier for hackers to use sensors to break into industrial networks and cause trouble.

Another reason that sensors and other intelligent devices have begun to capture the attention of hackers is that most of these devices have not been designed for cybersecurity. Add to that the fact that they are designed to collect and pass along data within a network. “Vulnerabilities in these devices could give hackers the means to hijack a session, change the data or modify data collection patterns in a way that might deceive the end-consumer—be it a person or a

machine," says Dave Weinstein, vice president of threat research at cybersecurity supplier Claroty.

Vulnerabilities fall into two basic categories. The first is software bugs that hackers can exploit to launch attacks either internally against the control network itself or externally against some other target. The second category of vulnerabilities is the hardware. It is possible to launch an attack by manipulating the physical properties of the hardware itself, such as by using acoustics or electromagnetic waves to mount transduction attacks that spoof data.

"Hardware vulnerabilities, while scarier, are less common," Weinstein reports. "The majority of incidents relate to software bugs—and these are far easier to fix than hardware vulnerabilities."

Even so, these vulnerabilities can pose serious threats to manufacturing operations. "Attackers aren't targeting credit card numbers or other personal information," observes Eric Braun, engineering director for applications, gateways, and security at Emerson Automation Solutions.

When it comes to attacks on industrial control systems (ICSs), many of the perpetrators are looking to cause physical damage. For evidence, Braun points to the Triton malware discovered at a petrochemical plant back in 2017, which took aim at the facility's safety system.

The most likely vector for a hacker to launch an attack on a sensor or like device would be from the higher, Internet-facing layers of the Purdue reference model. Such attacks have typically begun with some sort of phishing scheme. "Attackers will target individuals and attempt to get them to open a malicious attachment or click on a malicious link," Braun explains. "These actions will allow the attackers to steal credentials, navigate through the network, and work their way down to the lower layers of the Purdue model." In a segmented network with firewalls protecting each segment, however, it is unlikely that a hacker would drill that deeply into a network.

A new attack vector

What is more likely these days is for hackers to attack sensors that are no longer at the bottom of the hierarchy outlined in the Purdue model. Today's IIoT devices communicate directly with whatever or whoever needs the data that they are exchanging. With this kind of connectivity, a drive for a welding robot, for example, could be transmitting utilization data to the robot's builder via the cloud. "It could be saying that, based on my duty cycle, I'm going to need to have a particular part replaced in approximately 17 days and four hours," says Dan Schaffer, product marketing manager at Phoenix Contact.

As helpful as this exchange of data can be for maximizing performance and uptime, the robot is talking directly to the Internet rather than going through a conventional control hierarchy. This direct communication circumvents the several layers of firewalls that would exist between the logical segmentations of a secured network following the Purdue model or security standards like ISA99 and IEC 62443. "If there is a flaw in the robot's operating system, it

Phoenix Contact's mGuard security router and other appliances can serve as firewalls in industrial networks

could allow the robot to be the victim of a buffer overflow or some sort of other communications attack," Schaffer notes.

Such vulnerabilities can sneak up on users who initially designed the network security of their manufacturing operations around the Purdue or other model. "These users think that they are adhering to the model, but really aren't," Schaffer says. "They think that they are following best practices but aren't."

Among the devices lulling users to let their guards down in this manner are the IP cameras that are appearing just about everywhere these days. "Visual imagery is becoming a key stream of data for processes," Schaffer says. "Cameras are cheap and easily deployed technologies that give you immediate visibility into what's going on at a given location." Because these devices were typically not designed with network security in mind, video streams transmitted over the Internet from remote locations can easily be an attack vector.

To drive the point home, Schaffer points to two vulnerabilities—overflow and authentication vulnerabilities—that were discovered recently in iLnkP2P, a widely used peer-to-peer software from Shenzhen Yunni Technology. More than 2 million IoT devices, including IP cameras, are affected. It is possible for hackers to exploit these vulnerabilities both to intercept the video streams and to steal device credentials.

Unprotected IP cameras are also among the IoT devices that are susceptible to a recent variant of the Emotet Trojan malware first discovered in the banking industry. The new variant enlists IP cameras and other IoT devices as proxies in command-and-control attacks,

thereby allowing Emotet to communicate through an intermediary, instead of directly with the command-and-control server.

Shield against attacks

To guard against these kinds of threats, security experts urge users to ensure that their sensors and intelligent devices are safely tucked behind suitable firewalls. And because no network is impregnable, they further advise users to develop a defense strategy that includes both dividing the network into logical segments to contain any intrusions that might occur and monitoring traffic to detect and stop those intrusions.

To support this effort, automation vendors have rolled out a number of devices that can serve as firewalls in industrial networks. For example, Phoenix Contact's FL mGuard line of cybersecurity appliances includes industrial-grade routers and concentrators. Even the company's I/O devices and safety bridges are designed to support cybersecurity. Devices like these use encryption to protect data and authentication protocols to permit only authorized traffic. They can also actively block traffic based on who it's coming from, where it's coming from, and the type of traffic it is.

"The technology is of the same type that the IT folks are using in their data centers," Schaffer says.

A big difference, however, is that Phoenix Contact and other automation vendors are packaging their technology for the control cabinet out on the factory floor. That means the devices are hardened to withstand the humidity, temperatures, and electromagnetic interference typically found in manufacturing facilities. Another important difference is that these industrial security devices are designed to be managed by a control engineer rather than an IT expert who manages networks for a living.

Emerson has incorporated many of the same defensive principles in its wireless technology, which is based on the WirelessHART protocol. "WirelessHART has done a lot to secure sensor networks," Braun reports. "It has proven to be a very secure alternative to some of the more unprotected wired networks."

Built-in security measures protect against many kinds of cyber intrusions, including replay attacks, eavesdropping, spoofing, man-in-the-middle, and denial-of-service (DoS) attacks. WirelessHART, for example, supports layers and encrypts all data with multiple keys using AES-128 bit encryption. "All devices on the network, moreover, are authenticated so a user doesn't have to worry about unwanted or rogue activity," Braun says.

In fact, the encrypted transmissions in wireless communications is currently filling a void at the lower levels of the Purdue model, according to Aurel Buda, factory automation product manager at Turck. "With the exception of wireless communication systems, hardly any communication protocols at the field level in automation supports encryption," he says.

Buda attributes this lack of support in part to the separation that manufacturing companies have tried to maintain between their automation and IT networks. In the past, the perception was that the separation made securing field-level communications unnecessary.

Another reason that Buda gives for the scarcity of encryption support at the field level is money. "Secure communication comes at a cost," he says. "Considering that large facilities consist of thousands of field devices, the utilization of intrinsically secure components would increase their costs significantly."

Scout for intruders

When coupled with the practice of shutting off unused ports, controlling the traffic permitted to cross firewalls limits the visibility that outsiders might otherwise have into the network. "Not knowing what is there on the network makes it much more difficult to do anything, let alone anything malicious," Schaffer notes. "It's difficult to attack something you can't see."

Although a good cyber defense will strive to make the devices on a network as invisible as possible to hackers, it will strive to maximize their visibility to authorized personnel overseeing the network. "You can't protect what you can't see," Weinstein explains. "So, at a minimum, users must increase the visibility of their OT [operational technology] network assets to include those sensors and other devices at levels 0 and 1 of the Purdue model."

For Weinstein, visibility goes beyond simply adding them to a detailed inventory containing a list of devices on the network and their configuration settings. Visibility also includes the ability to inspect the communications among those devices. "Industrial cybersecurity demands a deep understanding of each asset's function and the relationships among the devices," he says. "Only by dissecting and correlating these process automation conversations from every corner of the network can 100 percent visibility be achieved."

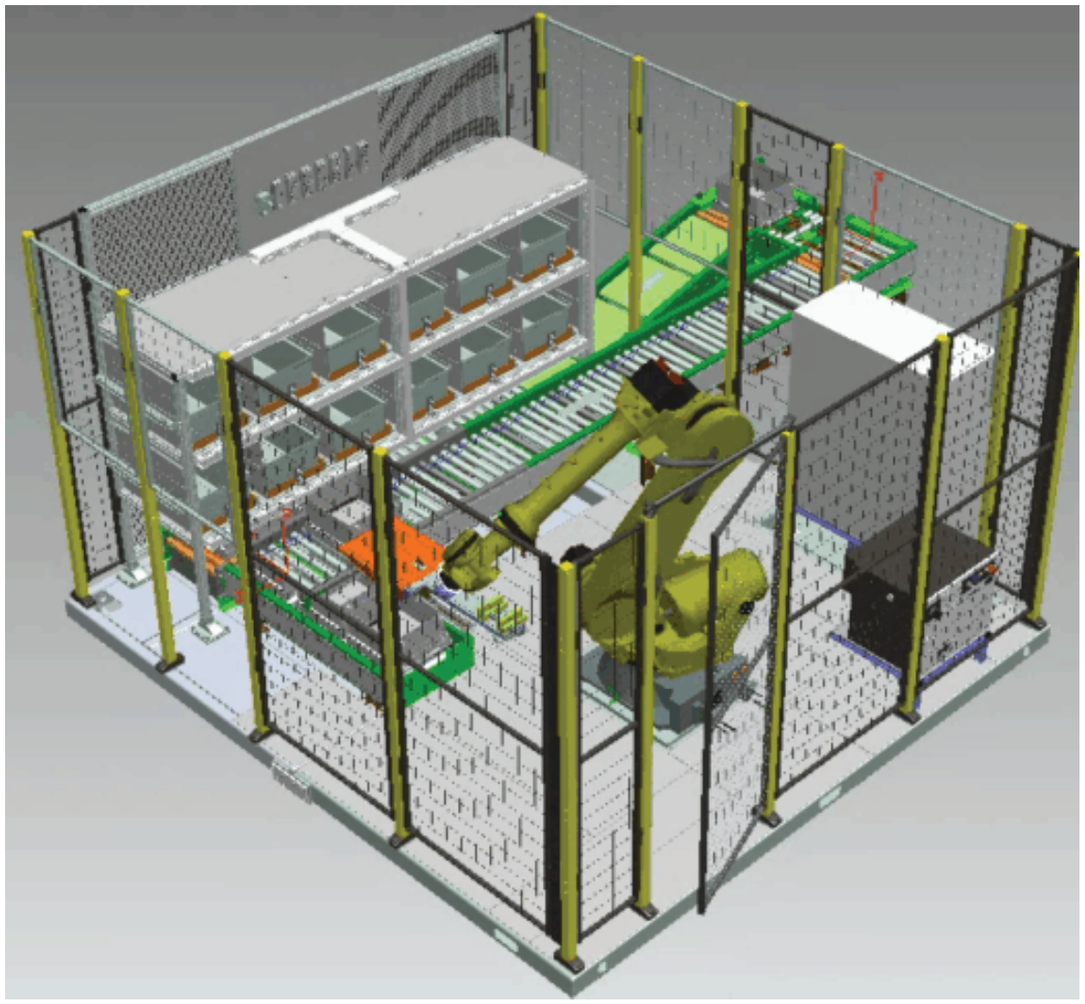
To help users achieve this goal, Claroty has developed tools that use multispectral data acquisition (MDA), a combination of passive monitoring, active querying, and application database parsing. Through passive collection, the tools automatically inventory the facility's assets and profile each asset's communication pattern. Active querying is a targeted process for gathering those details not collectable through passive monitoring. Because some of the richest and most up-to-date asset data resides in the configuration files used to restore systems from backup, MDA also parses these large and complex binary files. The resulting collection of patterns form a baseline that Claroty's software uses to detect security problems.

Ultimately, though, the visibility spectrum of all security measures must bring sensors and other devices under the same cybersecurity umbrella that is protecting the rest of the network. "Protecting automation infrastructures requires holistic cybersecurity concepts that have to be reevaluated in regular audits," Buda says.

Virtual Commissioning of a Robotic Cell

To develop a new robotic system for the material handling industry, JR Automation used a combination of Siemens simulation technologies to create a digital twin of the system that included the robots, PLC, HMI, and sensors.

David Greenfield, Director of Content/Editor-in-Chief

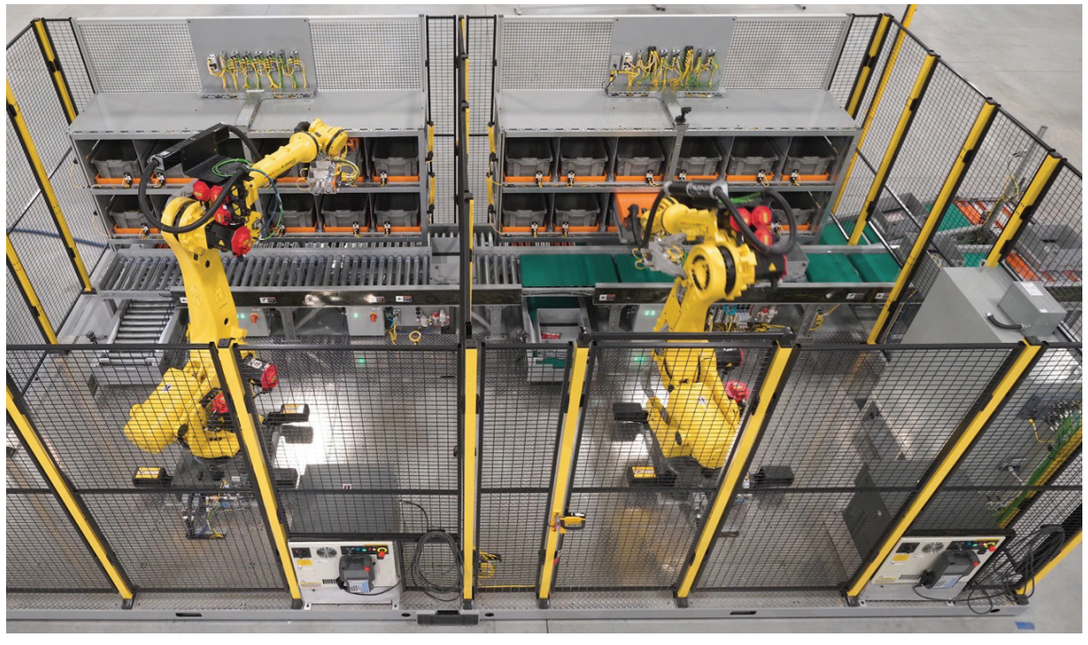


The robotic flexible sortation system (RFSS) in a one-robot configuration. Source: JR Automation

Digital twin technology has been generating a lot of buzz over past the past few years. While the potential for the technology is broad—from detailed remote maintenance and repair to artificial intelligence-enabled process optimization—the rubber is hitting the road early for this technology around virtual commissioning.

Automation World recently covered a digital twin application for virtual commissioning in an article detailing Burr Oak Tool's use of the technology to reduce time to market for its equipment and to train tool operators. More recently, we learned that JR Automation, a supplier of intelligent automated manufacturing and distribution technologies, is using digital twin technology to virtually commission a robotic cell developed for material handling applications.

At the 2019 Siemens Automation Summit, JR Automation's Matt Cagle, engineering manager, and Marc Walters, senior controls engineer, described their development of a patent-pending robotic flexible sortation system (RFSS) prototype using digital twin technology. The RFSS incorporates a Fanuc R2000-iC/165F robot, as well as proximity sensors, reed sensors, and photoelectric sensors (more than 25 of which were simulated in the digital twin). It also includes a Siemens S7-1515F programmable logic controller (PLC), and a Siemens TP1200 Comfort human machine interface (HMI). Software used to develop and simulate the RFSS included Siemens TIA Portal v15.1, Siemens Simatic PLCSim Advanced, and Siemens Process Simulate solutions.



Birds-eye view of a built RFSS in a two-robot configuration. Source: JR Automation

Robot in RFSS placing item in tray.

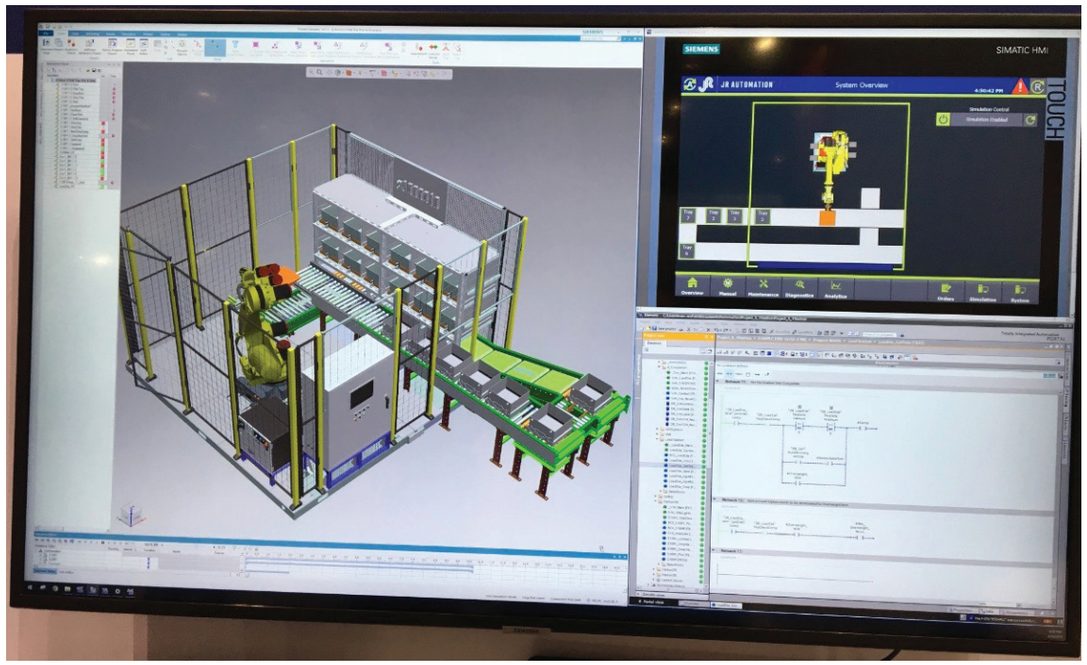
Up to 1,500 sorts per hour

The target application for the RFSS is essentially any operation that sorts product, said Cagle. Potential customers include e-commerce companies, like Amazon and Walmart, as well as users in the automotive, defense, and aerospace industries who employ kitting, sequencing, and kit assembly operations.

Cagle noted the RFSS was designed to be easily scalable, suitable for tight footprints, and capable of interfacing with virtually any delivery system—from conveyors, to autonomous vehicles, to fork trucks. The size of items the RFSS can sort is limited only to the payload of the industrial robot used in the system, he said. Robots in the prototype system have a lifting capacity of 165 kg, but some are capable of up to 1,350 kg (2,975 lbs).

Cagle pointed out that each robot in the RFSS is capable of 500 sorts per hour and that the RFSS is designed to allow up to three robots to be placed in series and controlled by one PLC, yielding a throughput of 1,500 sorts per hour. “Common sortation systems capable of 10,500 sorts per hour typically occupy approximately 25,000 sq. ft.,” he said. “But the RFSS system is capable of the same number of sorts while occupying only 12,500 sq. ft.”

“The design of the RFSS also limits down time due to maintenance activities,” Cagle added. “During maintenance on a multi-robot RFSS, a single robot can be bypassed while the others continue to run.”



View of the RFSS in Siemens Simatic HMI and configuration in Siemens TIA Portal. Source: JR Automation

Real-world discoveries

"During development, we quickly found value in the virtual commissioning process, as we discovered mechanical interference and programming issues we would not have seen prior to building out the system without virtual commissioning," said Cagle.

The typical development process for this kind of robotic cell involves programming and mechanical design teams working together, according to Cagle. But this collaboration doesn't tend to happen until those teams are on the shop floor physically building the system. "With early virtual commissioning, you can see if the locations where you're expecting to mount devices may be wrong—or the space needed for those devices may be missing," he said. "Virtual commissioning provides early feedback to mechanical personnel, so they don't have to scrap real world designs later."

During development, we quickly found value in the virtual commissioning process as we discovered mechanical interference and programming issues we would not have seen prior to building out the system without virtual commissioning.

He added that having the ability to visualize the complete system in advance of the build means that the customer can also have input to improve the design and help highlight potential safety issues.

Applied technologies

JR Automation built their simulations of the robotic cell in TIA Portal, using Siemens Simatic S7-PLCSim Advanced to incorporate

real world PLC and HMI data. With this combination of software, "we're not just simulating a robot, we're bringing all the real-world devices in the system into the 3D world," said Walters. This allows for complete virtual debugging of the devices. "Robot manufacturers have simulation tools for their robots, but nothing around it," , he said. "PLCSim Advanced brings all this together."

Using TIA Portal with PLCSim Advanced, you can communicate with the simulated environment and the hardware on the floor, Walters explained. "This software brings robots, PLCs, and HMIs together so that you can see all interlocks and handshake signals to determine if anything is missing. For us, the digital twin means that we can run an entire virtual material handling system on a PC. The PLC dictates how the robot handles materials and we can verify it in PLCSim Advanced. Then we use PLCSim Advanced to simulate the HMI in remote mode for debugging and commissioning."

Walters added that JR Automation also uses Siemens Process Simulate to create digital scenarios with multiple machines, robots, conveyors, and sensors. With Process Simulate, you can verify reach and cycle times, and do event-based simulations. Having the ability to do this in one environment means that there's no need to know multiple software or robot packages. "It's robot agnostic and shines with multiple robots," Walters said.

As with the Burr Oak Tools virtual commissioning application referenced above, a key aspect of this JR Automation project is the high-speed PLC connection to the simulation.

"OPC communications are too slow to connect virtual PLCs and simulation," said Walters, as they are in the 300-500 millisecond range. But the communication pipe connecting the virtual model and the virtual PLC in PLCSim Advanced allows for synchronized communications in the 15-20 millisecond range.

Return on investment

Cagle said they know they saved weeks of debugging time with this combination of software, but total ROI (return on investment) remains to be determined. "This is the first project we've done with this and we just completed it in April," he said.

Beyond initial ROI, another benefit Cagle highlighted is the ability for JR Automation to use this software to train users on use of the system. "In this virtual world, people can push buttons and try things to see what happens," he said. "Also, we can make faults happen in the virtual world to train users on how to effectively recover from them."

Hardened Wearables Bring Help Into the Field

Voice-controlled, hands-free wearable devices are bringing virtual and augmented reality to field service, training and other uses.

Lauren Gibbons Paul , Contributing Writer

HoloLens uses Microsoft Dynamics 365 Remote Assist to digitally place experts from all over the world anywhere in the field.

When you're 100 yards up in the air trying to fix a wind tower in a blowing gale, you don't want to take a chance that the piece of paper containing your work instructions snags on the pole and blows away. Such pitfalls might be a thing of the past thanks to a new class of industrial wearable devices that is enabling field service personnel to devote both hands to their tasks.

The equipment attaches to a hard hat or directly to the wearer's head, allowing navigation of critical repair data by voice, even when the wind sounds like a jet engine. Unlike wearable devices that might be used in gaming applications, these wearables are hardened to meet the rigors of industrial environments. They are still generally affordable—typically ranging from $2,000 to $5,000 per device before discounts—especially when you consider the potential ROI they can bring to industry.

"When the machine is down, the company is losing money," says Andy Lowery, CEO of RealWear, which makes ruggedized wearables. Being able to make quicker repairs is a huge benefit, he adds, and so is increased worker safety.

RealWear is one of the more well-known companies in this space, having recently announced its HMT-1 wearable Android-based

Chevron bought 100 HoloLens devices to use for remote assist in its refineries.

tablet. Ruggedized to work in the most punishing environments, the HMT-1 provides voice access to connected systems so a worker can access instructions, manuals, knowledgebases, email, chat—any type of document. It works in noise conditions reaching 95-100 dB.

Virtual "expert on call" is another hot application for industrial wearables, giving field service personnel the chance to have a live call for troubleshooting with an expert located elsewhere. This can even include sharing camera images. In its most rudimentary form, the application resembles something like FaceTime. Other "expert on call" options can also extend to virtual reality versions of experts to help solve problems.

Shell has begun rolling out RealWear's HMT-1Z1 voice-controlled, head-mounted device for use at several of its operational facilities around the world. The hands-free platform is the first commercially available device that can be used by field workers in highly restricted ATEX Zone 1 C1/D1 zones where potentially explosive gases are present.

The oil major is using the HMT-1Z1 for remote assistance—enabling a maintenance worker, for example, to get real-time assistance via a video call. The expert on the other end of the call can essentially see through the eyes of the onsite worker and offer over-the-shoulder assistance.

In addition to saving time and money, field service applications like this are widely viewed as being an effective way to transfer knowledge from a generation on the cusp of leaving the workforce

Shell has begun rolling out RealWear's HMT-1Z1 for remote assistance applications.

to those just coming up. "Folks are retiring in big numbers. These younger workers have to be supported," says Vincent Higgins, general manager of Connected Plant/Connected Worker for Honeywell, which is the global supplier of RealWear's HMT-1Z1.

Industrial wearables are able to provide workers in the field the information they need when they need it. "This allows the retiring experts to proactively capture information about the assets," says Todd Boyd, founder and CEO of Tacit, which provides software that can be used on a variety of hardware types. "That is very useful to someone who comes along two or three months later. Being able to access a digital envelope where you can access manuals and previous discussions is invaluable."

Various forms of reality

Industrial wearables getting the most attention at the moment employ virtual reality (VR), mixed reality (MR) or augmented reality (AR) to aid industrial applications. VR is a completely immersive digital experience (such as that offered by the Oculus Rift), providing a realistic simulation of a 3D environment experienced and controlled by body movement. It is used primarily in industrial design or training—because it doesn't allow for situational awareness, it is ill-suited for field applications. AR, on the other hand, layers digital, interactive objects on top of the physical environment, making it more appropriate for field work.

Somewhere in the middle, MR devices feature a world in which physical objects interact with digital objects. MR encompasses

The Trimble XR10 with HoloLens 2, introduced early this year, can be used for training and visualization without the safety risks.

the spectrum from AR to VR, blending the physical and digital worlds to produce new environments where physical and digital objects coexist and interact in real time.

Microsoft's HoloLens is an MR holographic computer that enables hands-free interaction with 3D digital objects. Announced early this year at MWC Barcelona (formerly Mobile World Congress), the Trimble XR10 with HoloLens 2 is a standout for training and field service use. One possible use would be for an oil company to create a 3D digital twin of an oil rig—a replica it can use for training and visualization without the safety risks, says Aviad Almagor, director of Trimble's MR program.

MR is also handy for design. "By placing design content on top of the physical environment, I can compare the digital asset with the physical construction to see if what was designed is being built correctly," Almagor says. "You can see information associated with this asset, you see it in context, and you see the information on top of it."

Chevron bought 100 HoloLens devices at roughly $5,000 apiece and is using Microsoft Dynamics 365 Remote Assist to digitally place experts from all over the world anywhere in the field, including locations that are difficult to reach. The investment has paid off in spades. Bisram Samlall, technology and innovation team lead at Chevron's El Segundo Refinery in California, says the HoloLens is "transformative" and provides "a tremendous reduction in operating expense." The remote expert application gives Chevron a competitive advantage, he adds. The refinery also

uses HoloLens for remote inspection of its assets in real time.

Whereas the HoloLens mixes the physical world with the virtual, the RealWear HMT-1 and HMT-1Z1, in contrast, remain firmly rooted in the real world. The heads-up display system resembles the old displays that pilots used to wear, augmenting reality while maintaining situational awareness, a la the old Google Glass.

A RealWear device is not used for training applications, but rather in the field. "It's used when I need to fix something and I want to see the data. I need to do that in a very non-obtrusive, non-compromising way," Lowery says. "This can't be a system where we are taking our hands away to give information."

Through its software and hardware combination, the HMT-1 is considered to be "voice-robust," meaning that it is capable of operating in the highest noise levels and without Wi-Fi access. "Our system maintains voice access no matter what," Lowery says. "You can barely hear yourself speaking, but you can still control the device with your voice."

The HMT-1Z1 has received the Intrinsically Safe certification, which goes far beyond what a consumer device provides—safety from ignition, for example. And it is reliable, with a failure rate of less than 0.1 percent. Application-wise, RealWear is focused for now on four spaces: oil and gas, energy, transportation and general manufacturing.

RealWear sold more than 10,000 systems in its first year and has also inked some high-profile partnerships. Honeywell has teamed up with RealWear for its robust, safety-certified system. "No iPhone can be brought into a plant. You have to have a certified device so it won't spark," Higgins says. "Typically, it has to be built from the inside out for that purpose."

A software approach

Not all applications—especially training and service in non-dangerous environments—require hardware that has a safety certification or even a high degree of built-in safety. Tacit's software allows users to leverage consumer-grade hardware they already have deployed, such as tablets, smartphones and other wearables.

"We're focused on things that are simple and pragmatic for remote guidance—being able to see what the worker is seeing in the field and quickly get to a common understanding of the problem," Boyd says. "These are simple things done around photo and video, but the user can bring in other elements as well. Everything is in the context of an asset."

Tacit also offers quick startup: Customers download the Tacit app, select the device they want to use, then launch the app on their device. "We are focused on it being simple, but if we can save an expert one trip into the field, the software pays for itself," Boyd says. All of the sessions are saved on the back end for reuse, which is a major plus in an industry that has many retiring personnel.

Honeywell is another vendor cre-ating software for wearables via its RealWear partnership mentioned above. "We are all about

building software for the next-generation connected digital worker," Higgins says. "We are enabling the field worker to be much more effective, safer and smarter in the way they do their work. We look for opportunities to co-brand and co-market with hardware companies." Honeywell sees its role as providing a service and technology to customers that fits under the heading of digital transformation.

Toward that end, solutions benefiting workers in the trenches is an important piece, says Greg Sullivan, director of communications for Microsoft Commercial, the division that brought out the HoloLens.

"We believe first-line workers have not directly benefited from the digital revolution to anywhere near the degree information workers have," he says. Devices like the HoloLens "enable first-line workers to be more efficient and productive, augmenting and enhancing the workforce, not replacing it."

In addition to enhancing safety and efficiency, industrial wearables "help solve for the pending skills gap, enable effective processes to be mined and workplace wisdom to be passed on," Sullivan adds.

Digitizing Legacy Pneumatics

Emerson’s Aventics Smart Pneumatics Analyzer connects to compressed air supply on machines to prove the benefits of the Industrial Internet of Things data analysis.

David Greenfield, Director of Content/Editor-in-Chief

Emerson's Aventics Smart Pneumatics Analyzer connects to compressed air supply on machines to prove the benefits of the Industrial Internet of Things data analysis.

Once they understand the concept of the Industrial Internet of Things (IIoT), the one question most companies have about it is: How do we get started?

Since no one wants to begin with anything too ambitious yet still be able to capture quantifiable results, Emerson has introduced a new tool to help pneumatic system users see the benefits of IIoT through data gathered from the company's own equipment. By connecting Emerson's new Aventics Smart Pneumatics Analyzer to the compressed air supply on an existing machine, Emerson says users can have access to instant analysis options for key machine characteristics, such as compressed air consumption and possible leakages.

The Aventics Smart Pneumatics Analyzer detects the system operating state, analyzes data, and provides processed information to users for status-oriented maintenance. While other similar technologies collect all available data and transfer it unfiltered, Emerson points out that the Smart Pneumatics Analyzer evaluates the data locally and uses it to generate information about the status of the system.

All data from the machine's valves, as well as from components connected to the I/O modules on the valve system, are read into the analyzer's microprocessor and processed via algorithms. These algorithms are based on Aventics pneumatic product engineering and applications (Emerson acquired Aventics in 2018).

The analyzer unit is a portable device in a case that contains a Smart Pneumatics Monitor, AS series air preparation units, and a

tablet for visualizing the live data. With this device, Emerson says it can show a user within minutes how to use IIoT-enabled data for insights into their machines.

Emerson notes that the analyzer can be used to collect data for condition monitoring to anticipate wear before it leads to machine downtimes. Once user-defined limits are reached, the analyzer can automatically send messages to ERP and MES systems, as well as maintenance or other staff. The company adds that data collected by the analyzer can also help optimize a pneumatic systems' energy efficiency.