Can our data truly be safe in the cloud? That’s the question many people are still asking when considering whether or not to use cloud-based solutions for storage of their most critical data.

Successful cyberattacks of consumer banking data and medical and government records have been relatively common, but manufacturing operations using the cloud generally have more layers of security and much better tools available at their disposal for locking down the critical intellectual property data and the operational equipment of the factory floor.

With the wave of new Industrial Internet of Things (IIoT) and Internet of Things (IoT) devices coming online with the move to smart manufacturing, many cybersecurity experts are still worrying that the manufacturing industry currently doesn’t
have the readiness required for adding on the burden of connecting to the Internet potentially millions of smart devices and sensors, most of which were not originally designed to be secure. But with new cloud-based solutions and extra networking safeguards, the migration of manufacturing to the IIoT may actually come off easier than expected.

Lessons of Stuxnet for OT (Operational Technology)

Perhaps the best-known cyberattack on a plant, Stuxnet, unleashed a zero-day exploit worm that successfully disabled the industrial equipment controlling the centrifuges at an Iranian nuclear plant in 2008-2009. In that case, the worm embedded computer code into the Siemens Simatic PLCs and STEP 7 software controlling the centrifuges, altering their speed and eventually damaging the systems. Since that attack, a German steel mill was shut down in 2014 by cyber thieves and, according to a March 2016 report in Wired magazine, the Ukrainian power grid was temporarily shut down late last year by a cyberattack.

“Stuxnet was this amazing piece of software,” said David Edstrom, chief technical officer of Memex Inc. (Burlington, ON, Canada), a developer of manufacturing execution systems (MES) software and Web-enabled automation systems. “It was a very impressive piece of software in how it had to hide and was activated later.”

“A lot of these systems were never designed to be secure.”

Most operational technology (OT) devices including the controllers, PLCs and sensors typically found in factory automation just aren’t designed with many of the security measures found in information technology (IT) systems. As manufacturers rush to embrace the IIoT, the industry needs to provide more security for the cyber-physical infrastructure of the manufacturing shop floor. The Stuxnet malicious code is the most famous example of a CPS (cyber-physical security) attack, added Edstrom, but others include MEDJACK, the highjacking of medical devices, as well as a tire-pressure monitoring system (TPMS) attack, and the remote hack of a Jeep vehicle later shown in a 60 Minutes episode.

“A lot of these systems were never designed to be secure,” said Edstrom. With more builders embracing Web-
connected machine tools on the shop floor through MTConnect and other protocols, the industry needs to get more-secure solutions around factory automation devices, he added.

“It absolutely can be done, you can put wrappers around the thing,” Edstrom said of retrofitting existing machine tools with the required shop-floor security.

Securing the Cyber-Physical Infrastructure

Software is involved in virtually all types of cyberattacks, although there’s a big difference in the types of vulnerabilities for OT versus IT infrastructure. “At its heart, there’s software doing this,” said Perry Pederson, co-founder and principal, The Langner Group LLC (Herndon, VA), a cybersecurity consulting company. “On the IT side, the software of concern is typically malware, viruses, worms or ransomware. But on the OT side, typically what you find in the more sophisticated attacks are features.”

Examples of IT vulnerabilities include zero-day attacks, buffer overflow, cross-site scripting, simple passwords, phishing schemes, and other malicious methods. But with an OT attack, it often involves features, Pederson said, which use the actual commands for the systems involved. “It doesn’t mimic the command, it is in fact the real command,” he said. “It is the exact command that an engineer would be issuing.”

In such cases, an attack on operational technology could involve just slight changes to the command that would affect manufacturing.

Cybersecurity threats have moved from simpler hacks by amateurs toward highly complex threats posed by nation states, according to cybersecurity consultants at The Langner Group.
product quality, Pederson said, not just dimensions, and would be classified as an Advanced Persistent Threat (APT). “It’s a very different ballgame, and these hackers are likely to have a different intent,” he said. “Of course, the criminals are getting slicker, as in the case of ransomware against a hospital. They’re getting better at this.”

Many APT attacks are carried out not by individuals but by nation states, he added, aiming not to steal things but to damage physical infrastructure in attacks that may extend over a long period of time. “The Ukrainian attack on the power grid last year was a hot topic on all the advanced cybersecurity forums,” he added, “and another one, Shamoon, wiped out all of Saudi Aramco’s computers.”

The Langner Group was founded in 2013, and Pederson said his partner, Ralph Langner, co-founder and managing principal, worked with the team that reengineered Stuxnet. The Langner Group currently offers cybersecurity services to manufacturers and has customers in the nuclear, chemical, and pharmaceutical industries.

In many cases, the sensors being deployed in the IoT are not at all secure, Pederson said. “That is a huge assumption that is being made,” he said. “A lot of these IoT devices will have Ethernet ports, you plug it in and the sensor will broadcast. Again, this was all designed around the concept of convenience, not security.”

Retrofitting such systems and sensors with proper security measures is possible. “It is, in fact, doable,” Pederson said. “Based on the school of hard
knocks, we have figured it out with Stuxnet.” Langner Group offers a cybersecurity framework, called Robust Industrial Control Systems Planning and Evaluation (RIPE), to give companies a blueprint for securing their cyberphysical systems.

“Everything is in there, the policies are in there, the schema is in there, and you can build it with that,” Pederson said. The company also built a software version, called myRIPE, that Pederson said includes all of RIPE’s policies, inventory, and tools for implementing change controls and management. Finnish utility TVO employs RIPE to assure OT security for the Olkiluoto nuclear power plant, which includes three nuclear reactors and an associated final fuel storage facility, and Pederson said the plant has been running the myRIPE software in a pilot project for about six months.

New Tools for the Cyber Fight

While many experts say the cybersecurity situation is worsening, manufacturing organizations have a substantial set of new tools to combat potential cyber theft.

“Manufacturing is a lower-value target for cyber-attacks compared to financial, personal, government or strong IP targets.”

“As we’ve seen with many types of devices [computers, smartphones, tablets], machines [cars], and systems [government, utility, energy, etc.], connectivity entices a particular group of people to attempt to find vulnerabilities,” noted Rob Black, senior director of product management for ThingWorx, a PTC (Needham, MA) business unit. “Manufacturing facilities likely will not be an exception as more companies adopt connected strategies. Some risks include data loss, leaking of private/confidential information, and even physical damage.”

In some cases, organizations may resist connectivity because of security concerns, but most of these organizations likely already have some kind of connected operation, Black said.

“For example, most manufacturers are connected to an ERP system to receive orders and notify the enterprise that the order has been completed,” he noted. “These organizations need to be proactive in building security into these systems, and keeping these security solutions up to date over time.”

Citing the recent attacks against manufacturing and infrastructure in Germany and Ukraine, Black said manufacturers need to bring traditional information technology security to operational technology networks. “OT is typically what runs in manufacturing plants. This includes robust system segmentation, keeping software up to date, ensuring that only authorized users can access systems, and committed network monitoring,” he said.

A number of technical approaches can be considered for helping to secure manufacturing operations. “What’s most important is that the organization treats security as
a top priority and has a purpose-built design to protect its infrastructure,” he said.

Important security considerations include device and user interactions, methods for providing security updates to devices, and the potential for hackers to locate devices through the Internet, Black added.

“It doesn’t mimic the command, it is in fact the real command.”

“With ThingWorx, PTC helps its customers address a number of security considerations, as the platform provides a flexible permission and visibility architecture. This includes design and run-time permissions, permissions down to the property level, and a visibility model based on organizational structure,” Black said. “Second, the latest version of ThingWorx offers sophisticated software and content management tools, which allow an organization to easily distribute security patches on an as-needed basis. Third, ThingWorx allows for device-initiated communication. Each device has a pre-set parent server to communicate with. Instead of worrying about millions of entry points, the secured server is the single method of IoT system connection.”

Locking Down Security Ops

This year, Siemens AG (Berlin and Munich) opened CSOCs (Cyber Security Operations Centers) in Munich, Lisbon, and
Milford, OH, that will allow Siemens’ industrial security specialists based at these sites to monitor facilities worldwide for cyber threats and to warn companies of security incidents and coordinate proactive countermeasures.

Siemens also expanded its collaboration with Intel Security for industrial security solutions at the Hannover Messe show in Germany, and released its new MindSphere cloud security offering. The expanded Siemens and Intel collaboration is meant to help protect industrial automation systems from increased cyber threats. The partnership leverages Intel Security solutions, such as anti-virus software, white-listing and security information and event management (SIEM) within the framework of plant security services. The offering encompasses Intel Security solutions, including McAfee VirusScan, McAfee Application Control, McAfee ePolicy Orchestrator (ePO) and McAfee Enterprise Security Manager.

MindSphere is Siemens’ open industry cloud offering that is being offered as a beta release. “MindSphere is a new service offering that people can get from Siemens, and the other piece is the analytics portion,” said Tom Elswick, director of business development, Automation Products, Factory Automation, Siemens Industry Inc. Digital Factory Division (Norcross, GA). MindSphere will form the basis of data-based services from Siemens, such as preventative maintenance of machine tools or integrated drive systems.

Fast, Secure Cloud-Based MES

Another new entry for the cloud is the MES software recently released by 42Q, the product division of contract manufacturer Sanmina (San Jose, CA). The 42Q cloud-based MES software has been used by Sanmina in the electronics sector for a few years, and the company in May announced a commercial version of the software.

Key features of 42Q include a fully cloud-based MES that as a cloud solution does not require an IT professional to install and configure but is said to be easily configured by businesses. The 42Q MES offers fast, robust functionality, with tracking, serialization, routing, work instructions and paperless travelers that can be configured and used the same day. With its on-demand pricing, the 42Q software’s pay-per-use subscription model gives businesses flexibility.

The growth in IIoT devices potentially exposes manufacturers to potential risks from cyberattacks. But in some cases, cloud-based solutions can actually improve upon security compared with many on-premises solutions.

“We agree that the potential risks increase with the growing number of interconnected devices and systems. The good news is that the providers of IoT and IIoT management and orchestration solutions are building stronger security into their technology,” said Srivats Ramaswami, 42Q chief technical officer. “Manufacturing is a lower-value target for cyber attacks compared to financial, personal, government or strong IP targets.”

A number of precautions are necessary for manufacturers to secure their manufacturing operations, he added.
“First and foremost, extending good practices and technologies from IT security into the manufacturing environment is a great start,” Ramaswami said. “Legacy on-premise systems are more vulnerable as there are more attack vectors available to cyber criminals.”

Sanmina uses best practices to secure physical and network perimeters, as well as securing devices and applications against vulnerabilities, said Manesh Patel, 42Q’s CIO. “More recently, we have transitioned to using white-listing technologies vs. the traditional black-listing solutions such as anti-virus. This has significantly reduced the risk of cyberattacks.”

Ramaswami said 42Q uses tier 1 cloud providers that have significant “out of the box” security capabilities. “On top of that, 42Q provides additional levels of security within its cloud solution, supplemented with network security that includes WAFs [Web Application Firewalls] to verify access to 42Q services,” he said.

“Also, 42Q customers have security measures and protocols within their facilities. This layered approach provides in-depth security. Additionally, the security investments and expertise from tier 1 cloud providers have put them on a stronger security trajectory than on-premise solutions.”

See the NEW FVM-3016DCL II at IMTS, it’s our next generation, premier double column bridge machine, that’s backed by more than 30 years’ of researching, developing, manufacturing and servicing high-precision machine tools.

Better stability. Higher profitability. Increased productivity. Ease of operation. This state-of-the-art machine is designed for high-speed, high-precision and high-productivity machining and is suitable for such industries as aerospace, automotive industries, mold making and job shops. Its heavy-duty frame offers extreme rigidity, with major parts of the machine constructed of high-quality Meehanite cast iron for superior stability. The oversized column and box-type beam construction provide excellent support and damping characteristics. The cross rail is designed with three rigid 55mm linear roller ways that support the load in vertical and horizontal directions. The entire X-travel of the table is fully supported by 12 pieces of sliding blocks, eliminating overhanging problems.

- Table Size: 122” x 57”
- Spindle Speed: 6,000RPM
- Table Load: 17,600 lbs.
- Spindle Power: 35HP (FANUC)
- Tool Capacity: 24 Tools
- X, Y, Z-axis Travel: 122”, 63”, 30.7”
- Spindle Taper: #50
- Distance Between Columns: 70.9"
- Table Height From Floor: 33.5”
- Transmission: 2-speed Gear
- FANUC 0i-MF Control
- Many Standard Accessories

Learn how the highly profitable NEW FVM-3016DCL II can work for you. Call your local dealer to see our comprehensive product line for all your machining needs. Or contact Chevalier at 800-243-8253. Visit us on the web at www.ChevalierUSA.com.