More and more, companies are talking about “going digital.” This includes concepts of interconnectivity described by the Industrial Internet of Things (IIoT) and Industry 4.0 that are enabled by advances in sensors, data analytics, computing networks, software and other technologies.

This special report contains recent news articles (2017) from Chemical Engineering magazine that give a timely and informative overview of digitalization as well as a number of articles (2016) on related cybersecurity issues.
Table of Contents

Section One: News articles

The Digital Transformation in the CPI .................................................................................................................. 4
An overview of how the chemical process industries are looking to the IIoT to help form new business models in a competitive environment

Refineries Explore IIoT Tools to Maximize Profits .......................................................................................... 7
New IIoT- and cloud-enabled digital tools and services give petroleum refiners new avenues to increase profitability and safety, but also require greater attention to cybersecurity

A New Mentality in Process Modeling ............................................................................................................. 12
Predictive process models enable more efficient operations and higher-value products

The Future of Safety Sensors is Here Now ........................................................................................................ 16
Wearable sensors enhance CPI worker safety and help close the approaching skills gap

Section Two: Cybersecurity articles

Cybersecurity: You Cannot Secure What You Cannot See ............................................................................. 21
Follow this guidance to understand today's cybersecurity risk landscape and take the necessary steps to create a sound industrial control system cybersecurity program, including the development of a comprehensive, in-depth cyber-asset inventory

Cybersecurity Defense for Industrial Process-Control Systems .................................................................... 26
Security techniques widely used in information technology (IT) require special considerations to be useful in operational settings. Here are several that should get closer attention

Plant Functional Safety Requires IT Security .................................................................................................. 32
Cybersecurity is critical for plant safety. Principles developed for plant safety can be applied to the security of IT systems
Today, technological advances are being made and implemented at an accelerated pace that is quickly changing the way we live and work. In our day-to-day environments we encounter “smart” objects, including our phones, cars and devices throughout our homes. And, these devices are being connected to each other. This trend is also taking place in industry, and while perhaps not as rapidly as with our personal devices, changes are occurring quickly.

What is the digital transformation?
More and more, smart sensors and equipment that contain smart diagnostic features are being used in industry to generate large volumes of data. Advanced computing technologies are allowing these devices to be connected to each other, and to use the data in a variety of ways. This growing interconnectedness of industrial operations is what is meant by the now familiar term, the Industrial Internet of Things (IIoT). As Marcelo Carugo, senior director Chemical and Refining Solutions, Emerson Automation Solutions (St. Louis, Mo.; www.emerson.com) states, “IIoT is partly about how we make data accessible and then get the right data to the right person, in the right format, at the right time — to make a decision. It’s about transferring digital data into digital intelligence by using the thousands of touch and sensing points in your plant and advanced analytics to help you recognize patterns and make decisions based on patterns instead of individual measurements.”

Industry 4.0 is another familiar term, perhaps more so in Europe than elsewhere, because it has其 origins in Germany. The term refers to this interconnectedness and related concepts in the digital transformation as a fourth industrial revolution, with the first three including mechanization, mass production and automation. Digitization, digitalization and “smart industry” are additional terms associated with the current movement toward the implementation of IIoT and the newest digital technologies. These terms are used...
A key driver for the digital transformation in the CPI is maintaining a competitive edge. Global competition, immediate communications and technological advances are creating an environment where businesses need to respond with increasing speed. Aligning production and business through the tools available with digitalization offers new possibilities for business models.

John Cate, commercial director for Surface Chemistry at Akzo Nobel N.V. (Amsterdam, the Netherlands; www.akzonobel.com) says, “We’ve been driving digitalization across our entire business. It’s all about efficiency and optimization. The digital world delivers more comprehensible and actionable data than we have ever had before. By replacing gut-feeling with comprehensive, realtime data, we are able to make better decisions. Whether this is about plant utilization, selecting R&D projects to fund, or sales accounts to focus on, we now have data work for us instead of the other way around.” He further explains that IIoT can help combine supply and demand intelligence and that it is essential in today’s environment, “Forget about getting ahead — just to ensure survival in today’s chemical industry, this [IIoT] should be high up on top management’s agenda. And the earlier you start understanding the IIoT and implementing digitalization, the more effective you’ll be in execution over time.”

Dow’s Bardin also expects digitalization to affect all aspects of business and production. “We are connecting data streams from R&D, marketing, supply chain and manufacturing to better serve our markets,” he says. And he also sees applications in safety and sustainability, “We can use robotics, augmented reality, big data, the digital twins and other aspects of Industry 4.0 to help achieve Dow’s 2025 sustainability goals and to continue to improve our safety performance. Safety, as well as cybersecurity, remain paramount as our industry continues to evolve.”

Earlier this year, Evonik Industries AG (Essen, Germany; www.evonic.com) confirmed its commitment to the digital transformation by establishing a digitalization subsidiary, Evonik Digital GmbH (Figure 2). The group is building digital expertise and developing digital business models under the guidance of Henrik Hahn, who holds the newly created position of chief digital officer (CDO). Evonik is also the first chemical company to join the Industrial Internet Consortium (IIC; www.iiconsortium.com), which is a global organization formed to promote the growth of the IIoT. Hahn says that it will become more and more common to realize truly personalized customer experiences, and in the future, there may be more competition between business models rather than between products or process technology. “Therefore we believe strategy, not technology, drives digital transformation,” he says.

**Technological advances**

Technology, however, is an enabler for digital transformation. There is much going on in this area, and new developments are occurring quickly. Several key developing areas are the following: **Sensors** have been ubiquitous in the CPI for decades. In recent years, however, advances in smart sensor technology and implementation have helped to make sensors one of the powerful enablers of the IIoT. Automation vendors, such as Siemens AG (Munich, Germany; www.siemens.com), Endress+Hauser (Greenwood, Ind.; www.us.endress.com), Honeywell Process Solutions (HPS; Houston; www.honeywellprocess.com), Emerson and many others offer a wide variety of sensors. Regarding sensors, Jeroen Pul, marketing manager and digital lead for AkzoNobel Surface Chemistry says, “More sensors equals more data. More data equals better decisions. In general, and at AkzoNobel, we’re employing more creative use of sen-

**Insights from industry leaders**

A key driver for the digital transformation in the CPI is maintaining a competitive edge. Global competition, immediate communications and technological advances are creating
sensors to measure all aspects that impact our business.”

In addition to developing new sensors, research is also going on to optimize placement of sensors — where do you best locate them in a plant? Stephen E. Zitney, at the Research & Innovation Center, U.S. Dept. of Energy, National Energy Technology Laboratory (NETL; www.netl.doe.gov) is studying underlying technologies for optimal sensor network design in a digitalization framework. Four key applications for optimization-based sensor placement technology include: better disturbance rejection in plants; better state estimation (using data from other sensors to estimate process variables that are not directly measurable, perhaps due to harsh operating environments); condition monitoring (the “health” of equipment); and fault diagnosis.

**Augmented and virtual reality** are familiar to some from the gaming industry. Advances in virtual reality software and more readily available hardware are enabling the use of these techniques in the CPI. Two of the targeted application areas are training and asset management.

One example of a dynamic simulator enhanced by a 3-D virtual plant is one that was developed and deployed at the Advanced Virtual Energy Simulation Training and Research (AVESTAR) Center at West Virginia University (Morgantown; www.wvu.edu) in collaboration with the NETL. The simulator is for an IGCC (integrated gasification combined cycle) system with carbon dioxide capture (Figure 3). NETL’s Zitney, who led the project, explains that it provides a very realistic, immersive training system for operators, engineers and students. It is currently being used at the university to educate chemical engineering students in process dynamics, operations and control. Vendors, such as Schneider Electric (Rueil-Malmaison, France; www.schneider-electric.com) and others, offer software for augmented and virtual reality simulations.

Another application where 3-D reality modeling has great potential is in asset management. Bentley Systems, Inc. (Exton, Pa.; www.bentley.com), for example, offers software that can combine photos taken from the ground, from drones and from laser scans to create 3-D reconstructions of facilities. These reality models can be used for planning maintenance, construction, training and more.

**Process modeling and simulation** capabilities are increasing as software becomes more advanced and more readily available (see A New Mentality in Process Modeling, pp. 22–25). One of the areas gaining momentum is in moving from steady-state process optimization that is run periodically, to continuous dynamics optimization and control. So called “digital twins” are realtime dynamic models that run alongside a functioning plant. These dynamic models can use data from sensors installed in the plant to match its realtime status and condition, and to carry out offline dynamic studies to help optimize its performance. These digital twins can also be used to train operators. Vendors such as Honeywell Process Solutions and others offer digital twin technology (also see Refineries Explore IIoT Tools to Maximize Profits, Chem. Eng. May, pp. 16–20).

**Convergence of IT, OT and ET**

To draw the full benefits of the digital transformation, cultural changes are needed in addition to technological ones. A better working relationship between operational technology (OT), information technology (IT) and engineering technology (ET) has been cited as an important step. Greg Gorbach, vice president of the ARC Advisory Group (Dedham, Mass.; www.arcweb.com) says, “Chemical companies are revisiting their own business processes and technology approaches as competitors and partners start to employ ‘digitized’ business processes and exploit the increasing convergence between OT and IT on the plant floor, to connect the enterprise as a whole to the extended supply chain and throughout the ecosystem.”

One of the areas where this convergence is most needed is in cybersecurity. While cybersecurity on enterprise IT has been well defined with firewalls, routers, anti-virus software and more, the needs on the OT side are less well defined. Eddie Habibi, CEO and founder of PAS Inc. (Houston, www.pas.com) says “Operational technology used to be thought of as ‘cyber-immune,’ but we’ve come to know that OT is also vulnerable.” Because “we cannot know what the cyber hackers are thinking or will be doing next,” Habibi sees cybersecurity as a compelling need for IIoT. On the OT side, he says that there are a tremendous number of assets that are unprotected, and part of the problem is that owners are often not aware of what cyber assets they have. Taking an inventory is a first step that he recommends. And on the cultural side, training employees in cybersecurity — even the most basic steps — is much needed.

The new technologies and advanced computing that are now available with the dawn of the digital transformation offer amazing possibilities. To put it into perspective, Dow’s Bar- din offers the following insight: “A key in this environment is to determine what makes sense for your business, develop a concise strategy that will achieve the desired objectives, and stick to the principles of that strategy to screen out the hype in order to find the nuggets of technology that can provide true, long-term benefit.”

Dorothy Lozowski
While several forces are creating conditions in which U.S. petroleum refiners can thrive in 2017 and beyond, success and profitability are not guaranteed (see sidebar, p. 20). Refiners must address changing supply and demand for individual refined products, fluctuations in crude oil prices and dynamic geopolitical factors, all while pursuing the industry’s ever-present imperative for efficient and safe operations. And refinery operations are taking place in an environment where the retirement of experienced workers is ongoing and the industry infrastructure is aging. The sum of these forces makes for a challenging environment for the nation’s 139 active petroleum refineries.

To strengthen their chances of success, refiners are increasingly exploring digital tools that take advantage of the emerging Industrial Internet of Things (IIoT), as well as advanced software for data analysis that can optimize process operations and reduce downtime. A host of new offerings are becoming available, and several were discussed at the annual meeting of the American Fuel and Petrochemical Manufacturers (AFPM; Washington, D.C.; www.afpm.org), which took place in San Antonio, Tex. in late March.

IIoT opportunity

The historical approach to refinery operation has largely been characterized by a “run to fail” mentality, where abnormal conditions and malfunctions were detected only when alarms arose or when a component broke or failed. The IIoT enables operators, engineers and plant managers to capture and analyze data so they can predictively identify potential issues before problems arise. A plant enabled by IIoT is equipped with a combination of sensors, automation systems and cloud-based technologies that are integrated with its current systems and data analytics capabilities. Streaming data from sensors and instruments allow plants to quickly assess current conditions and identify warning signs for abnormal operations. Beyond that, digital tools that enable plants to access the benefits of the IIoT and cloud computing are becoming instruments for boosting profitability.

The recent proliferation of sensors and software, combined with advanced analytics capabilities, has allowed plants to move to a predictive-maintenance system, says Paul Bjacek, the chemicals and natural resources research lead for business consulting firm Accenture (www.accenture.com). “But we’ve also seen what we call a ‘digital decoupling’ in the chemical process industries (CPI) and elsewhere, in which digital technology, including IIoT tools, is becoming a primary driver of value that goes beyond being a system to improve conventional processes,” Bjacek says.

According to proponents of IIoT-enabled digital systems and advanced analytics, the new tools can allow improved decision-making by aggregating data from multiple sources — cost-effectively generating data...
not available previously. It can then allow pattern recognition and analytics to guide actions based on that wealth of data. Benefits of such IIoT-enabled tools are said to include the following:

- Increasing the rate of asset utilization by reducing unplanned downtime
- Minimizing small efficiency losses from sources that may not have been detectable previously
- Raising operating efficiency through improved monitoring of energy usage
- Improving operations by continuous monitoring and by providing instant access to information that supports decision-making
- Maintaining the effectiveness of control loops, controllers and models over time, so the benefits of advanced process control are sustained
- Lowering overall process risk, thus improving safety
- Reducing maintenance costs

Focus on economics

In order to realize these benefits, though, refineries need ways to transform all of the captured data into information within a real-world, operational context. A host of companies have been developing systems for providing tangible value for IIoT-related data collection and analysis.

Martin Turk, a global solution architect for industrial clients at Schneider Electric SE (Rueil-Malmaison, France; www.schneider-electric.com) says, “There is a need to begin with the problems that need to be fixed and to ask how these new [IIoT-related] technologies can help solve them, instead of starting with the tools and trying to find what problems they could address. At Schneider, we’re taking a value-focused approach to IIoT, where the objective is to leverage the IIoT to make petroleum refineries more profitable,” he says.

In February 2017, Schneider introduced patented software known as Profit Advisor (Figure 1), which uses data analytics to measure financial performance of industrial operations in realtime. Profit Advisor works with process data historians to mine both past and realtime operating data, and then crunches those data through proprietary segment-specific accounting algorithms, the company says, to determine realtime operational profitability and potential savings.

Developed in collaboration with Seeq Corp. (Seattle, Wash.; www.seeq.com), Schneider’s Profit Advisor helps make economic-based decisions, in part by using continuous comparisons between designed performance and actual performance, Turk says. “It allows us to predict the impact of operator decisions on plant economics, making each operator more like a proprietor,” he says.

Profit Advisor measures the realtime profit performance of each major plant asset and unit operation, and the whole plant, so it is a departure from current cost-accounting systems that only measure financial performance of the overall plant, Schneider Electric says. The product is designed to allow individual plant personnel to “see and understand the return-on-investment and business value of their actions . . . in realtime,” the company adds, em-
powering them to make better decisions about operational profitability.

The system can also make it easier for workers to focus efforts on activities likely to provide the greatest financial returns and allows them to predict the profitability of possible changes before they are made, which can minimize risk and eliminate waste, Turk explains. For example, assessing the cost of a given period of downtime to fix a component could be compared to the costs of continuing to run a piece of equipment in a slightly degraded or suboptimal state for a certain period, Turk says.

Schneider Electric's Profit Advisor exists within a larger system of digital tools that includes Avantis PRiSM (process information signal monitoring), a predictive asset-analytics solution that can provide early notification of equipment health issues days, weeks or months before failure, and ARPM (automated rigorous performance monitoring). ARPM is a model-based online application designed to provide operators and engineers with real-time information about the performance of plant assets (for example, compressor efficiency) so that they can make better and faster decisions regarding what to do to correct for deviations from expected behavior.

PRiSM was originally designed for rotating equipment in other sectors, allowing operators to detect deviations and examine likely causes of problems, Turk explains, but his company is now moving this tool into refineries and adapting it to handle other equipment classes, such as heat exchangers and reactors.

Connected ecosystem

With all of the IIoT-related technology available, it has become relatively easy to collect data, but using those data thoughtfully to really make smart decisions about what to do with those data is what we are focused on, says Don Empie, communications director at Honeywell Process Solutions (HPS; Houston; www.honeywellprocess.com).

Honeywell is in the early stages of implementing its HPS Connected Plant initiative, which uses IIoT-enabled data collection and predictive analytics to enhance profitability across multiple facility sites, Empie says (Figure 2). To support the effort, HPS has created what it called “an ecosystem of OEMs [original equipment manufacturers],” each of which brings deep and specific expertise in different equipment classes. HPS Connected Plant is designed to harness the IIoT to tap into the deep knowledge of Honeywell and its network of suppliers and partners, Empie says, and by doing so, end-users are better able to make use of data enabled by IIoT systems.

A key part of HPS Connected Plant — and an example of how HPS is taking advantage of existing expertise — is Honeywell subsidiary UOP LLC’s (Des Plaines, Ill.; www.uop.com) Connected Performance Service (CPS) offerings, which were launched in autumn of 2016. UOP’s cloud-based software services continuously monitor streaming plant data and apply advanced analytics and machine learning to identify latent or emerging underperformance, alert plant personnel and make specific operational recommendations. The objectives include reducing unplanned downtime, increasing safety, raising efficiency and improving supply chain management.

Leveraging UOP process models and best practices, the CPS services create a “digital twin” of a plant that operates virtually in the cloud. “This ‘digital twin’ is kind of a utopia plant operating in the cloud that allows realtime comparisons between actual and simulated plant performance,” explains Zak Alzein, Honeywell UOP vice president and general manager for CPS.

“We are offering a holistic approach to optimizing asset capabilities and maximizing uptime,” Alzein adds, “by bringing together rigorous knowledge of process technology with new software tools.” These IIoT-enabled tools take into account equipment inputs and feed properties and link them via cloud computing to maintain performance over time and provide a platform for continuous innovation and improvement, he says.

Two critical strengths for CPS services are their machine-learning algorithms and the open partnership between HPS and UOP. Since each petroleum refinery is unique, broad process technology experience is important. “Our fundamental knowledge of the chemistry is married to the data analytics and the machine learning,” Alzein says. The UOP vice president thinks the technology world has reached an inflection point in machine learning, where these types of algorithms are found in many places, including in ordinary web browsing and smartphone applications. “Machine learning can eventually create almost a ‘self-healing’ plant that can use the IIoT to quickly introduce software updates and security patches, and proactively manage its own maintenance, for example,” Alzein says.

Thus far, Honeywell UOP has announced three plants in which the services will be used, with more announcements forthcoming. The facilities announced to date are the Binh Son Refining and Petrochemical Co. Ltd. complex in Quang Ngai, Vietnam, the Delek Refining Inc. refinery in Tyler, Tex., and the Al Waha Petrochemicals Co. facility in Jubail, Saudi Arabia.
“Adoption is slow in this industry, but the plants are recognizing the potential benefits of these tools and these approaches,” remarks Alzein.

**Remote process support**

The March AFPM meeting also saw the launch of the KBC Co-Pilot Program, which is a service using simulation technology with IIoT and cloud computing tools to access the expertise of strategic and technical consultants at KBC Advanced Technologies (Walton-on-Thames, U.K.; www.kbcat.com). In Q3 2016, KBC became a wholly owned subsidiary of automation company Yokogawa Electric Corp. (Tokyo, Japan; www.yokogawa.com).

The Co-Pilot program is the initial manifestation of the KBC Production Core, which envisions automation of all aspects of production operations, with integrated technology and consulting best practices that leverage cloud computing and the IIoT.

The first release under the program is a Refinery Unit Performance Co-Pilot, says Jason Durst, Co-Pilot Program Manager at KBC, and is focused on driving value for clients by providing them with the tools and expertise to collaboratively maximize the potential from oil-refinery process units. Future releases will add Co-Pilot solutions for other asset types.

The Refinery Unit Performance Co-Pilot service monitors process operations at a facility in real time to remotely support the plant with expertise and insight that supplements the plant’s own capabilities and resources. It tracks data from multiple sources, including actual operating units and simulation programs, says Durst, and through Web-based dashboards, allows both clients and KBC subject matter experts to analyze the raw data and standardized unit performance indicators to make decisions to increase unit performance.

Co-Pilot is focused on bringing value to the client, Durst adds, and it is suited to process operations where the following may be true: managers are not confident that their operating plan is always realistic and achievable; an inexperienced workforce means the unit operation often misses plan; engineers lack the tools and knowledge to maximize profit or reduce risk; or operators do not always automatically know when they are deviating from plan.

Co-Pilot assures asset operators that their simulation and planning tools are up-to-date through the cloud, and that any adjustments made or recommended by their engineers result in optimal process performance and safe operation of equipment within recognized limits, KBC says.

**Cybersecurity risks**

The proliferation of internet-connected devices and sensors associated with IIoT technologies, coupled with increased use of cloud computing and data-as-a-service models, has further raised cybersecurity concerns for industrial control systems. Attention on the topic continues to grow and AFPM meeting organizers included a session about cybersecurity and automation systems. Among the themes explored by speakers was...
U.S. PETROLEUM REFINING OUTLOOK

U.S. Dept. of Energy data indicate that U.S. refining capacity grew by almost 2% in 2016, and Chet Thompson, president of the American Fuel and Petrochemical Manufacturers (AFPM; Washington, D.C.; www.afpm.org), called 2016 a good — but not great — year for the petroleum refining industry, with exports of refined products robust at 3.3 million barrels per day (bbl/d) and demand projections remaining strong.

AFPM leaders commented on the positive outlook for their industry that has been set up with the new Trump Administration in the U.S. Greg Goff, who chairs the AFPM board of directors says, “We are at a tipping point for opportunity now, and we as an industry have to rise up with a sense of duty and be leaders. We have a business-friendly White House, we have executive branch agencies that are not hostile to our industry, and we have a center-right Congress.”

Aside from the “seismic political shift” that led to Trump becoming President and the Republican Congress, Thompson pointed out that AFPM members have what he clearly sees as allies in Rick Perry (former Texas governor and new Secretary of Energy), Rex Tillerson (former ExxonMobil executive and new Secretary of State), and Scott Pruitt (former Oklahoma attorney general and new EPA administrator).

While no mention was made of addressing climate change concerns, Thompson and Goff both accepted the presence of Federal regulations for the industry. “Governmental regulations are not necessarily bad, but we need transparency in how they are made and how they are justified and how they are written,” Thompson says. “We’re not opposed to regulations as long as they are reasonable and cost-effective.

Thompson called on Congress and the Administration to bring about corporate tax reform and repeal the Renewable Fuel Standard (RFS), as well as expressed support for the White House America First Energy Plan (www.whitehouse.gov/america-first-energy). The document, which appeared shortly after Trump’s inauguration has been criticized for failing to mention renewable energy, climate change and investment in utility grid infrastructure.

the need to merge the operational technology (OT) sector of the business with the information technology (IT) area, the traditional “home” to cybersecurity countermeasures (for more information, see Chem. Eng., June 2014, pp. 30–35).

Eddie Habibi, founder and CEO of PAS Inc. (Houston; www.pas.com) spoke about the need for petroleum refineries and other CPI companies to undertake a comprehensive inventory of what he calls “cyber-assets,” which includes all control-system sensors, input-output devices, computer workstations, mobile devices, and others. “You can’t secure it if you don’t know it exists,” Habibi says. “If you have a complete inventory of cyber assets, you can identify vulnerabilities and determine if unauthorized changes have occurred,” he notes (for more information, see Chem. Eng., October 2016, pp. 60–64).

The traditional “IT-centric” view of cyber endpoints for industrial control systems neglects many parts of the distributed control systems (DCS) and programmable logic controllers (PLC) that exist below the level of information networks. That portion, which Habibi termed the “production-centric” cyber endpoints, consists of 80% of the assets that require inventorying, he says.

Aside from the comprehensive cyber-asset inventory, Habibi also recommended that companies conduct a prioritization exercise for the costs and consequences of various types of cyberattacks, or other incidents in which cybersecurity may be at risk unintentionally or non-maliciously. This can better ensure that resources are devoted to cybersecurity in a thoughtful way.

In addition, attention should be paid to how cyber assets are backed up, and how recovery from a cyberattack would be accomplished.

According to Habibi and others at the meeting, the cyberattack “threat landscape” is growing, but so is the recognition of cybersecurity’s importance at a grassroots level. It is important to realize that industrial control systems have characteristics of a living organism that continually change, Habibi remarked, and also that eliminating the problem of cybersecurity will never be accomplished with a single solution.

Another speaker at the cybersecurity session was Gavin Mead, principal, cyber services for KPMG LLP (New York; www.kpmg.com/us). Mead also addressed the need for cybersecurity to extend into the OT world. Cybersecurity has been a hot topic in IT for several years, but the wave of interest in securing OT components from cyber threats has been more recent.

Mead pointed out several reasons for why the cybersecurity threat is growing. These include the fact that industrial automation systems are more sophisticated now, and that real-time business decisions are increasingly made with information from the control system. In addition, commoditized IT systems are common, and they support the OT system. Meanwhile, cyber attackers are increasingly sophisticated and well-funded.

The greatest risk to companies comes from failing to spend their financial resources for cybersecurity in the smartest way, Mead says. “We spend a disproportionate amount of money on assessing the problem and not enough on what the remediation will look like,” he says. “That should come sooner in the process.”

“The topic of cybersecurity is well discussed now, but there is still not enough sharing of information about cyberattack incidents,” Mead says.

Jeff Melrose, principal technology strategist for cybersecurity at Yokogawa Corp. of America (Sugar Land, Tex.; www.yokogawa.com/us) added a new dimension to the AFPM session by discussing potential cybersecurity threats associated with drones. He says drone technology, even that available to hobbyists, has evolved to the point where their range is up to three miles, and they have the ability to maintain a stable hover or follow a target autonomously for 30 minutes more.

A drone equipped with electronic transmitters could theoretically follow a target and be directed remotely to disrupt wireless communications or surveil. Melrose suggested that refineries should begin instructing physical security personnel to look for drone activity near plants and should update procedures to include what to do if a drone approaches a facility.

Scott Jenkins
When they hear the words “process modeling,” some may envision an engineer sitting in front of a laptop waiting for a distillation column flowsheet to converge. While flowsheet simulations are still an invaluable step for engineering design, process modeling is becoming an overarching part of operations as a whole, serving various purposes throughout the entire operational chain — from conceptual design to continuous process improvements to end-use product applications.

Modeling product performance
At Optimize 2017, the users’ conference for Aspen Technology, Inc. (Bedford, Mass.; www.aspentech.com), David Kolesar, senior engineering leader from the Dow Chemical Co. (Midland, Mich.; www.dow.com) presented an example where process modeling at the molecular level allowed Dow to fine-tune polymer products to meet the requirements of various application tests while also decreasing batch cycle times. When certain products began failing application tests, and a root-cause analysis indicated no issues with raw-material quality, the team turned to process modeling to evaluate the polymers’ intrinsic properties, focusing on the molecular weight. However, it was determined that the batches were indeed achieving the target molecular weight, so another factor had to be the culprit.

Through extensive modeling using Aspen Polymers and Aspen Dynamics, the team determined that the polymers were rearranging and branching, impacting the structure and ultimate application properties of the polymer. These structural changes were deemed to be the source of the failures. The team was able to model the relationship between the polymers’ intrinsic properties, structure and application requirements to “reverse engineer” the best polymer structure for the application tests. This modeling capability allowed Dow to “work backwards from customer needs,” explained Kolesar, listing adhesive stickiness and noise creation among the important application properties being evaluated for these polymers. Kolesar highlighted model-guided experimentation — completing modeling activities prior to plant trials and pilot work — as a major driver in expediting process advancement and reducing the time to market for new products.

With its Bonfire property predictor tool, NOVA Chemicals Corp. (Calgary, Canada; www.novachem.com) brings the ability to model product applications straight to its customers. Bonfire was developed to help NOVA’s resin customers evaluate different structures of multilayer films by modeling key properties, such as secant modulus, moisture barrier and bending stiffness. For instance, users can predict how employing a new polyethylene resin will impact film properties before conducting physical trials. “Running these simulations can eliminate some film structure designs that would not be expected to meet property targets and identify structures that are more promising,” says Dan Ward, senior technical service specialist and developer of the Bonfire tool. A new release of the tool introduced a larger resin database, and work is currently underway to incorporate machine direction tear and penetration energy, as well as a blown film calculator, into the model. “Longer term, we are also evaluating new calculations for film creep, tensile and impact strength and optical properties, as well as accounting for
end-use environmental factors, such as storage temperature and relative humidity,” explains Ward. “We believe that Bonfire is the only integrated model that calculates many film properties simultaneously and allows the user to estimate property tradeoffs when developing a multilayer film or making a change,” he says.

At a recently opened technology center in São Paulo, Brazil, scientists from Solenis (Wilmington, Del.; www.solenis.com) develop models for a cooling-tower pilot plant (Figure 1) to simulate various treatment processes for water samples from customers’ cooling towers. “Simulating customer processes in a laboratory setting allows us to investigate a wide variety of problem-solving scenarios in a controlled environment,” says Edmir Carone Jr., technology and development manager at Solenis. These efforts have not only aided in the selection of appropriate cooling-water treatment options for specific processes, but have also allowed users to reduce their consumption of water and treatment chemicals. Furthermore, the cooling-tower models have accelerated the development of new cooling-water treatment chemistries, according to Carone. Among the important parameters simulated in the cooling-tower models are water temperature, skin temperature, pH, oxidation-reduction potential (ORP), conductivity and scale, and well as information from on-line corrosion monitoring.

Visualizing complex scenarios
An incident involving the accidental release of chemicals, whether via explosion, fire or toxic dispersion, is an extremely complex situation that holds a number of potentially dire consequences. “Conducting a modeling analysis to determine the potential impacts from a hazardous toxic release is important in order to understand the effects it could have on personnel, nearby communities and equipment,” says Tiffany Stefanescu, senior product specialist and meteorologist for Breeze Software, a division of Trinity Consultants (Dallas, Tex.; www.breeze-software.com). Incident Analyst, a program offered by Breeze Software, models the consequences of accidental chemical releases (Figure 2), and provides practical information for emergency response planning, facility design, real-time assessment of hazards and reconstruction of past incidents. The software is also set up so that users can conduct U.S. Environmental Protection Agency (EPA; www.epa.gov) Risk Management Program Offsite analyses, adds Stefanescu.

With numerous mathematical models included and a database consisting of over 180 chemicals and mixtures, Incident Analyst can assess the potential consequences for a release event, taking into account site meteorological conditions and levels of concern (LOC), the threshold values above which a hazard might exist. “For each LOC modeled, Incident Analyst will estimate a hazard zone where the chemical concentration, overpressure and thermal radiation values are predicted to exceed that LOC at some time after
a release begins,” says Stefanescu. The modeling capabilities in Incident Analyst also allow Breeze to develop custom realtime modeling systems that read onsite meteorological and monitored process data, and then automatically run the models within Incident Analyst using predetermined scenarios to produce realtime concentrations. “This realtime modeling capability is becoming increasingly popular and even mandatory for certain facilities, since it allows companies to make better operational decisions and address public concerns based on realistic conditions,” comments Stefanescu.

For some extremely complex or sensitive process anomalies, combining several pillars of modeling, such as fluid dynamics and structural stress analysis, can be helpful in gaining a full evaluation of the process. One such example of a complicated scenario that requires “co-simulation” is the investigation of the acoustics of flow-induced pipeline vibrations. Acoustic data are useful for evaluating the extent that a damaged pipeline will affect fluid flow, and also to estimate the damaged pipe’s suitability for continued operation. Typically, these types of assessments are first approached using industry design codes and empirical data. For instance, the U.K.’s Energy Institute (London; www.energyinst.org) provides guidelines and calculations to determine the likelihood of failure due to vibration, but doesn’t necessarily provide methods for assessing or mitigating the vibrations, explains Matt Straw, managing director of Norton Straw Consultants (Derby, U.K.; www.nortonstraw.com). This is where the detailed analysis facilitated by co-simulation becomes critical. If these initial evaluations indicate the presence of a problem, a rigorous model that couples computational fluid dynamics (CFD) and structural analysis tools (Figure 3), and ultimately, fatigue analysis, is required, says Straw. This allows operators to ascertain the timeline for making modifications and also how the vibration may impact process integrity. “The work that we’ve done has often involved assessing the fluid dynamics of the system to see if the energy content of the system or the turbulence generated by the flow could cause any resonance in the structure. Then you can couple that with analysis of the structure itself to see how it responds,” says Straw.

Site survey data can be used to recreate the geometry of the system, and if damaged, this will show any piping irregularity, which is input into the model. From there, simulation is used to produce the time history of the pressure generated inside the pipe from the fluid flow and translate that into the effects on the structural behavior using finite element analysis (FEA). Finally, the modeling data are used in a fatigue assessment that will determine if the design life is threatened or if mitigation is required.

Straw emphasizes that traditional process simulator software is not designed to do these sorts of analyses, and that is why using multiple platforms like CFD and FEA is necessary to ensure a robust model of both the process system and the mechanical structure. He has also used co-simulation for selecting materials of construction for piping and equipment that may experience very low temperatures due to Joule-Thompson cooling.

Underlining the importance of integrating multiple simulation and modeling pillars, Siemens Product Lifecycle Management Software (PLM; www.siemens.com/plm) launched its SimCenter platform in 2016, which brings together a number of software and analysis tools. “Essentially what is designed using process simulation can be analyzed using CFD and DEM [discrete element modeling]. That analysis tells you how you can actually employ your design before it is implemented,” says Ravi Aglave, director of Siemens PLM Software’s Chemical & Process Industry division.

A key facet of SimCenter is the ability to produce digital twins — virtual, sensor-enabled representations of an individual equipment component or process that allow engineers to predict the effect of process changes or upsets. “If you can know how equipment will perform under different conditions by using a digital twin, then you have a predictive ability that can be used to control that equipment,” explains Aglave. Modeling with a digital twin may pinpoint specific process variables that should be measured to better predict process behavior. “Based on those expectations, you can modify the control algorithm to achieve the optimum for...
that new condition," he continues. This enables a quicker response to changes in operating conditions or product distribution demands.

**Looking to the next generation**

Because modeling and monitoring capabilities have matured in recent years, engineers have unprecedented amounts of data at their disposal, but the best ways to utilize so-called big data are not always clear. “Many engineers do not understand what the meaning of ‘big data’ is, let alone the application of it to the chemical process industries [CPI]. Ask ten engineers and you would be at risk of getting ten or more different versions,” comments Andy Howell, chief executive officer of KBC Advanced Technologies Ltd. (Surrey, U.K.; www.kbcat.com). In short, says Howell, big data and the availability of smart devices and mature process models — ones that go beyond traditional engineering design to incorporate operations, planning and logistics via cloud-based infrastructures — are driving the emergence of predictive, rather than reactive, analytics. “The process simulator has graduated from the design system of the past to the operations system of the future,” says Howell. He suggests that a marriage of thermodynamic simulation with equipment degradation modeling (considering erosion, corrosion or other types of damage) is essential for predictive analytics to become the CPI norm. Furthermore, energy management is another sphere where process modeling is helping CPI facilities maximize production. “Recent innovations in process simulation now model the gas turbines and power-generating equipment within the flowsheet, including the fuel and air quality from the process. This means an operator can optimize production versus power and can reduce energy costs,” explains Howell.

At AspenTech’s Optimize 2017 event, a panel of experts discussed some trends in modeling that are moving the industry forward, including big data and the push toward predictive analytics. A common thread among the panelists was that big data is not only changing how facilities operate, but also how engineers think. The panelists agreed that this shift in mindset should begin with undergraduate chemical engineering education, as data science and statistics become more intertwined with traditional engineering tasks. “A wide spectrum of expertise is required from engineers. Statistics and data analysis courses are crucial in chemical engineering education,” emphasized John MacGregor, distinguished professor emeritus at McMaster University (Hamilton, Ont., Canada; www.mcmaster.ca).

Kai Dadhe, head of the Computer Aided Process Engineering and Automation division of Evonik Industries (Essen, Germany; www.evonik.com), commented: “Digitalization and big data are about breaking silos, with respect to both data and disciplines.” Ultimately, this holistic mentality will ensure that engineers are well equipped for the most demanding process modeling tasks in the CPI.
For many years, sensors have been used in the chemical process industries (CPI) for many activities, including monitoring the health and safety of employees. In these applications, sensors were especially helpful when used to accumulate data on workers, identify potential exposures to hazardous chemicals and to monitor confined space entry and dangerous inspections. However, many of the sensors that were used for these applications were large and had to be carried by hand or placed at a specific point within the plant or process line. More recently, the advent of smaller, advanced sensor technologies and the ability to locate them in wearable items, such as helmets, smart watches and smart glasses, and connect them to today’s powerful communications infrastructures, all contribute to enhance the safety of CPI employees.

“With the advent of smaller sensors and microprocessors, monitors are becoming compact and wearable. They are wireless, so it is no longer necessary to have wires that interfere with an employee’s work, and they can transmit the information to the Internet of Things or the cloud so that data can be downloaded into a computer and analyzed in real time,” explains Russell Hayward, managing director of Strategic & Technical Initiatives with the American Industrial Hygiene Association (AIHA; Falls Church, Va.; www.aiha.org). “Smaller, wireless sensors have the potential to change the health and safety paradigm regarding collection of employee exposure data” (Figure 1).

For instance, Hayward says, with the proper procedures and processes in place, wearable sensors can now be placed on all operators in a particular chemical plant unit and set to alert workers when they enter an area of excessive exposure to a particular substance. “When the alarm triggers, the exposure is investigated and the data points are captured in a central repository and analyzed. It can then be determined when, where and why the alarm triggered and the situation can be corrected in a virtually realtime manner,” he says. “Prior to advanced sensor technology, we didn’t have the opportunity to monitor all operators and identify the areas of risk that operators were encountering on a task-by-task basis.”

Another game changer is the ability to place arrays of these advanced, miniaturized sensors around operating units and along facility fence lines and, during emergency response situations, link them to a communications infrastructure and provide virtually realtime data analysis. “In these situations, the data can be used to make emergency response decisions.”
The future of safety is here today

If this safety-enhancing sensor technology, coupled with wearable devices such as helmets, smart watches and smart glasses, seems like something that might be seen in the future, think again. It’s here now and is slowly beginning to make its way into the world of industrial processes.

For instance, Honeywell (Morris Plains, N.J.; www.honeywell.com) offers its Connected Worker solution, which provides safety intelligence to reduce worker injuries and prevent loss of life from “man-down” scenarios. The solution collects and provides sensor fusion, which refers to data collected from a variety of sensors on a worker that are compiled to provide an accurate picture of what that worker is experiencing. The solution monitors workers for toxic gas exposure, breathing, heart rate, posture and motion. The resulting data and actionable intelligence are displayed remotely on a visual, cloud-based dashboard, giving plant managers and incident commanders the information needed to better anticipate unsafe conditions and prevent potential “man-down” scenarios that could threaten worker safety.

“Employers are always trying to operate a safer environment, so we tried to create a solution that would help them with that. It can help protect the lone worker — those in hazardous areas or remote locations — because it uses the sensors and the connectiv-

DOWNTIME IS COSTLY

Are you using a permanent tube plug for continuous operation?

Pop-A-Plug® Heat Exchanger Tube Plugging System

Welding plugs into your Heat Exchangers can damage the tubes & tubesheet resulting in costly unplanned downtime.

Pop-A-Plug® Heat Exchanger Tube Plugging System

- No welding or hotwork required
- Will not damage adjacent tubes or tubesheet joints
- Safe, controlled, and repeatable installation
- Pressure rated up to 7000 PsIG (483 BarG)
- Will not degrade/eject like elastomer or friction fit plugs

For more information visit cw-estgroup.com/ce04
The sensors are consistently measuring exposure limits and warning the workers of danger. There’s a third activity element to alert the worker that he or she may be in a dangerous situation and also gives an alert to someone if the worker is in trouble. It also provides situational awareness in that the sensors are consistently measuring exposure limits and warning the workers of danger. There’s a third benefit around worker productivity, as the connectivity can be used to provide information to the workers with instructions about work flow,” says Prabhu Soundararajan, Connected Worker leader, with Honeywell.

Upskill, formerly known as APX Labs, (Herndon, Va.; www.upskill.io) provides its Skyline platform, which powers enterprise wearables that use sensor technology to connect workers to realtime information and to each other (Figure 2). “The fundamental purpose is connecting, keeping safe and providing information to the hands-on workforce as they do their work,” says Jay Kim, chief strategy officer with Upskill. “The benefit of wearable technology, such as smart glasses, is that their hands are now free so workers can keep their hands and eyes on the tasks at hand. This provides increased productivity, improved safety and better efficiency in activities throughout the facility and in hazardous situations.”

Further, says Kim, the technology provides critical sensor nodes within the visual factory. “Glasses and wearables go everywhere hands-on employees go, so a tremendous amount of data is generated by these operators,” he says. “Those data go back into the system to make data analysts and workers even smarter.”

In addition, the wearables allow information sharing. Shared information could include the actions and steps of safety procedures, such as lock out/tag out. Another safety-enhancing example might be the use of what Kim refers to as “a simple see-what-I-see scenario” in which the number of people sent into a hazardous area can be reduced because...
remotely located experts could provide “over-the-shoulder” coaching to an individual completing tasks in a dangerous area using a front-facing camera on the smart glasses, rather than sending the entire team in to complete the activity.

And, Vandrico Solutions (Vancouver, Canada; www.vandrico.com) is exploring the use of networked sensors coupled with software solutions and electronic technologies to increase the safety of miners (Figure 3). One of the potential uses here would be to use sensors that are able to determine shifts in rock and seismic activity, which are linked to software and wearable devices and used to send realtime alerts to workers in an automated way. “In mining, it’s often difficult to get signal propagation, so one of the theories we have is that wearable technology, such as helmets, smart watches and head-mounted displays, make sense because it goes on the body, which helps determine the realtime location of the worker, if needed, and gets the worker’s attention,” says Gonzalo Tuleda, CEO with Vandrico. “With the prolific use of smartphones, we all have notification fatigue and tend to ignore a lot of notifications. But a vibration on the wrist or a flashing light under a hard hat will get the worker’s attention when needed. By combining the sensors that are in the mine with a sensor on wearable technology, you can provide realtime safety alerts in an automated way.”

The sum of the parts
Advanced safety solutions such as these are dependent upon several system components. According to Honeywell’s Soundarrajan, in most solutions, advanced sensors are used to measure the hazard, such as a chemical parameter, gas or chemical substance. That data gets communicated from point A to point B via a communications infrastructure,
such as a bluetooth transmitter that takes the information to a cell phone or wearable device or a WiFi network that takes it to a control room or the cloud for storage. The communication infrastructure may also include location technology to track the location of the employee and sensor. And the third component, according to Vandrico’s Tuleda, is software. “Software is needed to help translate information from the sensors and the platform with which the sensor is communicating. The software should also have a logic component that is capable of analyzing the data and making realtime decisions about sending out alerts if set limits are surpassed or an incident is about to occur,” says Tuleda.

In addition, software connects the workers and the wearables to the IT infrastructure so they can access the information they need, and also has the capability to connect workers to the Internet of Things or WiFi network to provide situational awareness, says Kim. “Software platforms connect the human interface to the rest of the system,” he says.

**Collecting the data**

Prior to the use of advanced sensors, sophisticated software might not have been as important because there wasn’t as much data. “We were happy to have one or two data points per shift on an operator in a process unit,” says AIHA’s Hayward. “But with the advancement of today’s direct-read instruments, it may be possible to capture one, two, six or more data points per second. With that much data, it is becoming necessary to identify or develop tools, techniques and knowledge to analyze large data sets in order to make good, useful, scientifically based decisions.”

Honeywell’s Soundararajan calls this “data with context.” This is where the intelligence of connecting data collected by the sensors with software comes into play. “We are developing software and successfully implementing software architectures that are capable of collecting data and reporting exceptions.”

Today’s software is capable of collecting data, storing and analyzing it and then using that information to predict an incident before it happens. “The ability to alert users on their mobile or wearable devices notifies them and allows them to react to the situation quickly, which has the potential to save lives and millions of dollars,” says Soundararajan.

He adds that other software advancements allow the software to do a good sum of the work traditionally done by industrial hygienists. “Today in industry, the data are often in silos, sitting in different systems, but using software that brings it all together — from the data from the sensor level that is connected with a worker all the way to the enterprise systems. This means the experts don’t have to do the crunching of data. Typically, hygienists spend at least 8 to 10 hours a week with Excel sheets, but today’s technology can reduce the burden of analysis. Regular reports are now available on demand.”

In addition, those data are available if an incident has occurred or if a regulatory agency requests a report. “Hygienists can pull that report in seconds, rather than crunching numbers for 10 hours,” he explains.

In addition, software and stored data can be used to lessen the burden of the ever-growing skills gap in the process industry, says Upskill’s Kim. “One of the biggest themes we see in the industrial workforce is that there is a potential skills gap. The baby boomers have become the real domain experts, but as they are heading to retirement and millennials are coming in to replace the workforce, the facilities are at risk of having a tremendous loss of knowledge that wasn’t captured in their digital systems,” explains Kim. “Equipping workers with wearable, connected devices enables easier capturing and sharing of that tribal knowledge and information. In some cases, it can be as simple as recording a video of a certain process and associating it with a specific workflow. Once that is stored in the system, it can then be made available to trainees and employees who may not know how to complete the task. This has the potential to eliminate the expected knowledge and skills gap.”

Vandrico’s Tuleda agrees and says it is possible to take it a step further in the future: “We have the opportunity to capture the knowledge that the experienced workers have and the decisions they make given the data they are presented. We can capture those data and use machine learning algorithms to train artificial intelligences, which allows us to make a giant step toward the automated decision component of industrial and process operations,” he says. “The things smart sensors do reliably allows us to tap into the knowledge of trained, experienced people and learn from their decisions what works and what doesn’t and then transmit that information in both directions — into the system and into the hands of the worker in the field.”

**The future of wearable sensors**

Right now, such advanced technologies are in the early adoption stage with larger enterprises and, within those businesses, are mostly being employed in critical applications. However, early adopters are beginning to see enough significant increases in efficiency and safety that many are moving the technology into full-scale operational settings. “We are seeing not only early adopters making excellent progress with successfully implementing this technology into real operational settings, but we are also seeing them doing this faster than they have over the past five or six years. The technology is getting into the mainstream mindset of operational leaders in larger enterprises, which means it will likely begin to accelerate with new customers at a rate that is faster than it has been in the past,” says Kim.

Honeywell’s Soundararajan adds that the chemical industry is showing interest because they are constantly pushing the envelope on safety. “Sensing and connected systems are an excellent way to share knowledge and improve safety,” he says. “And for the chemical industry, which is a risky environment, this type of connected sensing technology helps make their world a much safer place.”

Joy LePree
In industrial facilities, cyber incidents typically result from three basic scenarios: a malicious attack from an outside individual or group; a cyber incident that results from an engineer making a mistake that alters a control process or diminishes safe operations; or the work of a disgruntled employee or ex-employee. No matter which of these scenarios you believe is real or presents the most risk, companies must take steps to protect their industrial control systems (ICS) from cyber incidents. What should companies do and how far should they go to ensure that risk is managed to a sufficient level? This article addresses the fundamental elements that an ICS cybersecurity program must contain, and shares guidance on how to develop an in-depth cyber asset inventory.

Cyber incidents
A malicious attack from an outside individual or group. Although such attacks have affected physical operations in a number of well-publicized cases, most outsider attacks to date have focused on proliferation and reconnaissance (get in, spread, gather information, and report back) as their primary objectives. The passive nature of these attacks has lulled many into believing there is more hype than reality in the likelihood of a malicious attack. Most cybersecurity experts would agree that attacks of this type to date are merely a prelude to attacks that will take more directed action in the future. The attack on a power plant in the Ukraine in December 2015 in which hundreds of thousands of people lost power in the dead of winter is a testament to what is to come.

A cyber incident resulting from human error. These mistakes can go undetected until it is too late. Most engineers who have worked in chemical process industries (CPI) facilities long enough can share stories of when such incidences have occurred.

The work of a disgruntled employee or ex-employee. With the spate of layoffs during the last several years — particularly in the oil-and-gas sector — the potential for an insider threat is a rising concern for chief information security officers. Georgia-Pacific recently incurred the wrath of a fired employee who, soon after being laid off, accessed and altered control systems from his home. The company required a significant amount of time to recover from the damage he had inflicted. That employee was successfully prosecuted.

Know your cyber assets
In the race for better ICS cybersecurity, CPI companies all face the same challenge — knowing what cyber assets they have in the plant. Operators and managers tend to have good insight into the non-proprietary assets, such as workstations and routers, but they often lack sufficient visibility into the proprietary assets that run critical processes and keep plants safe. This lack of visibility introduces a level of risk that negatively impacts cybersecurity, safety and compliance efforts.

To what extent does this lack of visibility exist? In one real-world example, an inventory at a plant site showed that 20% of the cyber assets were traditional information technology (IT) systems that standard protocols — for example, Windows Management Instrumentation (WMI) and Simple Network Management Protocol (SNMP) — could interrogate for detailed configuration information. These systems include Microsoft Windows workstations, servers, routers and switches that sit in front of the proprietary control systems. An inventory of these is important to have, but it only paints a
partial picture of what is happening within the overall control network.

In our example, the remaining 80% of cyber assets came from the proprietary industrial control systems, such as distributed control systems (DCS), programmable logic controllers (PLC), or safety instrumented systems (SIS). Unlike a workstation, ICS systems have no standard protocols to pull detailed configuration information (such as I/O cards, firmware, software installed, and control strategies).

There is also no option to put an agent on such systems to push data out, as doing so invalidates vendor support. These systems give hackers the greatest opportunity to wreak havoc in a plant, and they also create opportunities for well-intentioned engineers to make mistakes that adversely affect operations.

Create a cyber asset inventory

Efforts to collect an inventory of cyber assets within a control network typically take three forms — manual, vendor-supplied, and IT-only. The following discussion examines the positives and negatives of each approach.

Manual inventory. Manual gathering of inventory data is the most prevalent approach used today. Companies will send engineers into plants to perform a physical inventory, and they will gather a limited set of common data points, related to such information as manufacturer, model and version. The data are consolidated in a spreadsheet and used organizationally.

This approach is convenient, but is not economical, because engineers walking a plant are expensive resources and having them carry out inventory duty has high opportunity costs. Similarly, the manual gathering of inventory data is inherently prone to errors due to the human element, and this approach will typically yield an incomplete assessment, potentially missing swaths of important information, including control logic and shutdown interlocks. Such a data inventory can also quickly become outdated over time. Finally, there are few options for automation using a simple spreadsheet, as such a tool does not enable security policy monitoring and management of-change processes.

Vendor-supplied solutions. Control system vendors often provide a managed service offering that essentially throws additional outside help at manual inventory efforts. All of the problems with a manual inventory still exist, but internal resources noted previously are freed to do other high-value duties. Many vendors will also offer tools to manage cyber asset inventories, but these tools rarely extend beyond their own control systems. Companies that adopt such tools run the risk of creating solution silos that ultimately add complexity to a cybersecurity posture.

PLANT DESIGN RUNNING IN OUR VEINS – YOUR FUTURE ON OUR MIND

Free selection rather than ready-made kits: we integrate processes – not just parts – for more efficiency, flexibility and security. Innovative plant design from the plant architects.

www.zeppelin-systems.com

The architect of your visions

Circle 41 on p. 78 or go to adlinks.chemengonline.com/61500-41
environment. Complexity is counterproductive to building an effective ICS cybersecurity program.

**IT-only solutions.** There are many solutions available that can discover non-proprietary systems and provide detailed configuration information, as well as advanced analytics. Such products are quite good at these tasks and given the number of solution providers with such capabilities, this has become a commodity offering. CPI companies must have non-proprietary information as part of their cybersecurity program.

However, they must also recognize that the resulting data come from only about 20% of the cyber assets in a process control network. Ultimately, IT-only solution architectures cannot scale to include the much more complex, proprietary systems that comprise the remaining 80% of cyber assets in a plant.

**Exploring ‘Inventory in Depth’**

A best practice solution must overcome the limitations of today’s approaches to inventory. It must gather inventory data for both non-proprietary and proprietary cyber assets, it must contain deep configuration information, and it must break down data silos so that the wide variety of manufacturer control systems are made visible.

Next, we explore the elements for developing a best practice, comprehensive cyber asset inventory. We’ll refer to the end product as Inventory in Depth.

**One database to rule them all.**

The first element of an Inventory in Depth approach is to have both non-proprietary (IT) and proprietary operational technology (OT) data in a single repository. The ability to carry out automated vulnerability assessments, security policy enforcement, unauthorized change investigations, patch management processes, analytics and more is only as good as the breadth and depth of the inventory such efforts utilize. Gathering OT and IT assets into a single database ensures breadth; ensuring depth requires having all configuration data, such as I/O cards, firmware, software installed, and control strategies. Detailed configuration information gives engineers and cybersecurity personnel the same view of data, which translates into more consistent, coordinated, and speedier decisions — important capabilities when the goal is to prevent potential plant upsets or harm to personnel. Finally, the costs to maintain an inventory can decrease by as much as 90% as Inventory in Depth relies on automated data gathering; depending on the frequency, an evergreen inventory is also achievable.

**Criticality, priority, and interdependency.** Not all cyber assets have the same risk profile in light of plant processes. Therefore, when an unauthorized change happens on a critical asset, such as a safety instrumented
system (SIS), the incident-response protocol will have different steps and degrees of urgency than protocols for other systems, such as a data historian. Discriminating between cyber assets means having a method of categorizing the systems so that each can receive appropriate scrutiny and responsiveness if an incident occurs.

Since few systems act independently in a plant, it is also important to understand how systems are related to each other. Should the system go down due to a cyber attack or engineering mistake, personnel can make better recovery decisions based on knowing what other systems are affected. Having this information is a good engineering practice that also allows cybersecurity personnel to better manage risk across the entire enterprise.

**New device discovery.** While a simple “ping sweep” will identify new assets on a network, finding new or changed proprietary cyber assets relies on a different tactic — digging into the configuration files of proprietary systems and finding system references that are not currently inventoried. Once an asset is recognized, cybersecurity or engineering personnel should ideally receive notifications of a new device, as well as missing ones (for instance, those resulting from a system upgrade). Then, established workflows can guide them through the process of updating data imports, policies, processes and other cybersecurity functions.

**Enabling new usage scenarios**
An OT and IT inventory opens up new ICS cybersecurity use cases that were previously unavailable or difficult to achieve. Cybersecurity and operations personnel can now perform the following tasks:

1. **Identify exposure to published vulnerabilities**
   
   **Scenario:** ICS-CERT (Box, p. 62) [2] published a critical vulnerability advisory in early 2015 concerning multiple models and versions of a specific transmitter. This transmitter works across any manufacturer’s control system and not just the manufacturer’s. The advisory describes the vulnerability as critical, noting that it has the potential to impact operations if left unaddressed.
   
   **Solution:** If a comprehensive OT inventory exists, a simple query will immediately identify every control system that has this transmitter. Only an inventory that spans the heterogeneous, proprietary control systems in a plant will provide complete results. Once the situation is remediated, to prevent future occurrences of this vulnerability, an automated policy can look for and flag instances of when that same transmitter is reintroduced into the control environment (for example, through the spares inventory).

2. **Unauthorized change to a control strategy**
   
   **Scenario:** An engineer connects to a particular safety system to make a simple change. The engineer mistakenly removes the ability for the operator to recognize the availability of that safety system.
   
   **Solution:** Inventoried configuration data are analyzed for changes, with unauthorized changes flagged for
investigation. An incident-response protocol drives remediating actions needed to restore the safety system. The next data import captures evidence that the safety system’s configuration was properly restored.

3. Preparing for the inevitable breach

Scenario: Hackers gain access to systems in Level 1 and below. A multi-threaded attack includes firmware updates to serial-to-Ethernet devices, similar to the Ukrainian power plant hack carried out in December 2015.

Solution: Change detection utilizing a security baseline will surface the malicious firmware updates, and change management procedures and automated workflows will drive needed actions. If a worst-case scenario occurs, automated backups taken during the Inventory in Depth process will speed recovery, as part of a comprehensive disaster recovery plan.

Today, the majority of CPI operating companies cannot effectively execute these three use cases. Where they stumble is not having an accurate, comprehensive inventory of all their cyber assets, which hinders swift, consistent action when these security policies are violated.

A comprehensive solution

A best-in-class inventory management solution deciphers and integrates control-system configuration data from both proprietary and non-proprietary systems into a single repository. Such a solution detects new or missing devices, provides a facility for asset classification, enables appropriately leveled incident response protocols, and accurately captures system interdependencies in sufficient detail.

An automated, normalized inventory data across all major IT and OT assets in the control network presents a holistic view of control system assets — beyond the reach of traditional manual, vendor-supplied, or IT-only solutions. Plant personnel monitor and detect unauthorized changes centrally and then investigate, remediate, and mitigate through automated policies and workflows. The result is greater operational efficiency, improved audit capabilities for compliance, closed-loop patch-management processes, and a speedy recovery in the event of a lost production system.

References

1. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), 2014 Industrial Control Systems Assessments Overview and Analysis. Accessed online at: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/FY2014_Year_End_Assessment_Report_S508C.pdf


Author

David Zahn is chief marketing officer and the general manager of the Cybersecurity Business Unit at PAS (16055 Space Center Blvd, Suite 600, Houston, TX 77062; Phone: 281-286-6565; Email: david.zahn@pas.com). He has more than 24 years of enterprise software and services experience within startup and high-growth companies in the oil and gas sector and IT fields. Prior to PAS, Zahn was vice president of marketing at FuelQuest and vice president of marketing at Avalara. He is a frequent speaker at cybersecurity industry events, and holds a BA in economics and managerial studies from Rice University, and MBA from the McCombs School of Business at the University of Texas (Austin).

Miller-Stephenson Offers a Wide Range of Specialty Chemicals

Miller-Stephenson offers a wide range of specialty chemicals including PTFE Dry Lubricants, Krytox™ Lubricants, Solvent Cleaners, Contact Cleaners, Vertrel™ Solvents, milLube™ Lubricants, Connector Lubricants, Aero-Duster®, Adhesives and Sealants, Epoxy Resins, Vazo™ Free Radical Sources, and low global warming formulations and nPB & HCFC-225 replacements available!

For technical information call 800.307.1766
Quality and Service Since 1955

miller-stephenson
Connecticut • Illinois • California • Canada
http://ce.mschem.com
Krytox™, Vertrel™ and Vazo™ are trademarks of The Chemours Company FC, LLC

PROCO warehouses are always packed.

Over $2M in inventory means fast turnaround on the products you need. Enjoy 1-2 day shipping on hundreds of in-stock styles, compounds and sizes. With the largest inventory in North America, rely on Proco Products.

800-344-3246 | procoproducts.com
The Expansion Joint and Check Valve People

Circle 21 on p. 78 or go to adlinks.chemengonline.com/61500-21
Circle 27 on p. 78 or go to adlinks.chemengonline.com/61500-27
Industrial cybersecurity risks are widely appreciated. In April, the deputy director of the U.S. National Security Agency, Rich Ledgett, warned that industrial control systems (ICS) and other critical infrastructure assets remain vulnerable to attack (Figure 1). Robust cyberdefense of industrial facilities remains an ongoing challenge for the chemical process industries (CPI). The convergence between the world of information technology (IT) and the world of operational technology, in which control systems for industrial facilities reside, has brought tremendous benefits, along with more complex security concerns. The same convergence, however, has allowed the industrial world to adopt cyberdefense techniques that have been widely used in IT. This article discusses several key cybersecurity IT tools that can help industrial facilities establish a layered cybersecurity system for its operations.

**Cyber threats and consequences**
The Stuxnet worm, a computer virus that infamously affected Iran’s nuclear centrifuges,
and the damage due to a cyberattack of a
German steel mill reported in 2014 are evi-
dence that cyberattacks can have physical,
real-world impacts. But it is not necessary
to prompt an explosion to cause significant
disruption. A cyber attack on Ukraine’s elec-
tric power grid, and subsequent widespread
delay failure last December, was evidence of
that.

As NSA’s Ledgett put it, “You don’t need
to cause physical harm to affect critical infra-
structure assets.”

Cybersecurity risks are not easily ad-
dressed, however. One challenge is the
increasing sophistication of attacks. The
German government report on the steel
mill incident, for example, noted that the at-
tackers demonstrated not only expertise in
conventional IT security, “but also detailed
technical knowledge of the industrial control
systems and production processes used in
the plant.”

Moreover, once the tools and knowledge
to enable such attacks are developed, they
are often quickly commoditized and shared,
allowing others with fewer technical skills to
use them.

Another challenge, however, is simply the
increasing vulnerabilities introduced by the
growth of intelligent, connected devices in in-
dustrial control systems. As Chris Hankin, di-
rector of the Institute for Security Science and
Technology (ISST) at Imperial College, Lon-
don (www.imperial.ac.uk/security-institute),
remarked recently: “Almost every component
of such systems now has fully functional com-
puting capability and most of the connections
will now be Ethernet, Wi-Fi or will be using
Internet protocol.”

The growth of the Internet of Things —
and, more specifically the Industrial Internet
of Things (IIoT), in particular — is adding to
both the number of devices and their con-
nectivity. Today, the IT research and advisory
company Gartner Inc. (Stamford, Conn.;
www.gartner.com) estimates 6.4 billion con-
nected devices are in use worldwide. By
2020, it forecasts, that total will reach 20.8
ebillion. Moreover, heavy industries such as
utilities, oil and gas, and manufacturing are
among the leading users. Each device and
connection expands the possible attack sur-
fice for cyberattacks.

Closely connected to the increasing num-
ber of connected devices is the growth of the
network of remote computer servers
casually known as the “Cloud,” which pro-
vides access to infinitely scalable computing
power and storage. The Cloud provides an
opportunity to store and process the large
volumes of data resulting from the prolifera-
tion of connected devices, such as with the
IIoT. Again, however, it introduces new con-
nection and communication channels that
would-be cyberattackers will try to exploit.

Defense in depth
In fact, the security issues related to the IIoT
and Cloud storage result from the longer-
term challenges surrounding the conver-
gence between the IT and operational tech-
nology (OT) worlds. Open platforms and the
proliferation of third-party and open-source
software in industrial control systems has
long brought the power and efficiencies from
the enterprise side of the business to the
process side. But along with those benefits,
the convergence also brings associated se-
curity concerns.

To complicate matters, while the vulner-
abilities on both sides — enterprise and op-
erations — may be similar, the solutions are
often not directly transferable. The priorities
of each are necessarily different: while confi-
dentiality can be prioritized in the enterprise;
availability and integrity must, for the most
part, take priority on the OT side. In prac-
tice, a security solution cannot be allowed
to shutdown operator access to data or de-
vices that are essential to the safe running of
the plant, even if the security of those data is
at risk of being compromised.

ISST’s Hankin acknowledged this reality in
his speech: “While there has been a conver-
gence between the two worlds (IT and OT),
particularly in the past five years, there are
major differences, such as the fact the in-
dustrial control systems (ICS) tend to have
to operate in a time-critical way; they have to
operate around the clock; and edge clients, such as sensors and actuators, are becoming much more important” (Figure 2).

In essence, the options for ensuring security are more limited in the OT world. This is partly why the concept of “defense in depth” is so important to industrial security: without the option of configuring protection mechanisms to potentially inhibit system availability, it is even clearer in an OT setting that no single security solution can provide complete protection. A layered approach that employs several different defenses is the better goal. Such an approach means that if (or rather, when) one layer fails or is bypassed, another may block the attack. Defense in depth makes it more difficult to virtually break into a system, and, if it includes active monitoring and a good incidence-response plan, promotes quicker detection and responses that minimize the impact where an attack does breach security.

This also means that — perhaps even more so than in the IT world — security in an operational setting cannot rely solely on software. As in all operations, success is only achieved through a combination of people, processes and technology.

Adapting to the needs of OT
Notwithstanding these points, though, security developments in the IT world do prove valuable to operations. Provided the priorities of OT users are accommodated, and the solutions are implemented in an appropriate framework, recent IT developments offer significant potential to boost security in the OT world of industrial facilities.

Four recent technologies, in particular, are worth looking at in more detail:

- Risk-analysis technologies that enable plants to prioritize investments in cybersecurity
- Next-generation firewalls, which can bring about radical improvements in network protection

- Application whitelisting and device control to protect individual end nodes
- Advanced analytics, focused on using “big data” to detect and predict cyberattacks

The first three are already seeing significant uptake, and accompanying security benefits, among industrial users. The last offers a glimpse at how industrial cybersecurity is likely to continue to develop in the future, based on IT trends. It also demonstrates how the increasing connectivity and elastic computing power embodied by the IIoT and the Cloud can contribute to the security challenges they have done so much to highlight.

Risk analysis solutions
A key value of risk analysis is that it recognizes that resources are finite. Plant owners face numerous choices about where and how to apply security controls and solutions. Risk analysis techniques provide a way to quantify, and therefore prioritize, cybersecurity risks, to ensure that limited resources are applied effectively and efficiently to mitigate those that are most severe.

That quantification is aided by the existence of standard definitions of risk from bodies such as the International Organization for Standardization (ISO; Geneva, Switzerland; www.iso.org) and the National Institute of Standards and Technology (NIST; Gaithersburg, Md.; www.nist.gov). The former defines risk as “the potential that a given threat will exploit vulnerabilities of an asset or group of assets, and thereby cause harm to the organization.” The latter characterizes risk as “a function of the likelihood of a given threat source’s exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.”

Cybersecurity risk is therefore a function of vulnerabilities, threats and potential consequences of a successful compromise. By accepting this as a definition, risk can be quantified and prioritized.

In practice, vulnerabilities will always exist — whether in the form of a software bug or due to weak passwords or poor system configuration. They cannot be entirely eliminated. Threats, meanwhile, constantly vary, and will be driven not just by the availability of malicious software or technical knowledge, but also by the motivation and means of potential attackers. The consequences of exploiting a specific threat have to be calculated into a relative risk score for each vulnerability (Figure 3). Owner-operators of industrial control systems can then determine
what level of risk to mitigate, and which risks they are willing to accept — their risk appetite.

Since vulnerabilities and threats continually evolve and expand (with 200,000 new variants of malware identified every day, for example), the process must be continuous. Automating the risk-analysis process brings significant benefits to the security of a plant.

Risk-analysis software does so, and enables users to monitor networks and system devices in realtime (Figure 4). By consolidating complex site-wide data, risk-analysis software significantly improves the ability to detect threats and identify vulnerabilities. Perhaps more importantly, by calculating the risk for each device in realtime, it enables prioritization of risks by their potential impact to the plant or business. It also provides a realtime update when the risks change due to new threats or vulnerabilities to the system. Combined with well-configured alerts, users can assign resources more efficiently, and respond more effectively and more quickly to risks.

In the IT world, risk-analysis and risk-management solutions have seen widespread uptake, but there are difficulties in simply transposing these to an industrial setting. First, the requirements and competencies of the users — control engineers and operators, as opposed to IT staff — are different. An OT risk-analysis tool must present results that are meaningful to non-security specialists who operate the ICS around the clock.

Second, allowance has to be made for the OT environment. Many traditional vulnerability assessment (VA) tools used in enterprise systems may be unsuitable (and possibly unsafe) when applied to network activity in an ICS.

This is because they probe aggressively to test for vulnerabilities, launching a variety of network packets directed at every possible port on an end node. The responses are used to determine the state of each port, and whether the protocols are actively supported. A database of known vulnerabilities is then used to match the responses, and then further scanning of the device is attempted.

There are two key problem areas with this technique.

- Non-standard network traffic into poorly managed ports can cause unintended consequences — including locking up a communications port, tying up resources on the end node, or even hanging up an entire end node. This type of probing can reveal weaknesses in the configuration or programming of applications that results in unintended consequences.

- Network scanning can increase the load on an end node to an unmanageable level, resulting in a denial of service (with the node unable to complete normal operation), or even a node crash. To avoid this vulnerability, scanners must be “throttled” properly to protect both the end nodes as well as the network latency and bandwidth.

An IT VA tool may therefore introduce risks to the safe operation of an ICS, as much as it may identify them.

Essentially, realtime risk analysis in an OT environment must be tailored to ensure that it never interferes with normal plant operation or control. It must also provide realtime, actionable information that can be used by operators, security administrators and business leaders.

VA tools tailored to the ICS environment are now becoming available, and are seeing good uptake. With the scale of the cybersecurity challenge continually growing, they are likely to become an increasingly important tool in helping operators focus and tailor their cybersecurity strategies.

**Next-generation firewalls**

In IT systems, firewalls are among the most widely used cybersecurity measures. While antivirus software protects the end nodes, the firewall monitors and controls network traffic based on con-
figured security rules to detect and prevent network-based cyberattacks. For most business, they are the first line of defense in their cybersecurity strategy.

Next-generation firewalls (NGFWs) significantly enhance the protection capabilities of these systems. In addition to traditional network protection which restricts access to a particular port or address, NGFWs include deep packet inspection of network traffic in realtime.

Increased analysis of the content of network traffic (not just the source and destination addresses) facilitates a range of additional defenses:

- **Application profiling** — tracking application behavior to raise alerts or interrupt communications displaying abnormal behavior, or patterns associated with known malware
- **Protocol support** — including, in industrial NGFWs and most industrial control system protocols, such as Modbus, DNP3, OPC and HART. This allows the NGFW to be configured to restrict protocols to only specific functions, such as restricting the ability of applications using Modbus to write to certain registers, or restricting all write commands coming into the ICS
- **Potential to interface with the ICS domain controller to identify the user associated with specific application traffic on the plant control network and to block unauthorized users**
- **Advanced threat detection** (on high-end NGFW), based on network traffic patterns, and signatures of known malware

The potential benefits of NGFWs may even be greater in an OT than IT setting. Network traffic in the OT environment is typically more “predictable,” with most communication channels clearly defined. That makes it possible in many cases to more tightly lock down communications traffic on an ICS — and easier to determine deviations from normal network traffic patterns.

Again, there are significant challenges, though: an NGFW can decode some, but not all, encrypted traffic, for example. ICS owners also need to coordinate the NGFW selection with their process control vendors to ensure the correct configuration and to ensure that network performance is not affected when on critical operations and network traffic latency.

However, the potential rewards make this worthwhile. An NGFW not only provides tighter control of network traffic, but more intelligent control: it is as much about letting desirable traffic through as detecting and blocking threats.

More highly sophisticated control gives plant operators not only increased protection, but also the confidence to allow connections they would otherwise feel forced to block: to enable and control access for an increasing range of applications; to facilitate authorized personnel using mobile devices; and to promote collaboration across the enterprise with controlled access to realtime data.

**End-point protection**

Application whitelisting (AWL) is another staple in traditional cybersecurity approaches. It protects individual end nodes by restricting the files that can be executed to only those specifically authorized to run.

Its value is well recognized. Whitelisting is listed first among the top four strategies listed by the Australian government intelligence agency, the Signals Directorate, and last October, NIST published a guide to whitelisting for businesses.

As the NIST guide notes, the power of application whitelisting comes from its prescriptiveness: “Unlike security technologies, such as antivirus software, which block known bad activity and permit all other, application whitelisting technologies are designed to permit known good activity and block all other.”

Added to this, whitelisting avoids some of the maintenance required for technologies like antivirus software or intrusion prevention/detection systems (IPS or IDS). Such “blacklisting” technologies require frequent updates to the “known bad” signatures; DAT files (binary data files with .dat filenames) for antivirus solutions are updated daily with new “known malware” signatures. More sophisticated malware, meanwhile, is being designed to evade detection by signature-based security protections.

Application whitelisting therefore represents a strong additional line of defense against malware that is designed to add new software or modify existing software on an end-node. It can also offer some protection for obsolete operating systems no longer supported by new security patches (such as Windows Server 2003 and Windows XP operating systems).

There are challenges for an ICS, however. Whitelisting takes time to set up and configure in all systems. The difficulty lies in ensuring that all applications that need to be run on a particular node are enabled (or not blocked). In an ICS, the risks of blocking
or impacting normal operations are often greater, however. If improperly configured, a whitelisting solution can prevent normal operations, causing operators to lose visibility or control of the plant. It must therefore be tightly integrated into the control system operation, because it is active before every file execution on the system.

To minimize the risk, the AWL solution should be fully qualified by the ICS vendor or end-user before use. Most solutions also offer various operation modes: monitoring or observation, in which users can monitor unauthorized file execution without blocking any operations; “self approval” — in which message pop-ups enable users to override any blocked executable; and full implementation in which whitelisting policies are fully executed and enforced. The last should only be used after the site has validated the whitelisting configuration against all normal plant usage scenarios.

Where this is done, however, whitelisting has proven an effective and safe solution in industrial settings, bringing similar benefits for cybersecurity that have been realized in the IT world. In addition to managing executable files, whitelisting solutions increasingly offer a wide range of functionality:

- Managing USB (universal serial bus) and removable storage devices, allowing users to restrict USB device usage by vendor, serial number or function (restricting to read-only, for example)
- Extending device management capability to control wireless, Bluetooth and all plug-and-play devices on the system
- Protecting access to the local registry
- Managing access to non-executable files
- Protecting against malicious behavior of programs in memory (such as buffer overflows)
- Controlling execution of scripts or ActiveX controls
- Executing files with reputation-based decisions
- Tracking processes changing files on the system

Like NGFWs, application whitelisting is a mature technology and integral part of most IT cybersecurity strategies. Increasingly, the same is becoming true in the OT space.

Looking to the future

Advanced analytics, by contrast, remains resolutely immature in the industrial environment. It is, however, an important emerging technology that once again offers significant potential for OT systems.

While the value of risk analysis is that it recognizes resources for cybersecurity are finite, the value of advanced analytics is that it accepts that complete security is unachievable. With the threat landscape constantly evolving, it is impossible to completely mitigate all threats to the ICS.

Those that have the potential to do the most harm will be those threats of which organizations remain unaware. The faster plants can detect malicious actors on the system or network, the faster they can address them and minimize the damage.

Advanced analytics uses big data tools to monitor and analyze a wide range of information sources, from email and social media, to network flows and third-party threat feeds. With this information, it can identify abnormal patterns that indicate attacks or intrusions. Not only can advanced analytic techniques detect recognized threats, but they can also allow the ability to predict new, emerging dangers. Such systems, for example, can automatically notify users of a cyberattack occurring on a related system elsewhere in the world — in realtime — enabling them to take precautions to protect their own sites.

While advanced analytics are increasingly important in cybersecurity, there is little uptake to date in the OT world. That, however, is likely to change — as it has with other key technologies in the IT realm. Convergence between IT and OT means the challenges facing the two are often similar. As long as industrial users pay due regard to the distinctive requirements of process control systems, there is no reason the solutions for OT cannot draw on the lessons that have been learned. In time, it may have insights to share with IT as well.

Edited by Scott Jenkins

Author

Mike Baldi is a cybersecurity solutions architect at Honeywell Process Solutions (1860 West Rose Garden Lane, Phoenix, AZ 85027; Email: mike.baldi@honeywell.com; Phone: 602-293-1549). Baldi has worked for Honeywell for over 36 years. He led a team providing technical support for Industrial Process Control Systems and advanced applications, and was the lead systems engineer for HPS systems test. Baldi joined the HPS Global Architecture team in 2009, and became the chief cybersecurity architect for HPS, and the lead architect for the HPS Cyber Security Center-of-Excellence. He lead the design for security initiative — integrating security into HPS products and the HPS culture. He was also the primary focal point for HPS product and customer security issues, and for HPS product security certifications and compliance. Baldi recently moved to the Honeywell Industrial Cyber Security organization as a cybersecurity solutions architect. Baldi holds a B.S. degree in computer science, an MBA degree in technology management, and is CISSP certified.

Editor’s note: For more information on cybersecurity in the CPI, visit our website (www.chemengineer.com) and see articles by Andrew Ginter (Chem. Eng., July 2013) and Eric C. Cosman (Chem. Eng., June 2014).
When the Stuxnet computer worm attacked programmable logic controllers (PLCs) at Iranian nuclear facilities running an integrated system, centrifuges were commanded to literally rip themselves apart. This clear demonstration of the link between cybersecurity and safe industrial operations was a worldwide wakeup call for plant managers, IT and automation managers, safety engineers and many others.

Of course, smaller-scale attacks are much more likely, and they are happening. At one plant, where system maintenance was carried out remotely, a cyber attack from abroad revealed the vulnerability of using simple username/password authentication for remote access. The attack was discovered only after the data transmission volume exceeded the company's data plan.

Cyber-related safety risks do not necessarily result from criminal activity. During the commissioning of one plant, for example, the failure of engineering software during the recompiling of the memory mapped input (MMI) following a plant shutdown led to a situation in which an incorrect modification was loaded into an integrated safety controller, and then activated.

These incidents demonstrate the need for specific IT security improvements, and at the same time, raise broader questions about...
the relationship between cybersecurity and plant safety:
1. Can the “insecurity” of integrated control systems influence the functional safety of a plant?
2. What needs to be protected?
3. Can the principles developed for functional safety be applied to security?

This article considers these questions and includes operational examples and specific recommendations for improving security and safety at industrial facilities.

Safety and security standards
The International Electrotechnical Commission (IEC; Geneva, Switzerland; www.iec.ch) standard IEC 61508 is the international standard of rules for functional safety of electrical, electronic and programmable electronic safety-related systems. According to IEC 61508, functional safety is “part of the overall safety that depends on functional and physical units operating correctly in response to their inputs.”

By this definition, the answer to the first question posed earlier — Can the “insecurity” of integrated control systems influence the functional safety of a plant? — has to be “yes.” In the examples cited above, vulnerabilities to people and facilities were introduced. Clearly, functional safety was compromised, and while security breaches may not have led to deaths or injuries, there is no evidence to suggest that such a situation could not occur in the future.

Even ruling out malicious threats, the fact remains that IT security-based vulnerabilities can be found in all kinds of automation systems. This includes the safety-related system itself and the distributed control system (DCS), of which the safety system may be a part. This is one reason why so many safety experts call not only for the physical separation of safety instrumented system (SIS) and DCS components, but also for different engineering staffs or vendors to be responsible for each.

To answer the other questions, we need to highlight two other standards. One is the international standard IEC 61511 for SIS in the process industries. Whether independent or integrated into an overall basic process control system (BPCS), the SIS is a fundamental component of every industrial process facility.

In this model, the industrial process is surrounded by different risk-reduction layers, which collectively lower the risk to an acceptable level (Figure 1). The risk reduction claim for the safety layer is set by the safety integrity level (SIL).

The first line of protection for any plant is the control and monitoring layer, which includes the BPCS. By successfully carrying out its dedicated function, the BPCS reduces the risk of an unwanted event occurring. Typically, IEC 61511 stipulates that the risk reduction claim of a BPCS must be larger than 1 and smaller than 10. A risk-reduction capability of 10 corresponds to SIL 1.

The cyberattack and IT vulnerability prevention layer includes the SIS. The hardware and software in this level perform individual safety instrumented functions (SIFs). During the risk and hazard analyses carried out as part of the basic design process of every plant, the risk-reduction factor to be achieved by the protection layer is determined.

In most critical industrial processes, the SIS must be rated SIL 3, indicating a risk-reduction factor of 1,000, to bring the overall risk to an acceptable level.

At the mitigation layer, technical systems are allocated, allowing mitigation of damages in case the inner layers of protection fail. In many cases, mitigation systems are not encountered as being part of the safety system, as they are only activated after an event (that should have been prevented) happens. However, in cases where the mitigation system is credited as part of defining additional measures, it may be covered by the safety evaluation as well.

Now consider the IEC standard for cybersecurity. IEC 62443 covers the safe security techniques necessary to stop cyber attacks involving networks and systems at industrial facilities.
What requires protection?
According to the most recent version of IEC 61511, the answer to the question of what needs to be protected is that both norms and physical structures need to be protected. As for norms, the standard calls for the following:
- SIS security risk assessment
- Making the SIS sufficiently resilient against identified security risks
- Securing the performance of the SIS system, as well as diagnostic and fault handling, protection from unwanted program alterations, data for troubleshooting the SIF, and bypass restrictions so that alarms and manual shutdown are not disabled
- Enabling/disabling of read/write access via a sufficiently secure method
- Segregation of the SIS and BPCS networks

As for the structural requirements, IEC 61511 instructs operators to conduct an assessment of their SIS related to the following:
- Independence between protection layers
- Diversity of protection layers
- Physical separation between different protection layers
- Identification of common-cause failures between protection layers

One other IEC 61511 note has particular bearing on the issue of cybersecurity and plant safety. The standard states: “Wherever practicable, the SIF should be physically separated from the non-SIF.” Also, the standard demands that countermeasures be taken for foreseeable threats.

Applying safety principles
The IEC 61511 (safety) and IEC 62443 (security) standards coincide on the demand for independent layers of protection. Together, these standards prescribe:
- Independence between control systems and safety systems
- Reduction of systematic errors
- Separation of technical and management responsibility
- Reducing common-cause errors

The standards also reinforce that anything and everything within the system is only as strong as its weakest link. When using embedded safety systems, all hardware and software that could impair the safety function negatively should be treated as being part of the safety function.

IEC 61511 requires different, independent layers of protection. Unifying two layers of protection will require the new risk-reduction evaluation to prove that compliance with the overall risk reduction is reached when two different protection layers are in place.

Integrating BPCS and SIS
As an illustrative example, assume that a risk analysis of a given process has led to the conclusion that a SIL-3-compliant SIS is required. The traditional approach implies that a risk reduction of greater than 1,000
and less than 10,000 will be achieved. The risk reduction is partly covered by the BPCS (up to 10, as per IEC 61511) and by the SIS (1,000 in a SIL-3-compliant solution).

In the integrated solution, there will be common components for the BPCS and SIS. Depending on the individual setup, this will be either the central processing unit (CPU), input-output (I/O) buses or (parts) of the solution software (for example, the operating system), and symbol libraries.

The argument could be made that different components (of the same make) may be used for the SIS and BPCS. However, if common elements (such as operating systems and buses) are used, the systematic capabilities of such components may need to comply with the requirements mentioned above.

It should also be kept in mind that using components such as CPUs with freely configurable software on board – and using these same components for different tasks – may not be considered sufficient leveraging of the integrity level of the solution.

These commonly used components, in order to comply with the initial risk reduction requirements, will need to maintain a risk reduction of greater than 1,000 by less than 10,000. Practically, this means SIL 4, which is currently an unachievable level.

**Engineering’s key role in security**

The quality of engineering processes, tools and associated services may be even more important to overall safety results than BCPS and SIS hardware.

Proper engineering includes the following aspects:
- Reducing complexity by splitting tasks into independent modules
- Properly defining and verifying interfaces
- Testing each module intensively
- Maintain the “four-eyes” principle when reviewing engineering documents and results of implementation tasks, according to IEC 60158-1, paragraph 8.2.18

Application of this strategy requires engaging the various parties to make sure that potential deficiencies in each task are identified and corrected. While integrated tools can support the effectiveness of engineering processes, addressing aspects like common-cause failures requires first narrowing integration to a sustainable level. This helps maintain both efficient engineering processes and functional safety at the required level.

The previous comments about BPCS and SIS independence and diversity also apply to engineering tools. A potential hidden failure of the engineering tool may impair the desired reduction in overall risk.

There are two types of integrated solutions that have either a common configuration database for SIS and BPCS, or have independent databases for SIS and BPCS, but use the same data access mechanisms. Both solutions have the disadvantage of having a common cause for potential failures, which would infect both the BPCS and SIS.

The engineering tool for safety systems should overcome these issues by remaining independent (to the greatest extent reasonably possible) from the hardware and software environment. This is accomplished by having the complete functionality of the safety engineering tool, running in a Windows software environment, implemented in a way that allows it to be independent from Windows functions. This concept allows maximum protection from errors and creates a trusted set of engineering data that can be used to program the SIS.

Nevertheless, the engineering tool should allow integrated engineering by maintaining interfaces that permit automated transfer of configuration data (tag-oriented information as well as logic-oriented data) from third-party systems into the trusted set of engineering data used for programming the SIS.

Furthermore, having the same engineers in charge of programming the DCS and safety system ignores the proven benefits of the checks and balances of independent thinking. For this reason, IEC 61508 is setting recommendations...
for the degree of independence of parties involved in design, implementation and verification of the SIS.

**IT security recommendations**
Cybersecurity and plant safety are so intertwined in the connected world of industrial processes that an equal commitment to both is required to achieve the needed protection. Following the recommended international standards for functional safety for PLCs (IEC 61508), safety instrumented systems (IEC 61511) and cybersecurity (IEC 62443) provides a path to a safe, secure facility.

For the most robust security and reduced safety risks, the author advocates the traditional approach of standalone SIS and BPCS units — ideally from different vendors — versus an integrated BPCS/safety system from the same vendor.

For valid security and safety reasons, it is also good practice for companies to consider an independent safety system built on a proprietary operating system. Of course, such a system can and should be completely compatible with DCS products. Additionally, it should feature easy-to-use engineering tools with fully integrated configuration and programming and diagnostic capabilities.

Applying these recommendations and adhering to international standards for separate BPCS and SIS systems help plant operators meet their obligation to protect people, communities, the environment and their own financial security. The good news is that hardware, software and expertise are available today to help operators meet their obligations for the full lifecycle of their plants.

Edited by Scott Jenkins

**Author**
Peter Sieber is vice president for global sales and regional development for HIMA Paul Hildebrandt GmbH (Albert-Bassermann-Straße 28, 68782 Brühl, Germany, Phone +49-6202 709-0, p.sieber@hima.com), a leading specialist in safety automation systems. Sieber is participating in the ongoing effort by the steering committees working on functional safety and IT security standards, IEC 61508 and IEC 62443, respectively. He has been actively involved in the development of the definition of both functional safety guidelines and IT security guidelines for process automation applications.