Chemical Companies Playing Catch Up

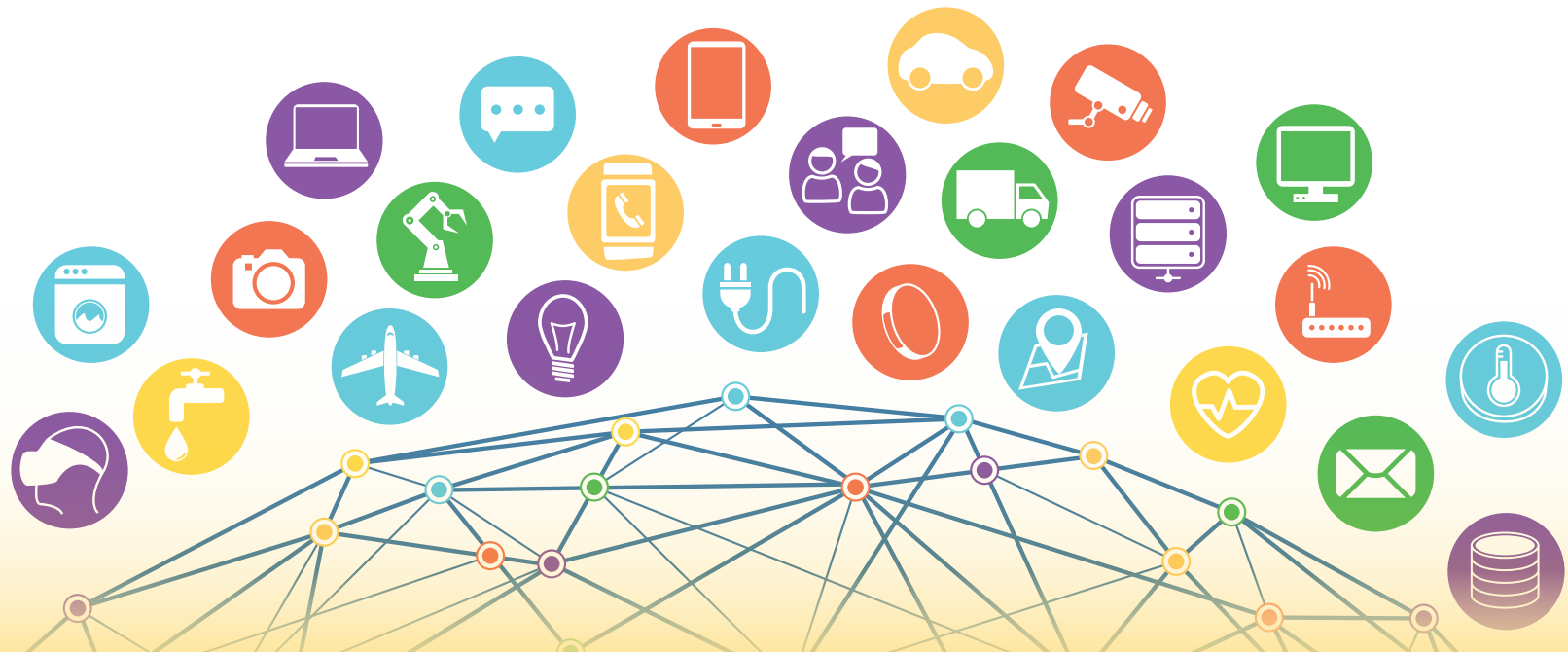
Now is the time for chemical companies to improve business intelligence and operational efficiency with automation technology.

By Dietz Ellis, Michael Gomez, Tim Johnson, Brad Raiford and Deborah Watson

Not long ago, chemical manufacturing processes ran in isolation with little to no outside interaction. Air-gapped technologies and practices remained unaffected by advancements as if in a state of suspended animation. However, process automation technologies and capabilities have caught up with the rest of the world. Chemical companies need manufacturing to evolve from manual analog processes to automated optimized processes interactively connecting to the larger virtual world to capitalize on improved business intelligence and operational efficiency.

Chemical companies, facing increased competitive pressures, now seek to leverage new process automation technology opportunities. Newer information technologies (IT) strategies leveraging large amounts of production-based "big data," analytics and the Internet of Things (IoT) are quickly becoming operation technology (OT) hot topics for companies seeking to optimize geographically dispersed processes and data while simultaneously creating centralized functional capabilities.

The adoption of new technologies requires a fundamental methodology shift in process automation implementation, operation and maintenance. The network architecture resulting from adoption of new technologies provides interconnected and interrelated facility processes supporting production-based big data analytics,



which facilitate the identification of new business opportunities, detect system failures and create new operation strategies for increased competitiveness.

Today's modern dynamic business model requires an exchange of information between process automation networks and untrusted networks outside process networks. Systems designed to operate with minimal or no communication outside traditional process networks have impeded process automation modernization efforts.

In a recent KPMG survey of 350 engineering and IT managers conducted for KPMG by Onepoll.com last year, 48% agreed that by connecting process automation networks to corporate IT infrastructure they will gain data exchange capabilities enabling proactive strategic planning. Half of the participants agreed that big data techniques may identify new opportunities for their business that they had not been able to previously identify.

Commercial off-the-shelf (COTS) technologies, open standards and protocols and consumer applications comprise the foundation of the enhanced digital process automation systems swiftly replacing aging analog process automaton technologies. The examples below show how process automation utilizes COTS such as wireless, Ethernet, the Internet and internet protocol (IP) for supporting process automation:

- One of the latest opportunities for technology expansion centers on the modification of the IoT creating the Industrial Internet of Things. IP-capable sensors transmit performance metrics to a process automation cloud service. The process automation cloud service performs predictive analytics delivering insights and actionable data extending beyond traditional process control to other functions, such as site safety and energy management;
- Technologies supporting mobile process management and control continue to experience increased traction and demand. Mobile applications provide field technicians views into real-time process that may not have previously been available, increasing job performance; and
- Web portals and interfaces provide a flexible, easy-to-access and accurate way for health, safety and environment (HS&E) to monitor the safety of plant resources. Connected monitors provide the ability to track resource locations, environmental exposures (e.g., gas leaks) and current states of health. These systems enable organizations to better protect employees and residents in surrounding neighborhoods.

As interconnectivity grows between enhanced digital process automation and external systems, the risk of cyberattacks ranging from espionage and intellectual property theft to plant safety increases. Modern process automation systems are now vulnerable to attack vectors, which previously affected only corporate IT systems. As with any other business risk, the threat of cyberattacks should not be underestimated. At a 2014 conference for the chemical industry hosted by Siemens, nearly 30% of attendees reported their companies had detected a breach of industrial security, and more than 80% agreed that industrial security is a growing threat to their business, according to an EngineerLive report.

The adoption of COTS and open standards by the process automation industry has increased exposure to malware and hackers attempting to gain access to and disrupt real-time processes and dependent infrastructure. With the disclosure of the Stuxnet cyberattack six years ago, attacks specifically targeting process automation systems have been on the rise.

In the past few years nuclear power plants, oil platforms and water treatment facilities have all been 'cyberattacked,' causing unplanned downtime with the potential to cause serious incidents if not detected during the early attack stages. Monitoring of the process automation network for such attacks needs to become the norm for chemical companies as the urge to integrate more and more of the automation plant into the overall business system gathers pace, according to an April report from EngineerLive.

Recent events indicate process automation could be at a tipping point. Long life cycles for process automation components combined with the adoption of COTS and open protocols have created a cybersecurity-maturity gap for process automation. Process automation adopted

As interconnectivity grows between enhanced digital process automation and external systems, the risk of cyberattacks ranging from espionage and intellectual property theft to plant safety increases.

IT-based technology over two decades ago focusing on process automation features and not the potential operational risk for these technologies. The security through obscurity approach worked for quite some time until the issues discussed began appearing regularly.

Now with process automation pushing for next-generation technology, which many IT departments struggle with deploying, running and maintaining the cybermaturity gap has been exposed and must be addressed. Bridging the process automation cybersecurity maturity gap necessitates a comprehensive strategy. Securing process automation is not a topic solely for technical implementation teams; it stems from security awareness across all layers of management and employees. A comprehensive process automation cybersecurity strategy must recognize the premise that process control system security is not the same as corporate IT security.

Security poses an ongoing risk and must be continually managed through the life cycles of all manufacturers. Thorough identification of business goals and objectives drive the development of a comprehensive and disciplined cybersecurity strategy enabling unified risk management and intentional convergence of IT and process automation environments. By adopting a holistic approach to a 'defense in depth' cybersecurity strategy, the process of strengthening protections against those who would seek to disrupt activities can begin, according to the EngineerLive report.

With these thoughts in mind, chemical manufacturers should consider these questions:

- How well do the IT and OT engineering departments communicate?;
- Does the organization have appropriate top-down management for the effective control of the converged environment?;
- Are bottom-up lines of communication in place, including event thresholds for notifying executive leadership?;
- Do security policies and practices take into account corporate IT, process automation systems, facilities and personnel, including gaps or redundancies?;
- Are suppliers (including second- and third-tier suppliers) fully involved in the cybersecurity program?;
- Has the cybersecurity strategy been aligned to the business so that everyone understands what is being protected, and why?; and
- Does the organization have an enterprise-wide, standards-based approach for managing cyberrisks?

To construct a "cybersuccess" strategy, companies need to leverage the diversity of available skillsets and knowledge bases. These four critical activities should be incorporated into cybersecurity strategy development efforts:

- Develop a foundation: This starts by identifying and educating all key stakeholders to secure their support and cooperation with the organization's security goals. Working together, stakeholders can identify gaps and develop the appropriate governance mechanisms to manage and control all aspects of control system cybersecurity;
- Plan and control: Develop capabilities and performance indicators to prioritize, coordinate and measure the work involved in improving security. Conduct detailed reviews of process automation environments to identify inherent risks. In particular, the risk management procedure is reviewed to ensure adequate inclusion and evaluation of process automation specific risks;
- Implement: Develop and implement methods enabling processes to operate with a level of cyber risk as low as reasonably practical. Regular strategy and capability reviews are incorporated to adjust to the rapidly evolving threat landscape; and
- Monitoring: Ensure risks are appropriately mitigated with periodic reviews of process automation environments. Routinely evaluate implemented processes/controls for compliance with cybersecurity strategies. Mitigate new risk vectors with threat intelligence monitoring for emerging risks impacting process automation environments and implementation of the appropriate updates and/or development of new processes/controls.

Building organizations on check-based compliance toward regulation does not create secure environments. Creating a culture of transparency and trust is key to developing the ability to defend the nation's critical infrastructure. Cybersecurity remains a priority for the chemical industry. Organizations that share data internally and across their industry sector will find they have an advantage in response time. Although every organization differs in cybersecurity requirements, a modular approach guided by stakeholder input across departments and/or business units strategically navigates these differences producing a well-grounded cybersecurity capability. ■

Dietz Ellis is director; Michael Gomez is partner; Tim Johnson is partner, transaction services; Brad Raiford is manager, cyber services; and Deborah Watson is director, information services with KPMG, a global network of professional firms that provide audit, tax and advisory services.