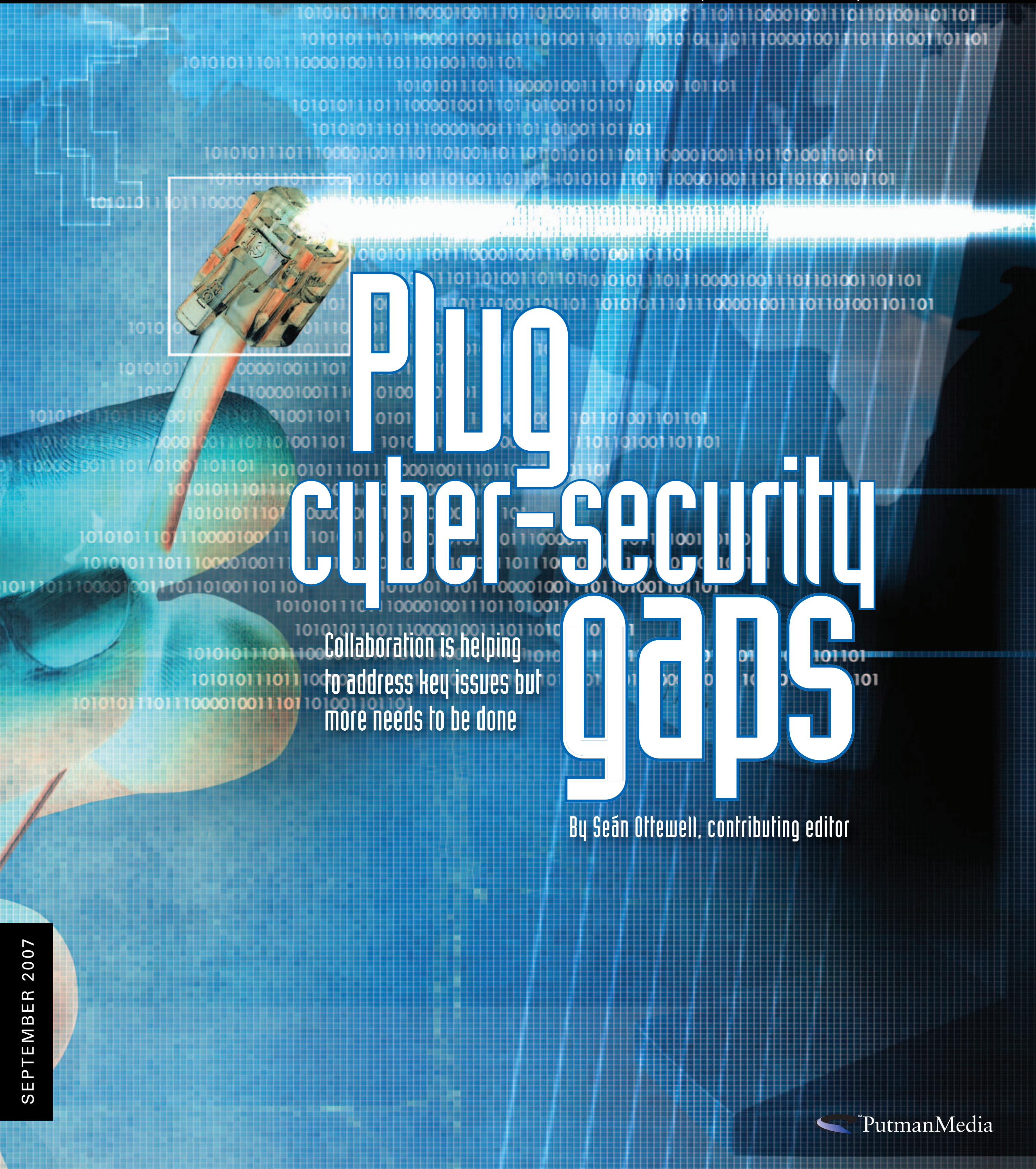
WWW.CHEMICALPROCESSING.COM

CHEMICAL PROCESSING

LEADERSHIP | EXPERTISE | INNOVATION



Plug cyber-security gaps

Collaboration is helping to address key issues but more needs to be done

By Seán Ottewell, contributing editor

SEPTEMBER 2007

PutmanMedia

With emerging high-profile U.S. government involvement in plant security, particularly by the Department of Homeland Security (DHS) under the new, first-ever federal anti-terrorism regulations for "high risk chemical facilities" (www.chemicalprocessing.com/articles/2007/095.html), the chemical industry must ratchet up its efforts. Both physical and cyber-security are getting increasing attention. Adequately protecting the plant perimeter and assets from physical intrusion, while undoubtedly often difficult, involves items that can be seen and issues that are readily understandable. Achieving robust cyber-security, on the other hand, means addressing communications, computer coding and other such factors that aren't visible or as easy to grasp. However, cyber-security certainly is getting high visibility today. There's a surge in interest in cyber-subjects such as security certification, defense-in-depth strategies, risk-based planning and improved policies and procedures.

Testifying to the high interest, cyber-security is a hot topic at many user group meetings and other conferences and forums at which vendors and their customers meet to develop and exchange ideas.

For example, the latest meeting of the Chemical Sector Cyber Security Program (CSCSP) of the Chemical Information Technology Center of the American Chemistry Council, Arlington, Va., attracted a record turnout. A total of 69 attendees representing 24 chemical companies, 11 technology providers, three academic institutions and DHS gathered in May in Miami to hear speakers tackle subjects such as integrating cyber-security with physical security and the supply chain, protection of intellectual property, cyber-security risk and compliance and trends in operational risk management.

Eric Cosman, steering team sponsor for the CSCSP's manufacturing and control systems team says that all the discussions and good practice developed over recent years are finally giving cyber-security a critical mass.

"Big companies like ours have been working on it for a long time," says Cosman, who is an engineering solutions architect for Dow Chemical. "However, things really didn't start to take off until after 9/11 and specifically the summer of 2002 with the launch of the CSCSP strategy. Before this, the level of awareness was very low because security is a very specialized topic. Over the last five years it has moved into the mainstream."

The increasing number of consulting firms and vendors offering services related to cyber-security certainly bears this out. For instance, at that meeting, Deloitte Consulting, East Brunswick, N.J., outlined how the growth in guidance and regulation had enabled it to develop such a service. Meanwhile, Invensys, London, U.K., for one, driven originally by demand from the U.S., has formed an enterprise network and security team to provide cyber-security consultancy services. It aims to provide packaged solutions, going right from initial site assessment to managed security services and covers any vendor's technology. The group currently is expanding its operations in Europe, the Middle East and Asia.

>> Certified secure

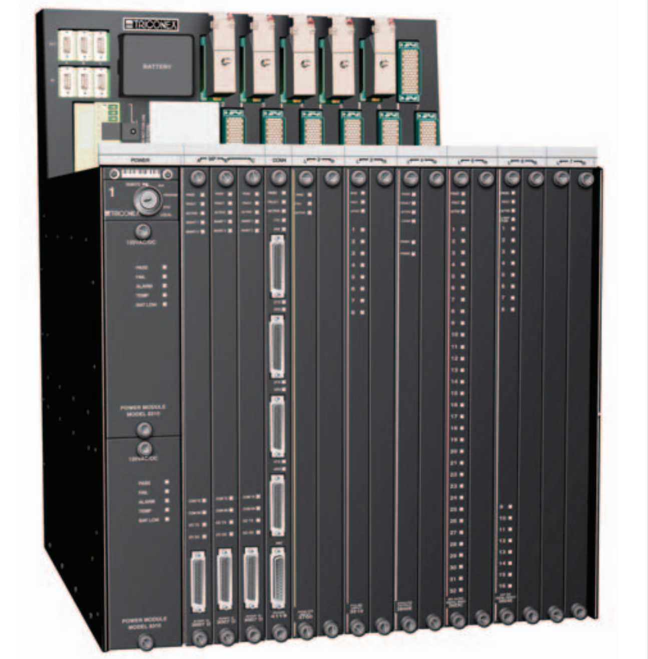


Figure 1. This controller was one of the first to successfully pass Achilles tests. *Source: Invensys Triconex.*

Cosman believes that the next hurdle is to turn this improved awareness and practice into usability.

"In my opinion we need security to be designed into other systems and to be operated in the same way as the industrial control system. In that way, it would be configured and used by control systems engineers in the same way as another system."

Cyber-security certification

One factor that certainly relates to usability is proving that products actually are secure. To meet that challenge, vendors increasingly are going to third-parties such as Wurldtech Labs, Vancouver, B.C., to certify the cyber-security of their offerings.

Wurldtech last year launched Achilles. It's designed to assess the overall security of industrial controllers and is claimed to provide the most complete, accurate and trustworthy information possible on their security. Products that pass its tests get a security certification. Level 1 certification focuses on Layers 2 to 4 (from supervisory control to the enterprise systems such as business planning and logistics) and the implementation of common protocols such as Ethernet, ARP, IP,

ICMP and UPD. So far, six controllers — from Emerson, Invensys, Yokogawa and ICS Triplex (which was just acquired by Rockwell Automation) — have earned Level 1 certification.

In Emerson's case, the testing covered its DeltaV controller and firewall. "Controllers with Level 1 certification have demonstrated the robustness to survive network cyber-attacks. One real benefit of passing these rigorous tests is to provide users with the ability to better plan the installation of security updates and new anti-virus signatures. Knowing that the controllers can survive a possible security incident provides an opportunity to schedule these patching tasks around process activities rather than always immediately deploying the updates," explains Bob Huba, Emerson senior product manager.

Invensys Triconex, Irvine, Calif., which specializes in safety instrumented systems, achieved certification for its Tricon version 10.3 controller (Figure 1). "Triconex systems have established the industry benchmark relative to international functional safety certifications. The achievement of Achilles certification for our Tricon system platform demonstrates our leadership in cyber-security, as well," boasts Luis Duran, Triconex brand director.

One of the key points to note about Wurldtech's certification program is that to be successful candidates must employ robust defense-in-depth strategies.

For example, DeltaV achieves this by providing rings of protection; an intruder must get past successive layers of protection devices. The DeltaV network sits at the center of protection layers that reportedly provide as much system isolation as possible from attacks originating in the plant LAN.

Triconex voices a common view that the move to open standards and protocols such as Ethernet and TCP/IP poses a significant security threat to devices. So, the company has just introduced a new Tricon Communications Module (TCM) with embedded OPC server. The TCM, which was used to communicate to the Tricon controller during the Achilles testing, is specifically designed to facilitate a secure information flow from the Tricon safety system to distributed control systems using standard protocols

Going beyond firewalls

Defense-in-depth was at the heart of what Eric Byres, CEO of Byres Security, Lantzville, B.C., spoke about at June's Honeywell Users' Group Americas 2007 Symposium in Phoenix, Ariz. He calls for a shift in the way industry looks at security, stressing that hiding behind a great big firewall isn't a viable solution. "Defense-in-depth is critical and those best practices are available now. We need to start using them," he says.

At the same conference, Kevin Staggs, global security architect for Honeywell, Morristown, N.J., also emphasized that defense-in-depth is a key strategy in ensuring cyber-security. Honeywell is partnering with both customers and suppliers, he notes, and is active on standards committees such as SP99 and SP100. He also points out that the company has issued various guides to help customers get up to speed with state-of-the-art cyber-security procedures and practices. Other vendors are doing likewise.

That said, Byres is convinced that a shift to defense-in-depth is happening at a certain level, particularly at the biggest companies in the chemical and oil industries. "But this still takes a surprising lot of convincing for some people. They think the firewall does it all and still have trouble understanding the importance of layers of protection," he adds.

Another challenge identified by Byres is the need to take a risk-based approach to the issue of cyber-security. "Safety is the perfect model for this and we can teach the risk-based approach to the IT world rather than the checklist approach that they use now. There's no doubt that some people are getting this, but it breaks down a bit in tier two companies — those that are not quite as rigorous in their approach to safety or that don't come from a safety-oriented background."

Getting a risk-based approach to take hold can be tough, notes Karl Williams, principal consultant, security for Invensys. "There aren't many who understand this. One interesting problem occurs when you get people on the IT/business side of the company and others on the operations/plant side and sometimes no bridge between them at all. In fact in some companies these can even be run as separate operations. Then you can end up with an IT versus operations/plant situation."

"Security needs to take a risk-based approach like that used in safety. So you need strategies to mitigate the risk. That requires more involved level of risk mitigation," says Jim Cahill, marketing communications manager for Emerson's Process Systems and Solutions business.

And underpinning all this work on certification, defense-in-depth and risk-based approaches are those all-important policies and procedures.

"Policies and procedures are a quick win area. Managing something as simple as laptops or memory sticks can be crucial," says Williams. Byres agrees. "All the technology in the world won't help you if you don't have the procedures in place."

Potential ISA role

Vendors are not only working more closely with third parties such as Wurldtech, McAfee and Microsoft but also are working more closely with each other. "We, the suppli-

ers, all believe cyber-security is not an area of differentiation — we need to do it," stresses Emerson's Cahill. "There's been a lot of contact between users and manufacturers to see where we can work together with respect to cyber-security — we're all very keen to do this," agrees Invensys's Williams.

The latest initiative in this collaborative effort involves the Automation Standards Compliance Institute (ACSI), Research Triangle Park, N.C., which is sponsored by ISA. As *CP* was going to press ACSI was in the midst of lining up members among tier one chemical and oil companies to support establishing an ISA Security Compliance Institute (SCI).

Many people think a firewall does it all and don't understand the importance of layers of protection.

"The idea for the SCI came from a group of about 15 initial companies on a standing group," says Andre Ristaino, ACSI managing director. "These included the larger suppliers of automation control products such as Invensys, Honeywell and Yokogawa plus the asset owners such as BP and Dupont. They put in the money to do a feasibility study."

This group has established the mission for the proposed organization. Unlike Wurldtech's Achilles Certification mark, which is a third-party endorsement of product quality, the aim of the SCI is to decrease the time, cost and risk of developing, acquiring and deploying control systems by establishing a collaborative industry-based program among asset owners, suppliers and other stakeholders.

ACSI says that a well designed and managed product-security certification process will reduce users costs and time commitment in product selection and deployment. For suppliers and integrators, the certification process provides a single conformance framework and an industry stamp of approval, resulting in faster time to market and lower development and integration costs. ACSI adds this also will help standards bodies and government agencies developing industrial security specifications to provide better, field-tested standards that are clearly being followed by industry. An ultimate goal of the organization is to push the conformance testing into the product development life cycle, so that products are more intrinsically secure.

"The ISA Secure designation that is expected to arise from the effort will identify and promote security-standards-conformant products and systems," notes Ristaino. "Certification provides the formal recognition of a product's conformance to an industry standard security specification, creating a key differentiator for the product."

The idea is that by 2010 an ISA description on procurement documents will indicate whether a product is ISA Secure. The next stage, planned for 2012, would cover out-of-the-box secure interoperability between different vendors' products.

Procedures aren't left out of the equation, either. "We're starting from the point of view of what is most measurable and then moving on to what's perceived as less urgent and harder to measure. So we start with the product, then its installation/integrity and finally the procedures," says Ristaino.

The due date for membership application returns was September 1, and Ristaino is quietly confident that the SCI will be up and running soon. "Yes, based on our feedback we are confident. We have the budget, full time staff and separate corporate identity that's really needed to run a program like this," he says.

A well-designed and managed product-security certification process will reduce user costs and time commitment.

For his part, Eric Cosman hopes that the idea will be embraced quickly by some of the bigger vendors. "If a couple of large companies come on board, the others will go along, too. I'm very in favor of the idea of the SCI; it's on the right track and the timing is right, too."

Cosman is involved in the ISA SP99 (Manufacturing and Control System Security) Committee, specifically as lead editor for the ISA SP99 Part 1 standard. Its publication would coincide with the SCI getting up and running, thus giving the organization a standard to measure against.

Eric Byres very enthusiastically supports the proposed new standard, describing it as "absolutely necessary." "Eventually some organization such as DHS is going to say that you have to comply with a certain standard. This would be relatively painless if that standard is already in place, but if it isn't, it will be made up by a government official and that could be exceedingly painful." **CP**

Reprinted with permission from Chemical Processing, September 2007.