WWW.CHEMICALPROCESSING.COM

CHEMICAL PROCESSING

LEADERSHIP | EXPERTISE | INNOVATION

CYBER SECURITY

SHIELD GETS STRONGER

Significant enhancements promise to bolster plant defenses

By Seán Ottewell, Editor at Large

STUXNET AND Shamoon acted as a wake-up call about the dangers of cyber attacks for many in the chemical industry and beyond. (For details about these two attacks, see "Potentially Serious Threat Targets Control Systems," http://goo.gl/Nx0c5b and "Recent Security Breach at Saudi Aramco Solidifies the Notion of Preparing for the Worst," http://goo.gl/OZLsjt.) Unfortunately, cyber threats persist and are growing in number.

"The entire critical infrastructure is now under threat," warns Bob Huba, Emerson Process Management product manager/system security architect marketing/business development, Round Rock, Texas. "Everyone and everything is a target," adds Jay Abdallah, Schneider Electric's EMEA cyber security manager, Jebel Ali, Dubai.

For automation vendors such as Emerson Process Management and Schneider Electric and specialist firms like Waterfall Security Solutions, Calgary, Alberta, and PAS, Houston, that offer defenses against cyber threats, the challenge is both to provide chemical companies with the cyber security they need, and to ensure the companies understand what these offerings really can — and can't — deliver.

"Before Stuxnet, users thought they were not security targets and were secure by being obscure. Security was not a 'hot topic' for them. Then came Aramco and Shamoon, and there is now a lot more emphasis on security by our customers. As a result, we've added more features and certifications to our products since then," notes Huba.

THE ROLE OF CERTIFICATIONS

Emerson has been Achilles Communications level 1 certified since DeltaV version 8 in 2006. (The certification comes from Wurldtech, Vancouver, B.C., which offers two security certification programs, Achilles Communications for device robustness with wire and wireless communications protocols, and Achilles Practices for practices used in system development lifecycle processes.) The company currently is working on Achilles Communications level 2, which should be completed in early 2015. In addition, the company has been Achilles Practices certified since 2011 and will complete its third annual certification by the end of 2014.

Users certainly should look for such certifications, says Huba. However, the success of any solution depends on how well a particular user understands cyber security as a whole, he cautions. "Certification doesn't make you secure; what it does do is assure the user that we have done a certain level of testing and have the expertise and awareness needed for that piece of equipment. It's very, very different from ATEX certification, for example, which gives a guarantee against a piece of equipment failing. You can't get an absolute guarantee of security."

It's important that users understand what the different certifications actually signify, he notes. Achilles Communications level 1, for example, means equipment can withstand a certain level of attack before it starts to respond inappropriately. ISA Secure (from the Security Compliance Institute of the International Society of Automation, Research Triangle Park, N.C.) adds some nuances to this, but is still focused on devices rather than systems. On the other hand, Achilles Practices certification means that a vendor complies with the cyber security standard of the International Instrument Users Association (WIB), Den Haag, the Netherlands, and thus is capable of providing products and services that make systems more secure.

"I don't think customers grasp this difference. They have to be intelligent about security in order to make intelligent decisions on what it can really do. While safety certifications ensure products are certified, systems and procedures have also to be put into place for full system security. Right now, however, there is no system certification for cyber security," Huba stresses.

Cyber threats won't disappear. So, you're never done; there are no "plug in and forget" solutions, he adds. Keeping up-to-date with upgrades, updates, patches and the like is essential; constant vigilance is very important.

To spur such vigilance, Emerson is striving to educate customers on the whole security issue. At the heart of this is an effort to ensure people on the operations side get a much better understanding of

ESSENTIAL COMMUNICATIONS

Figure 1. Meetings between people in operations and IT can enable each group to better understand what the other is doing. *Source: Emerson Process Management.*

what people on the information technology (IT) side are doing and vice versa (Figure 1).

"Companies are in different places with this IT/automation understanding, but for progress you have to understand how an automation system is designed, developed and run. Once IT and operations people understand each other and work together, we will get very much better security," he concludes.

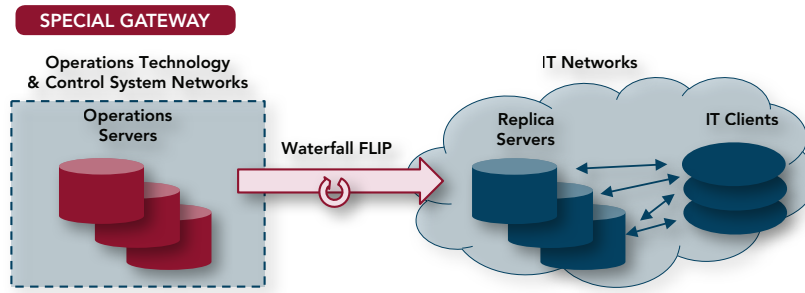

Figure 2. New unidirectional gateway allows temporary, controlled external inputs. *Source: Waterfall Security Solutions.*

While everything is a potential target, the success of any attack depends on the inherent vulnerabilities, the criticality of the assets and the ability to exploit these weaknesses — whether in the control, supervisory-control-and-data-acquisition (SCADA) or safety systems or in web gateways, databases or email infrastructure, stresses Schneider Electric. So, as the industry moves toward ISA Secure regulations, particularly EDSA (embedded device security assurance), SSA (system security assurance) and IEC 62443 (network and system security for industrial-process measurement and control), all Schneider Electric automation developments now encompass security from concept to delivery.

"An important security consideration, regardless of the industry, is risk calculation. This ultimately provides the appropriate framework and controls necessary to protect the most critical assets," says Abdallah.

"Automation systems will continue to be targets but the appropriate and responsible reaction by vendors must be how to manage the vulnerabilities and risks to acceptable levels. We can't control threats, they will always be there. What we can do, however, is deliver a consistently updated, protected and hardened system that utilizes several layers of defense (defense in depth) to protect the most critical assets," adds Gloucester, U.K.-based Gary Williams, Schneider Electric's technology manager, cyber security and communications.

The company sees great value in using next-generation firewalls, configured with specific single source/destination policies, security zones, network anti-virus, intrusion prevention and deep packet inspection.

DATA DIODES

"If properly configured, a firewall can absolutely provide a suitable level of protection. The key here is 'properly configured,' and if clients need the assurance of a unidirectional traffic pass at the hardware level, without worrying about the configuration aspect, a data diode is the way to go. Schneider Electric has partnered with vendors to provide data diode devices as part of an enhanced security offering for several of our core offerings," notes Abdallah.

Data diodes traditionally have served to protect government secrets and battlefield linkups. However, their simplicity — they essentially consist of a simple duplex fiber-optic connection with either the send or receive fiber disconnected — is prompting increasing demand in the world of industrial automation. To meet the need, Schneider is working with Waterfall Security Solutions, a provider of data diodes and unidirectional security gateways for industrial control networks.

"The Schneider team has our equipment right now as part of moving forward with our partnership. OSIsoft has tested out equipment that way as well, as has Westinghouse and other vendors. The GE iHistorian team has had our equipment in their labs and put it through its paces, to ensure that there is no impact on GE networks when our equipment separates those networks from external networks," notes Andrew Ginter, Waterfall's vice president of industrial security.

Industrial interest in unidirectional security gateways is benefiting from the wider acceptance the technology is gaining with international bodies. For examples, he cites its mention in the ISA SP99/IEC 62443 documents, its use as a core part of the NERC CIP (North American Electric Reliability Corp. Critical Infrastructure Protection) power-grid standards, and comments from the European Network and Information Security Agency (ENISA) that such gateways are stronger alternatives to firewalls.

The latest product from Waterfall is FLIP, a unidirectional security gateway that temporarily reverses gateway orientation under the control of the protected network to allow occasional external inputs, such as production plans and equipment control schedules (Figure 2). The new

modular architecture reduces rackspace requirements and provides for end-user replacement and expansion of gateway equipment without compromising security or enabling covert channels.

Launched last year, FLIP reportedly has garnered a lot of interest in the chemical industry. "Chemical companies who currently use unidirectional security gateways tend to use removable media every day or two in order to transfer anti-virus signatures and new production orders into the control system network from the corporate network. These folks are very interested in a stronger-than-firewalls approach to automating those manual tasks," says Ginter.

"So a lot of the vendors are partnering with us now to make us part of the security arsenal. One of the problems is that it is hard to make large pieces of software secure. A lot of the legacy automation systems are full of bugs. The vendors are doing what they can with patches, etc., but FLIP can provide a hard perimeter to that software interior," he adds.

FLIP, which started shipping two months ago, already is running at a number of pilot sites and test beds, including some at undisclosed chemical companies.

FIREWALL FALLACIES

Unfortunately, users frequently misunderstand the nature of firewalls, believes Karim Moti, director of marketing with cyber-security software provider PAS.

"Controls and plant personnel still hold a mindset that their systems are isolated because they have a firewall and cannot access email or the internet from machines within the control system. There is not a realization of the multitude of holes that are required in the firewalls in order to provide data to the business side or to allow vendors remote access for support," he explains.

The two primary vulnerabilities to the strong perimeter approach embodied by firewalls are maintaining only required traffic and local access to control system devices, he says. "Communication requirements through control system firewalls are constantly changing. New projects or business reporting requirements bring new requirements to open ports through the firewalls. Management of the firewalls must be diligent to ensure that communication paths are closed after the project is over or the requirement no longer exists. Then there is the issue of local access. Devices in the control system require maintenance and settings changes during the lifecycle of the plant. This work is normally done by connecting a laptop locally to the device. This completely bypasses the protections provided by the firewall and intrusion detection system."

Because traditional security tools don't support many of these devices, the best way to monitor their security is to watch changes to the configuration of the control system devices. However, plants typically have many devices from many vendors, so this is impractical and not effective. That's why PAS developed its Cyber Integrity software.

"Cyber Integrity maintains an accurate and up-to-date inventory and configuration baseline for the entire plant. Configuration changes are detected and reconciled against authorized changes. An incident response workflow is automatically triggered when unauthorized changes are detected," notes Moti.

In May, PAS announced the latest step in the development of the software — a technology partnership with Tripwire, Portland, Oregon, for integration of Cyber Integrity with that firm's risk-based security-and-compliance management software. The goal is to help companies efficiently and effectively achieve NERC CIP compliance.

The integration aims to provide customers with: a single process that enables continuous monitoring and rapidly captures detailed status information across a wide range of critical cyber assets, from computer systems and network devices to badge entry systems and SCADA devices; audit-ready reports and dashboards conveniently grouped via a flexible and extensible classification system; and automated assessment and aggregation of security data alerts that assist in detecting potential security breaches or configuration modifications that affect compliance status.

"This is relevant because many chemical companies have IT solutions such as Tripwire, which can be utilized at the process control layer but which does not have the capability to monitor the configuration of proprietary devices within the control system. PAS has partnered with Tripwire to provide the ability to share configuration information of both commercial off-the-shelf and proprietary devices, enabling a company to have a complete corporate view of all its assets within the company. This facilitates corporate information security resources to support control system security efforts in addition to enhancing risk management at the corporate level," Moti stresses.