Warding Off Digital Attacks: How to Secure Your Process Control Network

Chemical plants must include both their process control and building automation systems when developing a solution to combat security and safety threats

‘Many chemical companies don’t receive consistent information on how to best protect their sites.’ By Marilyn Guhr

4 Major Categories of Real-World Cyber Threats

If asked to picture weapons of terrorism, most people might conjure up images of explosives, biological contagions and the like. They probably wouldn’t visualize a computer memory stick purchased at the local electronics store. But even if a USB drive isn’t typically thought of as a terrorist weapon, it has the potential to produce results ranging from disruptive to devastating. In the world of chemical refineries and processing plants, a memory stick could easily infect a plant’s process control system with a virus and potentially put the safety of its workers and surrounding community at risk. Chemical plant security has become one of the most scrutinized issues since the Sept. 11 attacks on the U.S., with lawmakers and experts continuously calling attention to the havoc terrorists could wreak by disrupting operations at these facilities. Yet, many chemical companies don’t receive consistent information on how to best protect their sites.

Lawmakers will soon pass enforceable security regulations for industrial sites. Manufacturers, in turn, must be ready and have a best-in-class security strategy in place. One such strategy is to take a holistic view of the entire plant, considering a comprehensive and integrated approach to security and safety. Since the process control system is the heart of any chemical plant, ensuring you have a secure process control network (PCN) is a place to begin. The PCN is one of the most critical areas of a chemical facility &#151 and can be one of the most vulnerable to the growing threat of cyber terrorism. Cyber threats can be grouped into four categories: 1. Indiscriminant and potentially destructive: This is the most

publicized category, which includes viruses, Trojan horses and worm attacks. 2. Performance impacts and potential safety issues: Network spoofing and “denial-of-service” threats have performance implications. For example, a denial-of-service attack can clog a PCN with spurious requests, keeping an operator from receiving a legitimate alarm. 3. Confidentiality: With eavesdropping and password cracking, confidentiality becomes a concern. 4. Confidentiality, integrity and performance: This area includes data tampering, impersonation and packet modification and is especially hazardous if the intruder has malicious intent. All these categories have attendant safety issues. If the system is compromised, safety is compromised. Despite these threats, the PCN must provide a level of reliability, availability and performance to ensure a safe, uninterrupted operation. Securing a PCN involves several measures, which are examined below.

Assessing Vulnerabilities

The key to strengthening security at any facility is understanding existing weaknesses. An assessment should establish a baseline of a company’s current security processes, procedures and safeguards used to protect the PCN from external threats. That baseline is then the focus of recommendations that outline the procedures and changes that will remove or mitigate identified vulnerabilities. PCN vulnerabilities can be ranked based on their risk potential, and most sites will have some low- and medium-risk areas as well as a few high-risk areas. Some of the higher risk vulnerabilities are associated with poor or non-existent security policies including poor password management, missing or out-of-date anti-virus software and ineffective processes for communicating policies. Unsecured open ports present opportunities for the introduction of viruses. Consider that someone could cause significant disruption simply by inserting an infected USB stick in an unsecured open USB port and, as mentioned above, injecting a virus into an otherwise “clean” system &#151 an instance of “sneaker net” meeting cyber space.

Designing Network Security Infrastructure

[1] _____

Once identified, the next step is to design a solution that removes or mitigates these identified vulnerabilities. For example, a high-risk vulnerability is a direct connection between the corporate network and the process control network. This kind of configuration opens the doors for viruses, worms, etc., to be introduced into the PCN from the corporate or business network and vice versa. A more secure infrastructure would include a “demilitarized zone” with enhanced firewall protection for the PCN. This approach adds a new level of network security, controlling communications between the corporate network and PCN and minimizing potential threats.

Deploying Hot Fixes and Service Packs

The efficient and timely qualification and validation of hot fixes and service packs, such as those fixes issued by Microsoft, are key to a successful security strategy. It is incumbent on the process control vendor to validate and qualify these hot fixes and service packs for their platforms, providing up-to-date information to their

customer bases. Vendors who make this information readily available are providing great benefit to users of these systems.

Qualifying Antivirus Software

Process control vendors also need to be supportive of their customers with regard to the qualification of anti-virus software. And, since one leading anti-virus offering may be preferred over another, offering a choice of qualified anti-virus software is a plus.

Locking Down Control Network Nodes

Vendors can embrace a locked-down model that facilitates system security, providing customers with pre-configured security settings for files, directories and registry keys to protect against viruses, malicious users and inadvertent actions. Such a model would provide pre-configured groups and group policies that define the desktop behavior within an organization by role. Consider the following scenario. For operators, the policies would be very secure (or locked down), limiting the user to auto-start applications. For supervisors, the policy would be similar, very secure/locked down. Engineers, on the other hand, would be restricted to relevant engineering functions. Administrators might have unlimited access with secure settings such as screensaver with password after 15 minutes of non-activity. Basically, this model type focuses on controlling the desktop by user role, limiting what is seen via the “start” menu and restricting which Windows tools/functions may be invoked. The first step in the security journey is the assessment. Understanding and documenting vulnerabilities provides the best foundation for developing an approach that balances security and functionality. From this assessment, the design that meets site requirements can be developed. Once implemented, the cycle begins again &#151 with an assessment, at least on an annual basis, to verify that new vulnerabilities have not been introduced or existing ones have not been ignored. Although focusing on the process control network’s security aspects is very important, chemical companies cannot afford to lose focus on the entire facility. A holistic view of the plant ensures the protection of assets and people. Other vulnerabilities in plants can range from a lack of perimeter security to the challenges of tracking employees, contractors and visitors on-site. Security and safety concerns include the ability to move workers to a safe location within the plant during an emergency (also called mustering) and the ability to coordinate with first responders. In some plants, out-of-date technology hampers the ability to achieve the best results. The best solution a chemical plant can use to combat modern security and safety threats should include both process control and building automation systems. A unified system translates into faster event response, less-expensive implementation and lower maintenance costs. Ultimately, security is your responsibility. It’s best to work with a vendor that has a keen focus on security and an established track record. And, remember, security is a journey, not a destination. Peace of mind is the reward. *Marilyn Guhr is manager of global marketing and business development for cyber security and network services at Honeywell Process Solutions, 2500 W. Union Hills, P16, Phoenix, AZ 85027. Her expertise is in migration strategies, open systems infrastructure and services utilized to frame open systems, network and security service offerings. She has Six Sigma Certification. Questions about this article can be addressed to her at*

602-313-3362. Additional information is available at www.acs.honeywell.com.

Source URL (retrieved on *11/27/2014 - 1:45am*):
http://www.chem.info/news/2006/08/warding-digital-attacks-how-secure-your-process-control-network?qt-most_popular=0

Links:
[1] http://www.chem.info/ProductImages/0605/redsphere_lrg.jpg