Q&A With Enterasys: Secure Networks in Focus

The goal of Enterasys Networks, a company based in Andover, MA, with more than 3,500 customers, is to deliver secure networks that ensure the integrity of IT services. It designs, deploys, supports, and services integrated hardware and software solutions that intelligently sense and automatically respond to security threats &#151 and proactively prevent threats from entering networks. CHEM.INFO asked the company's vice president of marketing, Trent Waterhouse, to share his thoughts on today's security challenges. Waterhouse joined Enterasys in May 2006 with more than 15 years of high-tech hardware and software marketing experience.

Q: What's the most significant challenge when it comes to securing networks in industrial automation settings?

A: Industrial automation is a key foundation technology for the manufacturing and energy sectors, which are considered critical national infrastructure that needs to be protected from electronic terrorism based on its potential to disrupt the U.S. economy. The Enterasys Secure Networks for Industrial Automation solution is the first and only connectivity offering built to withstand the harsh environmental conditions of heavy manufacturing and energy industry facilities while simultaneously protecting the confidentiality, integrity, and availability of these real-time applications without sacrificing performance. Enterasys' unique role-based architecture ensures that devices and users are enabled and confined to specific behavior on the network. In addition, Enterasys' advanced QoS provides deterministic control of the proprietary applications found in industrial environments. The I-Series provides the automation industry with a fully hardened switch without sacrificing high-end functionality.

Q: What is the most common mistake made when selecting a network?A: Why buy "regular" industrial Ethernet when for the same or less money you could have "secure" industrial Ethernet. Security cannot be "bolted on" to the network somewhere. It needs to be built in everywhere to provide proactive protection against electronic threats and vulnerabilities on every single connection in the network &#151 fiber and copper, wired and wireless. Enterasys Secure Networks for Industrial Ethernet solutions can automatically sense and respond to security incidents in fractions of a second, assuring reliability and avoiding costly downtime of production control resources.

Q: How can solutions be built so that they withstand the harsh environmental conditions of chemical processing plants?A: The Enterasys I-Series is the first enterprise-class Ethernet switch with advanced security built to withstand the hot, dusty, and explosive gas conditions of the typical manufacturing plant or energy industry facilities. The I-Series achieves an ANSI/ISA Class-1, Division-2 rating with convection cooling; redundant DC power; industrial-grade components; and self-healing, sub-second, rapid-recovery ring topology protocols &#151 ensuring continuous reliability under the harshest conditions. Serviceability is enhanced through an optional memory configuration card that allows an unskilled attendant to perform a field replacement of an I-Series unit simply by pulling the

configuration card out of the old switch and inserting it into the new one. Copper and fiber I/O modules deliver 100Mbps Ethernet performance with dual Gigabit Ethernet uplinks to offer up to 24 ports of 100BaseTX, 16 ports of 100BaseFX, or a combination of fiber and copper connectivity with dual industrial-grade SFP optical uplinks.

Q: How can the user be sure the networked device (sensor, computer, printer, camera, badge access reader, etc.) is secure?

A: Security is assured through assessment, authentication, and authorization capabilities. Assessment verifies the “health” and “security posture” of networked devices to make sure they have the latest required O/S or application patch levels and virus signature updates. Authentication verifies the identity of the attached devices or users to prevent rogue PLCs, computers, cameras, etc. from gaining access to sensitive network information. If the user or device cannot pass identity authentication, no network access is granted. Authorization uses the principle of “least privilege” to ensure only specific users/devices can access specific applications at specific times from specific locations through role-based security and priority policies.