



SCADA Security Protections Are On The Increase

By **Hugh Njemanze**, Chief Technology Officer, **ArcSight**, Cupertino, CA

Pipeline SCADA systems are becoming more vulnerable to cyber attack. That is because they increasingly are being integrated with existing business information systems and deployed on common operating systems, such as Windows, to more easily provide decision makers with better information. These new connections and common systems have introduced a series of vulnerabilities that are potentially opening the door to viruses, worms and would-be attackers.

Trouble From Within

It is not just threats from the outside that are posing problems, but those from the inside as well. Careless employees can be the source of security risk by failing to update protection software or conducting inappropriate Web surfing and file downloading. Meanwhile, the use of contractors to run wells, platforms and pipelines serves as another vulnerability point for the oil and gas industry. These contractors can introduce security issues if their systems do not meet the necessary standards, especially if they connect to corporate systems through remote access.

Of course, an even bigger risk can come from a disgruntled employee who knows the SCADA system inside and out and is bent on causing damage. This was the case with a former employee of an Australian sewer control plant who decided to seek revenge after being turned down for re-employment. Armed with only a laptop and a data radio, he gained access to his employer's SCADA network from his car. He then proceeded to release 264,000 gallons of sewage into waterways. He was later convicted on 26 counts of unauthorized access to SCADA system computers and causing intentional damage.

Scare Tactics?

It is not unreasonable for some organizations to dismiss the recent talk of SCADA attacks as nothing more than scare tactics. After all, most doom-and-gloom predictions about cyber terrorism have never materialized. Even some of the most strident security experts say the risk that terrorists will strike a SCADA network is relatively small, mostly because a cyber attack may not scare the public as much as, say, a

subway bombing. Moreover, no one has ever been killed by a cyber terrorist.

Regardless, the danger is real. In 2001, the U.S. military discovered evidence in Afghanistan that al-Qaida terrorists were researching SCADA systems and cyber terrorism. Further, in the most comprehensive study of its kind, the British Columbia Institute of Technology found that major companies in the U.S. and other nations have recorded 135 SCADA security incidents over a period of four and a half years.

This past October, news leaked that the SCADA system at a water plant in Pennsylvania was accessed after an employee's laptop was compromised via the Internet, and then used as an entry point to install a computer virus and spyware on the plant's system.

The good news is that it is possible for oil and gas organizations to better secure their SCADA systems without sacrificing performance or crashing control systems. There is a growing realization that the problem can be addressed — and initiatives are now in place to do just that.

Project LOGIIC

One leading program is Project LOGIIC. That acronym stands for Linking the Oil and Gas Industry to Improve Cyber Security. The Department of Homeland Security (DHS) teamed with oil and gas companies to create Project LOGIIC, a groundbreaking effort to keep U.S. oil and gas control systems safe and secure.

The LOGIIC consortium brought together 14 organizations to identify ways to reduce cyber vulnerabilities in process control and SCADA systems. The goal of the project was to identify new types of security sensors for process control networks, develop better ways to protect the critical infrastructure, and then transfer that technology and know-how to actual field operations.

As a first step, LOGIIC focused on addressing the concern that, unlike business networks, SCADA systems and control networks are not monitored for cyber intrusions — thus making it extremely difficult to detect cyber criminals who might be attempting to compromise critical components.

Attack Scenarios

Consortium participants created a simulation test-bed at Sandia Labs in order to counter potential threats to the oil and gas industry based on hypothetical attack scenarios. One attack scenario highlighted the increased risk that control systems are exposed to as they get connected to Internet-enabled business networks. It showed how an outside intruder can hack into the business network and then, once inside, gain access to other networks, like a SCADA system, and actually tamper with a piece of equipment in the field.

Another scenario showed how an adversary could gain physical access to the process control systems from a remote location in the field, such as a pipeline flow meter. Each pipeline has flow meters at regular intervals to measure the flow of oil or gas. Doing little more than cutting a chain-link fence at the unmanned location, cyber criminals could then gain access to the control system network by simply popping open a box and plugging in their laptops. Once on the network, they could again disrupt operations, and cause even more damage by navigating to other corporate networks.

Yet another scenario outlined how a criminal could gain access to a refinery over a wireless network by spoofing MAC addresses. Once inside the network, the person could navigate into the refinery and actually seize control of the computer that monitors production flows.

Early Warning System

Project LOGIIC, with the help of technology partners like ArcSight, set its sights on identifying solutions that could act as early warning systems for cyber-security events. The goal was to stop intruders before they could cause any damage by correlating and analyzing abnormal events flowing in through the networks.

For instance, Project LOGIIC leveraged ArcSight's event correlation engine to collect messages and log entries from many different devices on the network and infer the relationships among them. If someone repeatedly attempted and failed to log into a work station, for example, those brute force log-in attempts were picked up by the sys-

tem. If somebody changed the IP address of a flow computer, which should rarely be done, that event raised alerts. There were even correlation rules detected rogue users on the network who hadn't been previously identified.

By intelligently piecing together the connections among many disparate events coming into the control center, the LOGIIC system could filter out much of the noise, identify significant patterns and ultimately provide the big security picture to plant operators.

Security For SCADA

Further leveraging technology like ArcSight, Project LOGIIC set about to build smart connectors to data sources unique to the oil and gas industry such as the Telvent SCADA system, the Honeywell DCS process control system and the OmniFlow flow computer system. Events from those systems were captured and correlated, providing clearer insights into

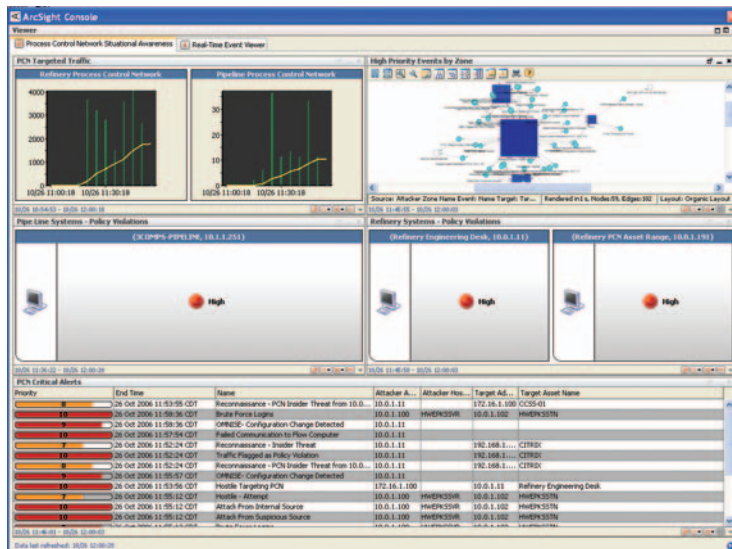
suspicious activity on the network.

To provide even greater situational awareness, LOGIIC assembled a centralized dashboard that mapped out everything from

could, for the first time, get a more complete understanding of everything going on in their environment.

SCADA security is indeed a hot topic these days. Suddenly there seem to be more people with malicious intent investigating ways to leverage a SCADA system to cause damage. However, as evidenced by initiatives like Project LOGIIC, the oil and gas industry is taking this threat seriously and implementing new security steps to protect the critical oil and gas infrastructures. *P&GJ*

Author: *Hugh Njemanze is Chief Technology Officer and Executive Vice President of Research and Development of ArcSight. He has been involved in the enterprise software market for more than 20 years. He most recently worked as the CTO of Verity where he led product development. Previously, he worked at Apple in soft-*



Situational Awareness Dashboard provides an at-a-glance view of your security posture.

spikes in event traffic to policy violations to critical alerts. From that single dashboard, plant operators and oil and gas executives

ware engineering where he was one of the key architects of the Apple Data Access Language (DAL).



ArcSight, a leader in Security and Network Information Management, delivers mission-critical solutions for security, network and IT operations that enable enterprises to turn operational data into action. ArcSight solutions address today's complex enterprise networks that span multiple organizations and corporate business initiatives. By comprehensively collecting, analyzing, managing and responding to security and network data, ArcSight solutions mitigate information risk for real-time threat management, compliance reporting and automated network response. ArcSight's customer base includes leading global enterprises, government agencies and MSSPs.