

[« Back](#) | [Print](#)

Protecting Industrial Networks against Evolved Cyber Threats: Air Liquide

A defense-in-depth security strategy protects Air Liquide against hackers. The head of its U.S. Operations Control Center explains.

By -- Manufacturing Business Technology, July 30, 2009

By Charles Neely Harper, Air Liquide Large Industries U.S. LP

Over the past year, hackers have increased their focus on finding vulnerabilities in technologies at gas, energy and manufacturing plants, with the intent of causing disruption to operations, whether it is for extortion or political gain. Most notably, 2008 saw the buffer overflow vulnerability in the facilities management software, CitectSCADA. This past February, a version of Areva's e-terrahabitat software package (which allows operators in power plants to monitor gas and electric levels, adjust transmission and distribution devices, and automate other core functions) was found to have a swarm of buffer overflow and denial-of-service bugs.

With this increased attention on this industry from hackers, no longer are basic technologies like firewalls enough to stop threats as new variants and attack vectors are created. At Air Liquide, a global provider of industrial and medical gases and related services, we have addressed this increased threat level with a defense-in-depth security strategy, which, following an extensive review of our systems, anticipates not only the current threats out there, but the threats of the future.

With more than 45,000 employees in 78 countries, Air Liquide offers solutions based on constantly enhanced technologies and produces air gases (oxygen, nitrogen, argon, rare gases) and many other gases including hydrogen. Our company contributes to the manufacturing of many everyday products: bubbles in sparkling beverages, protective atmosphere for packaged foods, oxygen for hospitals and homecare patients, ultra-pure gases for the semiconductor industry, hydrogen to desulfurize fuels, among others. We rely on production from nearly 150 plants across the United States to produce our products.

These manufacturing facilities create a unique security environment, where distributed control systems (DCS), programmable logic controllers (PLC) and supervisory control and data acquisition (SCADA) systems are crucial to ongoing operations. Very early on, we recognized that our plants must be protected from the growing potential of cyber threats, and we established sophisticated firewall technology and embedded supervision of existing network technology. However, considering the evolving threat landscape, we brought in a consultant to define a set of additional security requirements that would provide adequate protection of our industrial network, and after conducting extensive reviews, identified areas of Air Liquide's industrial security posture, which while strong and comprehensive, needed additional protection.

Thanks to its radio identification technology based on electronic tags (called "smart tags" or RFID) and its existing platform for data hosting and management, Air Liquide provides industrial customers with on line access to information to track mobile tanks, industrial operations and process automation.

[Learn more about Air Liquide RFID.](#)



Intrusion prevention systems: not just for the IT network

Understanding the crucial role that the industrial network and SCADA systems serve, we examined a couple of different avenues that would enable us to achieve our industrial network security objectives, beginning with simple TCP/UDP port blocking approaches in layer 3 switches, but the resulting protection capabilities of that solution did not align with what we envisioned. The layer 3 switch port blocking option proved less than ideal due to its inability to inspect traffic that was allowed through the open ports, leaving significant exposure to cyber threats. In addition, device configuration and management was a manual activity that would burden the Air Liquide IT staff.

As we pored over potential solutions, an important factor in the equation was the cost-effectiveness of the solution, since it would need to be deployed across our 200 plants nationwide.

Traditionally, when one thinks of intrusion prevention and firewall technology, it is in reference to the enterprise network on which the business collaborates or conducts transactions. However, we felt that the separate industrial network that powered our plants and SCADA systems would prove to be an innovative and cost-effective application of intrusion prevention system (IPS) technology while further illustrating our commitment to continuous plant operation and reliability of supply to our customers. We evaluated a list of network intrusion prevention solutions that could help us accomplish this goal and selected Top Layer Security's IPS 5500 solution, as it was the only one that combined the high levels of performance with the deep packet inspection that made us comfortable with putting it inline in our network, which simply cannot afford a minute being offline.

The right network performance makes all the difference

Air Liquide operates a small data center in each of its facilities, processing terabytes of data for the real-time command and control environment of SCADA, where thousands of data feeds are used to control pipelines, change production in plants, etc. Within these "command centers," personnel sit behind several consoles that control the manufacturing process. We were able to position the Top Layer IPS 5500 to protect these command centers from the threats of the outside world, as our performance requirements were easily exceeded by the high-performance network operation it delivers. SCADA traffic volume is usually somewhat small, but the high throughput of the IPS 5500 translated into increased protection against cyber threats with no detectable latency whatsoever, which gives us comfort in knowing that systems are running at optimal performance levels.

By moving forward with the implementation of Top Layer's IPS on our industrial network, we can depend on its highly-reliable deep packet inspection to protect the SCADA systems and industrial network from cyber threats that exist around every corner of the Internet. With intrusion prevention now part of our defense-in-depth strategy along with sophisticated firewall and other embedded supervision, we've been able to instantly identify oversized ping packets, and nefarious DNS protocol violations.

In addition, the bypass mode on the Top Layer IPS 5500 enabled us to plug the device into our network and immediately identify many active attacks originating from countless sources, many from locations we would have never guessed. A number of these threats were initiated by compromised computers that had not been patched with the latest Microsoft security updates, which alerted us to revise its patching process along the way.

Gaining the ability to view what is happening not only on our computer network, but on our industrial network, is enlightening. The visibility into this world of previously undetected cyber threats reassured our team that we were doing the right thing by adding intrusion prevention technology across our industrial network. As new vulnerabilities arise in other SCADA technology, often the Top Layer IPS can proactively protect against related attacks (e.g. attacks against the SCADA overflow vulnerability), and for each new vulnerability, Top Layer's TopResponse automatic update program provides us with the necessary steps for protection.

A different type of regulatory driver: FDA's impact on network security

At Air Liquide, we certainly put a priority on standard industry compliance regulations, but also, because we help customers increase productivity, manage their industrial gas supplies and improve the yield of their process or production sites, many of our gas products must be pharmaceutical-grade as regulated by the Food and Drug Administration (FDA).

The challenges of meeting FDA requirements highlighted our need for our industrial network and SCADA systems to be adequately protected, as a computer compromised by viruses, worms or other malware could negatively affect the production system, and ultimately lead to a violation of FDA regulations. Although FDA regulations are not commonly cited in IT security projects, they became a crucial consideration in Air Liquide's security ecosystem nonetheless.

To that end, Air Liquide embarked on a nationwide initiative to deploy IPS units across more than 100 sites in the U.S. Protecting our industrial network separately from our IT network proved to be a significant undertaking, but one well-worth the effort, as the potential losses associated with stalled production and remediation made the business case quite clear.

It can be easy to underestimate the value of vendor support when implementing a new solution, but, combined with top-notch technology, the entire Top Layer Security team was, and continues to be, great to work with - hands-on, thoughtful and responsive to our unique business needs for this endeavor.

As other gas and energy manufacturers consider protecting their industrial network against the threats present today, as well as those

coming tomorrow, an intrusion prevention system can prove to be a highly effective part of any defense-in-depth strategy to step up to the next generation of protection.

Charles Neely Harper is Director, National Supply & Pipeline Operations and head of Air Liquide's U.S. Operations Control Center (OCC) in Houston, Texas, a specialized team and state-of-the art facility that he has spent his entire career building and refining. He also holds the title of Air Liquide International Senior Expert, one of 57 around the world, for his work in Technical Operations - Plants and Pipelines. Charles began his career with Air Liquide in early 1977 in the operations of utility and air separation technologies at the Bayport, Texas plant. In 1979, Charles began to develop what was to become the OCC (Operations Control Center) by implementing the first industrial gas program to optimize the pipeline networks along the Texas Gulf Coast and Mississippi River. Since then, Charles' OCC team of engineers and specialists has continued to expand the decision support systems that now serve all Air Liquide's primary production facilities in the U.S.

Other important articles on industrial cybersecurity issues and tactics:

- [Cyber security: Safety instrumented systems, 5 incidents](#)
- [Security incident database public access: SCADA, manufacturing, process control cyber security info](#)
- [Industrial Cybersecurity Blog Posting: Industrial Control Systems Joint Working Group \(ICSJWG\) 2009 Fall Conference](#)
- Edited by Renee Robbins, MBT www.mbtmag.com

[« Back](#) | [Print](#)

© 2009 Reed Business Information, a division of Reed Elsevier Inc. All rights reserved.