



Published on *Government Security News* (<http://www.gsnmagazine.com>)

[Home](#) > Paradigm shift in SCADA security

## Paradigm shift in SCADA security

By *JGoodwin*

Created 06/20/2011 - 3:53pm

By: [Andrew Ginter](#)<sup>[1]</sup>

Change is coming in the world of industrial control systems or "SCADA" systems. There was a time when the computers and networks controlling most power plants, chemical plants and other critical infrastructures were not connected to external networks at all.

That changed in the mid-1990's. Businesses learned that there were big profits locked away in real-time inventory, equipment usage and other data. Firms started connecting their control system networks to their corporate networks. Fast forward to today. In the last 24 months, high-profile "advanced persistent threat" intrusions have successfully compromised an appalling number of military, government and corporate networks. In recent months, a handful of well-documented attacks took over control system computers as well. Imagine learning that parts of your safety-critical control system are under the thumb of adversaries on the other side of the planet.



*Andrew Ginter*

Cyber-security for industrial control systems has become a priority in recent years. A new development in network perimeter protection is gaining momentum; some even call it a paradigm shift -- *Unidirectional Gateways*.

A Unidirectional Gateway is simple in concept -- a pair of network appliances connected by a fiber-optic cable. The transmitting (TX) appliance in the control system network contains a laser. The receiving (RX) appliance in the corporate network contains a photocell. The TX can send to the RX, but not vice-versa.

Real-time data can get out to where the enterprise needs it, but no attacks, no viruses, nothing in fact, can get back through the gateway hardware to threaten the control system. Think of it as physical-layer protection for your network.

This comes as a paradigm shift for corporate IT security teams. To such teams, firewalls are very much the first line of perimeter defense. The problem is that firewalls are software systems -- software in the firewall looks at every message and decides whether to let it through. Software has vulnerabilities and advanced threats can exploit those vulnerabilities.

Unidirectional Gateways got started in arenas where security was paramount -- nuclear reactors and other very sensitive industrial sites. The latest Nuclear Energy Institute guidelines for the cyber security of reactor control networks offers two choices: either no connections at all across the perimeter of the most sensitive networks, or unidirectional connections only.

Other industries are taking note. It is bad enough these "advanced threats" are wreaking havoc on government and corporate networks. Nobody wants them taking over a power grid, or an oil pipeline or a chemical plant.

Think about the consequences of the last couple of industrial disasters the nation and the world have seen -- the Gulf oil spill and the tsunami at the Fukushima reactors. Now consider that advanced threats regularly compromise the best-protected corporate and control system networks. Put this together and firms are concluding the risk is unacceptable. Industrial sites are looking seriously at once more isolating their most sensitive control networks. Unidirectional Gateways provide the same protections as complete network isolation, but without cutting off access to the most valuable real-time data.

This is a big change for IT security. IT assumes they can control every machine and every component of their networks. They assume they can diagnose problems, fix them and make other changes, all from the comfort of their desks. The problem is that if they can do it, advanced attackers can too. The new thinking for control systems is network isolation via Unidirectional Gateways. IT will have to get used to it.

**Andrew Ginter is director of industrial security for Waterfall Security, of Calgary, Alberta, Canada. He can be reached at:**

**[andrew.ginter@waterfall-security.com](mailto:andrew.ginter@waterfall-security.com)**

[Homepage](#) [Market Sectors](#) [Technology Sectors](#) [Commentary & Opinion](#) [Infrastructure Protection](#) [Cyber Security](#) [Disaster Preparedness](#) | [Emergency Response](#) [IT Security](#)

*GSN: Government Security News*, 4770 Sunrise Highway, Suite 105, Massapequa Park, NY 11762

Phone: 212-344-0759

All content copyright © 2011 World Business Media, LLC. All rights reserved.

[Privacy Policy](#) | [Legal Information](#)

<\scr"+"ipt>"); //]]>-->

**Source URL:** [http://www.gsnmagazine.com/article/23644/paradigm\\_shift\\_scada\\_security](http://www.gsnmagazine.com/article/23644/paradigm_shift_scada_security)

**Links:**

[1] [http://www.gsnmagazine.com/author/23643/andrew\\_ginter](http://www.gsnmagazine.com/author/23643/andrew_ginter)