



## Industrial Control Systems are Vulnerable to Cyberterrorism, says GAO

(5/6/2004)

- Rich Merritt

According to the General Accounting Office (GAO), risks to industrial computer-based systems that control vital critical infrastructures, such as electrical grids, oil refineries, pipelines, and water treatment and distribution, are increasing and could have devastating consequences.

In testimony before the House Subcommittee on Technology Information Policy on March 30, Robert F. Dacey, Director of Information Security at GAO, said, "In addition to general cyber threats, which have been steadily increasing, several factors have contributed to the escalation of the risks of cyber attacks against control systems. These include the adoption of standardized technologies with known vulnerabilities and the increased connectivity of control systems to other systems."

Dacey noted that at least two such attacks have already occurred: "Control systems have already been subject to a number of cyber attacks, including attacks on a sewage treatment system in Australia in 2000 and, more recently, on a nuclear power plant in Ohio."

For the latter example, he is referring to the Slammer worm that penetrated a private computer network at Ohio's Davis-Besse nuclear power plant in January 2003. According to Kevin Poulsen, writing in *Security Focus*, Aug 19, 2003, it "disabled a safety monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall." Fortunately, the plant was shut down at the time, so no one was in danger.

The GAO report includes a detailed discussion of many initiatives to combat the problem. These include:

- Research and development of new security technologies to protect control systems. The Dept of Energy (DOE) is planning to establish a National SCADA Test Bed to test control system vulnerabilities.
- Development of requirements and standards for control system security. The North American Electric Reliability Council (NERC) is preparing to draft a standard that will include security requirements for control systems. In addition, the Process Controls Security Requirements Forum (PCSRF), established by NIST and NSA, is working to define a common set of information security requirements for control systems.
- Promote awareness of control system vulnerabilities. DOE has created security programs, trained teams to conduct security reviews, and developed cybersecurity courses.
- Implement effective security management programs, including policies and guidance that consider control system security.

The GAO threw in zingers throughout the report, noting that funding had been cut to many of the programs outlined above. To see the entire GAO report, go to [www.gao.gov](http://www.gao.gov).

The GAO report also said the Department of Homeland Security (DHS) hasn't moved very fast to deal with cybersecurity problems. As delicately and diplomatically as he could, Dacey said, "Many government and nongovernment entities are spearheading various initiatives to address the challenge of implementing cybersecurity for the vital systems that operate our nation's critical infrastructures. While some coordination is occurring, both federal and nonfederal control systems experts have expressed their concern that these efforts are not being adequately coordinated among government agencies, the private sector, and standards-setting bodies."

According to *Computerworld*, March 31, 2003, James F. McDonnell defended DHS by implying the job was huge. McDonnell, director of the Protective Security Div. at DHS, said it's his job to coordinate physical and cyber security for more than 1,700 facilities identified so far as containing critical national security infrastructure

systems. Of those, 565 contain SCADA systems that must be protected.

"It had never occurred to me that the potential threat from a computer somewhere half way around the world might exceed the harm that could be perpetrated by Mother Nature," said Rep. Adam Putnam (R-Fla.), the House subcommittee's chairman. "I have learned that today's SCADA systems have been designed with little or no attention to computer security."

It looks like DHS is on the case, after all. DHS recently issued a contract to Starthis, Arlington Hts., Ill., for research and development into improving SCADA security. Starthis will put Java 2 Enterprise Edition (J2EE) security features into its iTapestry software, used to link industrial control systems to enterprise software.

According to David Naylor, CEO of Starthis, the user authentication and authorization of J2EE enforces access restrictions. "These security enhancements are also applicable to regulated manufacturing environments, such as food and pharmaceuticals, where only appropriately trained and authorized individuals should be able to monitor or influence production systems," says Naylor.

If GAO and DHS have their way, it may be that process companies will be required to employ trained and licensed operators and control engineers. What a novel idea.