

## "Data storm" blamed for nuclear-plant shutdown

Robert Lemos, SecurityFocus 2007-05-18

The U.S. House of Representative's Committee on Homeland Security called this week for the Nuclear Regulatory Commission (NRC) to further investigate the cause of excessive network traffic that shut down an Alabama nuclear plant.

During [the incident](#), which happened last August at Unit 3 of the Browns Ferry nuclear power plant, operators manually shut down the reactor after two water recirculation pumps failed. The recirculation pumps control the flow of water through the reactor, and thus the power output of boiling-water reactors (BWRs) like Browns Ferry Unit 3. An investigation into the failure found that the controllers for the pumps locked up following a spike in data traffic -- referred to as a "data storm" in the NRC notice -- on the power plant's internal control system network. The deluge of data was apparently caused by a separate malfunctioning control device, known as a programmable logic controller (PLC).

In a letter dated May 14 but released to the public on Friday, the Committee on Homeland Security and the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology asked the chairman of the U.S. Nuclear Regulatory Commission to continue to investigate the incident.

"Conversations between the Homeland Security Committee staff and the NRC representatives suggest that it is possible that this incident could have come from outside the plant," Committee Chairman Bennie G. Thompson (D-Miss.) and Subcommittee Chairman James R. Langevin (D-RI) [stated in the letter](#). "Unless and until the cause of the excessive network load can be explained, there is no way for either the licensee (power company) or the NRC to know that this was not an external distributed denial-of-service attack."

The August 2006 incident is the latest network threat to affect the nation's power utilities. In January 2003, the Slammer worm [disrupted systems of Ohio's Davis-Besse nuclear power plant](#), but did not pose a safety risk because the plant had been offline since the prior year. However, the incident did [prompt a notice](#) from the NRC warning all power plant operators to take such risks into account.

In August 2003, nearly 50 million homes in the northeastern U.S. and neighboring Canadian provinces suffered from a loss of power after early warning systems failed to work properly, allowing a local outage to cascade across several power grids. A number of factors contributed to the failure, including [a bug in a common energy management system](#) and the MSBlast, or Blaster, worm which quickly spread among systems running Microsoft Windows, eventually claiming [more than 25 million systems](#).

No digital contagion has been fingered in the latest incident, said Terry Johnson, spokesman for the [Tennessee Valley Authority](#), the public power company that runs the Browns Ferry power plant.

"The integrated control system (ICS) network is not connected to the network outside the plant, but it is connected to a very large number of controllers and devices in the plant," Johnson said. "You can end up with a lot of information, and it appears to be more than it could handle."

The device responsible for flooding the network with data appears to be a programmable logic controller (PLC) connected to the plant's Ethernet network, according to an NRC information notice on the incident ([PDF](#)). The PLC controlled Unit 3's condensate demineralizer -- essentially a water softener for nuclear plants. The flood of data spewed out by the malfunctioning controller caused the variable frequency drive (VFD) controllers for the recirculation pumps to hang.

Such failures are common among PLC and supervisory control and data acquisition (SCADA) systems, because the manufacturers do not test the devices' handling of bad data, said Dale Peterson, CEO of industrial system security firm DigitalBond.

"What is happening in this marketplace is that vendors will build their own (network) stacks to make it cheaper," Peterson said. "And it works, but when (the device) gets anything that it didn't expect, it will gag."

In many cases, a simple vulnerability scan will even cause the devices to crash, Peterson said. During tests in an electrical substation, Nessus running in safe scan mode crashed devices, he said. In some cases, sending out broadcast data on the network will crash several of connected devices, he added.

"If you were to test any control systems that have any more than three or four (different) network-connected devices, they could be knocked over very easily," Peterson said.

The Browns Ferry nuclear power plant has had its share of difficulties. All three units of the plant were shutdown in 1985 due to performance and management problems, according to the NRC. Unit 2 was restarted in 1991, and Unit 3 started operating again in 1995. On Tuesday, the NRC gave the Tennessee Valley Authority [permission to restart Unit 1](#).

The Committee on Homeland Security gave the NRC until June 14 to respond to its letter.

[Privacy Statement](#)

Copyright 2006, SecurityFocus