Camera Triggers Plant Shutdown

SAFEGUARDING NUCLEAR CONTROLS

BY DARRELL DELAMAIDE

IF YOU THINK THEY'RE KIDDING when they tell airplane passengers to turn off cell phones and other electronic equipment for takeoffs and landings, think again. Radio frequency energy from a digital camera maintenance workers were using to photograph the control panel shut down Indian Point No. 2 in Westchester County, N.Y. last March.

Entergy, the operator of the plant, reported the incident to the Nuclear Regulatory Commission. In June, following local press reports, NRC confirmed that radio frequencies from a camera that was too close to a control panel somehow affected a boiler feed pump that provides water to four steam generators. The malfunction led to a drop in water levels that forced the company to shut down the plant two days ahead of a scheduled refueling.

No radiation was released. Entergy has since banned all digital cameras, cell phones, BlackBerries and other types of electronic equipment from control rooms in its plants and NRC promised to notify the 103 other nuclear power plants in the country about the incident.

NRC was quick to add that no remote signals could have had the same effect. "Somebody driving down the road with a radio transmitter is not going to be able to cause the same thing," says Neil Sheehan, an NRC spokesman. The thickness of the walls is designed among other things to shield the facility from this kind of interference.

In this case, it was the proximity of the camera, inside the walls, that was decisive. Nonetheless, the unexpected fragility of these mammoth power plants is likely to add to concern about their vulnerability.

Andrew Spano, Westchester County executive, told local television news reporters he wanted the NRC to investigate. "We get assurances all the time that it's absolutely safe, etcetera, and then something like this pops up," he said in an interview with WABC-TV. "I mean, this is a camera."

A digital camera was the culprit in an earlier incident at the Haddam Neck nuclear plant in Connecticut in 1997, only this time it was the camera flash that was blamed for releasing Halon gas as photos were being taken of the fire detection system panel for a training manual.

The NRC's information notice captured some of the drama in this incident after two camera flashes: "Within 3 to 5 seconds of the second flash, Halon discharged from the overhead nozzles…. It was characterized by a loud roar, fog, and significant air turbulence. The discharge scattered loose papers around the control room and dislodged several ceiling tiles, support frame pieces, and lighting fixture plexiglass covers." The control room was quickly evacuated but re-manned within an hour.

What is worrying about these incidents, critics say, is that operators of the plants seem to be unaware that these things can happen. An engineer's report from Entergy to the NRC regarding the Indian Point incident said the control room staff was "not aware that just having a digital camera turned on in close proximity to other digital equipment could cause a problem."

Ignorance was also a factor in an unplanned shutdown at the Hatch nuclear power plant in Georgia in March after a software update was installed on a single computer. This time, the Southern Company technician installing the update on the plant's business computer was aware that the computer was linked to one of the facility's primary control systems. But he was not aware that that the software was designed to synchronize data between both networks, so that a reboot in the business system computer would force a similar reset in the control system computer.

When he rebooted the updated computer, it reset the data on the control system, causing safety systems to mistakenly interpret the lack of data as a drop in water reservoirs that cool the radioactive nuclear fuel rods. So the plant's automated safety systems triggered a shutdown.

Valmont Newmark offers a winning hand full of products to fit your specific needs.

Valmont Newmark knows your power delivery structure needs may not be as easy as specifying one type of pole for the entire project. Terrain, environment and soil conditions are all factors when determining the structure that best fits the need. As the nation's premier provider of spun concrete, tubular steel and hybrid poles, we provide single-source access to a diverse product portfolio. Now you can easily customize line segments with site-specific poles, enhancing economics and total line integrity. Valmont Newmark will help you choose the most efficient structures to deliver power to your customers.

Our 14 locations (including our two newest PennSummit locations) throughout the United States and in Mexico, help facilitate a timely delivery.

valmont NEWMARK

Utility Division, Valmont Industries, Inc.
Two Perimeter Park South, Suite 475 West
Birmingham, Alabama 35243
800-533-5103 • Fax: 205-968-7201
www.valmont-newmark.com

Valmont Newmark—Your one source for steel, concrete, hybrid, transmission, distribution, and substation power delivery structures.

Plant engineers subsequently removed all physical connections between the two systems, but cyber experts noted that this type of problem can occur when corporate computer systems are connected to sensitive control systems that were never designed with security in mind.

Although these incidents were relatively harmless, the idea that nuclear plants are so vulnerable to such unintended consequences – which could someday include a catastrophic release of radiation – won't reassure a jittery public that still hasn't gotten over the 1979 meltdown at Three Mile Island.

NRC's communications policies are hardly reassuring. NRC's event notification report for the March 24 Indian Point incident doesn't mention the role of the digital camera at all, only a loss of speed in the feed pump. Entergy's incident report also neglected to mention the digital camera. It's like the old joke of saying someone died of heart failure due to a bullet through the heart. It was only when the local press got wind of the incident in June that NRC promised an information notice.

Still, as NRC's Sheehan notes, the plants themselves performed as required by automatically shutting down. "That's what they're designed to do if there is any sort of anomaly involving any security feature," he says.

TECHNOLOGY FRONTIER

Gatherings »

www.energycentral.com/events

To view any of these events, please go to www.energycentral.com/quicklink and type the quick link code (QL:) into the quick link box.

OCTOBER

1-2	World Energy Engineering Congress Washington	QL:	E17886
1-4	Eolica Expo 2008 Rome	QL:	E17241
13-14	Utility Tech Congress Dubai, UAE	QL:	E18261
15-18	Knowledge 2008 Utility CIO Summit Napa, Calif.	QL:	E18277
21-23	AMRChina Dalian, China	QL:	E18525
26-29	SAP for Utilities San Antonio	QL:	E17784
27-29	T&D World University Dallas	QL:	E17839

NOVEMBER

3-6	Southeastern Electricity Metering Association Clearwater Beach, Fla.	QL:	E18028
19-21	RENEXPO® South-East Europe Bucharest, Romania	QL:	E18611
26-28	Hydropower Plants Vienna, Austria	QL:	E17976

Dealing with Cyber Threats

ENERGY COMPANIES STEP UP PREPARATION

BY PAUL KORZENIOWSKI

THE ATTACKS ON 9/11 ILLUSTRATED how terrorists' minds work. Their approach was not simply to kill as many individuals as possible; it was to cause as much disruption to the U.S. way of life as possible. In the days after the attack, airlines were closed, companies closed up shop, and the aftereffects were seen in the stock market for many months. In examining what they could attack to cause similar damage, the nation's energy grid emerges as a possible target, one with many potential entry points.

In the aftermath of 9/11, the government as well as energy providers took stock of the possible damage and have been trying to close up possible holes. "A lot of work has been done to secure the energy grid but more is needed," said Joseph Bucciero, senior vice president of KEMA, an international energy consulting company.

The limitations of the efforts stem as much from the breadth of the challenges found with cyber security as from the industry's response itself. A terrorist only needs to find one security hole in a complex network while energy companies have to seal all possible entry points.

The nature of the energy business complicates the security task. "Unlike most companies, energy corporations run two separate networks: one that controls the flow of energy and a second that supports their administrative functions," said Chuck Newton, president of Newton-Evans market research firm.

The more vulnerable area may be with the former, and part of the reason is recent technical advances. In the old days, power companies had technicians go from manhole to manhole to determine which part of their grid had problems. Now, they have automated systems that monitor and control the flow of energy from place to place. Lately, they have been expanding the reach of these systems. Power providers have been reaching into businesses and consumers' homes, so they have more knowledge about demand.

While these changes enable energy companies to streamline their operations, they create new security challenges. In most cases, supervisory