



# ASIS COUNCILS



## Utilities Security Council “The Current” December 2011

### Just a few things from the Chairman

#### Utilities Security Council Leadership

##### Chairman

Allan Wick, CPP, PSP, PCI

##### 1<sup>st</sup> Vice-Chairman

Luis Morales, CPP

##### 1<sup>st</sup> Vice-Chairman

Doug Powell, CPP, PSP

#### COMMITTEES (Chairmen)

##### Membership & Newsletter

###### Editor

Bob Hulshouser, CPP

##### Annual Seminar & Session

###### Reviewers

Jeff Campbell, CPP

##### Council Administrative

Doug Powell, CPP, PSP

##### Subject Matter Experts

Chris McColm, CPP

##### Guidelines & Standards

Jeff Campbell, CPP

Wow, what an exciting year! As December 31<sup>st</sup> rapidly rushes towards us, it's time to take stock of what we accomplished this year and to plan how we wish to raise the bar in 2012.

Some of this year's achievements:

- 83% of the Council members hold at least 1 certification
- 25% of our members are “Young Professionals”
- This newsletter was initiated & it has been published monthly
- The Council sponsored 3 seminar sessions, had 5 speakers & 5 moderators
- Our Latin Americas Security Subcommittee was created with 10 members
- Our European Security Subcommittee was expanded by 4 members
- We had one “Security Management” article and one book review
- ASIS approved our first two-day conference in years to be held in 2012

Planned activities for 2012:

- 90% of the Council members hold at least 1 certification
- Continue to publish this newsletter monthly
- Sponsor 5 seminar sessions, 7 speakers & 7 moderators
- Expand the Latin Americas Security Subcommittee to 20 members
- Expand the European Security Subcommittee by 5 members
- Publish 10 White Papers
- Conduct 4 webinars from the published White Papers
- Conduct well attended, successful two-day conference in June
- Offer a one day pre-seminar track at the annual seminar

I am so thankful to be able to work shoulder-to-shoulder with such a talented group of professionals and I will look forward to continuing to serve ASIS International, our Council and the sector members we represent.

I hope everyone has the June 4-5, 2012 Utilities Security Conference on their calendar and in their budgets!

Wishing each of you and your families a safe and joyous holiday season!

*Allan Wick, CFE, CPP, PSP, PCI*

### SCADA vulnerability imperils critical infrastructure, feds warn.

December 14, *The Register* – (International) An electronic device used to control machinery in water plants and other industrial facilities contains serious weaknesses that allow attackers to take it over remotely, the U.S. Industrial Control Systems Cyber Emergency Response Team warned.

Some models of the Modicon Quantum PLC used in industrial control systems contain multiple hidden accounts that use predetermined passwords to grant remote access, the agency said in an advisory issued December 14. Palatine, Illinois-based Schneider Electric, the maker of the device, produced fixes for some of the weaknesses, and continues to develop additional mitigations. The programmable logic controllers reside at the lowest levels of an industrial plant, where computerized sensors meet the valves, turbines, or other machinery being controlled.



# ASIS COUNCILS



## Utilities Security Council

The default passwords are hard-coded into Ethernet cards the systems use to funnel commands into the devices, and gets temperatures and other data out of them. The Ethernet modules also allow administrators to remotely log into the machinery using protocols such as telnet, FTP, and the Windriver Debug port.

According to a blog post published December 12 by an independent security researcher, the NOE 100 and NOE 771 modules contain at least 14 hard-coded passwords, some of which are published in support manuals. Even in cases where the passcodes are obscured using cryptographic hashes, they are easy to recover thanks to documented weaknesses in the underlying VxWorks operating system. As a result, attackers can exploit the weakness to log into devices and gain privilege access to their controls.

Source: [http://www.theregister.co.uk/2011/12/14/scada\\_bugs\\_threaten\\_critical\\_infrastructure/](http://www.theregister.co.uk/2011/12/14/scada_bugs_threaten_critical_infrastructure/)

### **Senators Call on Senate Energy and Natural Resources Committee to Launch Oversight Hearing to Review U.S. Grid Reliability Standards after Recent Outages Affect Millions**

A bipartisan group of U.S. senators from New England sent a letter Tuesday asking the Senate Energy and Natural Resources Committee to launch an oversight hearing to review the nation's electric grid reliability standards after a series of major power outages affected millions of New England customers in recent years.

In August, Hurricane Irene cut power to millions of customers on the U.S. East Coast and an October snowstorm in New England cut power to more than two million utility customers. In both cases, outages lasted as long as week for some customers.

The senators' letter calls particular attention to the inadequacy of utility mutual assistance groups (MAGs), which exist to support utilities in contracting for additional line and repair crews as needed to restore power after a major outage. The senators claim that the inadequacy of the MAG system contributed to the slow pace of restoration in the hardest-hit states during recent outage events and raised concerns that the system may prove deficient in the face of future disasters.

Source: [http://www.renewgridmag.com/e107\\_plugins/content/content.php?content.7723](http://www.renewgridmag.com/e107_plugins/content/content.php?content.7723)

<http://blumenthal.senate.gov/newsroom/press/release/shaheen-blumenthal-lead-call-for-review-of-electric-gridreliability->

### **Electrical grid needs cybersecurity oversight**

In a recently released report, researchers from the Massachusetts Institute of Technology say that a single federal agency should be tasked with protecting the United States' electrical grid from cyberattacks; the Obama administration has proposed that DHS assume responsibility for the grid, while Congress has submitted proposals for both the Department of Energy and the Federal Energy Regulatory Commission (FERC).

To read more: <http://www.homelandsecuritynewswire.com/dr20111214-electrical-grid-needs-cybersecurity-oversight-study>

### **Oil Pipeline**

*Thanks to Michael Nagina for providing this article.*

OTTAWA - A group of Manitoba chiefs may block existing oil pipelines to protest problems in First Nations communities like Attawapiskat. At a special assembly in Ottawa this week, Terry Nelson, the former chief for the Roseau River First Nation in Manitoba, said there were plans to launch actions against oil pipelines in Manitoba, Saskatchewan and Alberta, along the U.S. border. Manitoba chiefs also submitted a resolution calling on the Assembly of First Nations (AFN) to back the action.

The ongoing housing crisis at Attawapiskat First Nation, located along the coast of James Bay, seems to have sparked debate about chronic problems in First Nations communities like education, health care, housing and environmental concerns. Chiefs at the Ottawa assembly meeting called on the AFN to request the United Nations appoint a special agent to monitor the government's response to Attawapiskat. Source: <http://www.winnipegssun.com/2011/12/08/manitoba-chiefs-plan-to-block-pipelines-in-protest>

### **Greenpeace Tactic**

*Thanks to Doug Powell for providing this article.*

Greenpeace activists diverted oil executives from a meeting on drilling prospects off Greenland and gave them a 20-minute environmental presentation, according to a Greenpeace story on their website. Oil companies including Shell, BP and Chevron were invited to a meeting by the Greenlandic Bureau of Minerals and Petroleum in Copenhagen to discuss prospecting oil in the waters off Danish territory.



# ASIS COUNCILS



## Utilities Security Council

Around 20 Greenpeace activists in suits and ties greeted some of the oil executives in the building lobby and, while pretending to be their hosts, led them to a different floor of the building which Greenpeace had rented under an assumed company name.

Once the oil company executives were seated in Greenpeace's rented room, the activists presented a 20-minute film on the environmental risks associated with drilling for oil off Greenland, according to Greenpeace Arctic specialist Jon Burgwald.

The Greenlandic Bureau of Minerals and Petroleum confirmed that "some of the people invited were detoured to another floor." Greenpeace has undertaken other actions to stop oil exploration off Greenland. In June two Greenpeace activists climbed a Cairn Energy rig in an effort to stop drilling, there. The Vancouver Province:

<http://www2.canada.com/theprovince/news/story.html?id=bac9e000-2f65-41d7-a873-23cfa3f27e96> (Friday, December 02, 2011)

### Water Pump Hack Mystery Solved

It was the broken water pump heard 'round the world.

Cyberwar watchers took notice this month when a leaked intelligence memo claimed Russian hackers had remotely destroyed a water pump at an Illinois utility. The report spawned dozens of sensational stories characterizing it as the first-ever reported destruction of U.S. infrastructure by a hacker. Some described it as America's very own Stuxnet attack.

Except, it turns out, it wasn't. Within a week of the report's release, DHS bluntly contradicted the memo, saying that it could find no evidence that a hack occurred. In truth, the water pump simply burned out, as pumps are wont to do, and a government-funded intelligence center incorrectly linked the failure to an internet connection from a Russian IP address months earlier.

Now, in an exclusive interview with Threat Level, the contractor behind that Russian IP address says a single phone call could have prevented the string of errors that led to the dramatic false alarm. "I could have straightened it up with just one phone call, and this would all have been defused," said Jim Mimitz, founder and owner of Navionics Research, who helped set up the utility's control system. "They assumed Mimitz would never ever have been in Russia. They shouldn't have assumed that."

Mimitz's small integrator company helped set up the Supervisory Control and Data Acquisition system (SCADA) used by the Curran Gardner Public Water District outside of Springfield, Illinois, and provided occasional support to the district. His company specializes in SCADA systems, which are used to control and monitor infrastructure and manufacturing equipment. Mimitz says last June, he and his family were on vacation in Russia when someone from Curran Gardner called his cell phone seeking advice on a matter and asked Mimitz to remotely examine some data-history charts stored on the SCADA computer. Mimitz, who didn't mention to Curran Gardner that he was on vacation in Russia, used his credentials to remotely log in to the system and check the data. He also logged in during a layover in Germany, using his mobile phone. "I wasn't manipulating the system or making any changes or turning anything on or off," Mimitz told Threat Level.

But five months later, when a water pump failed, that Russian IP address became the lead character in a 21<sup>st</sup> century version of a Red Scare movie. On Nov. 8, a water district employee investigating the pump failure called in a contract computer repairman to check it out. The repairman examined the logs on the SCADA system and saw the Russian IP address connecting to the system in June. Mimitz's username appeared in the logs next to the IP address. The water district passed the information to the Environmental Protection Agency, which governs rural water systems. "Why we did that, I think it was just out of an abundance of caution," says Don Craven, a water district trustee. "If we had a problem we would have to report it to EPA eventually."

But from there, the information made its way to the Illinois Statewide Terrorism and Intelligence Center, a so-called fusion center composed of Illinois State Police and representatives from the FBI, DHS and other government agencies. Even though Mimitz's username was connected to the Russian IP address in the SCADA log, no one from the fusion center bothered to call him to ask if he had logged in to the system from Russia. Instead, the center released a report on Nov. 10 titled "Public Water District Cyber Intrusion" that connected the broken water pump to the Russian log-in five months earlier, inexplicably stating that the intruder from Russia had turned the SCADA system on and off, causing the pump to burn out. "And at that point ... all hell broke loose," Craven said.

Whoever wrote the fusion center report assumed that someone had hacked Mimitz's computer and stolen his credentials in order to use them to hack into Curran Gardner's SCADA system and sabotage the water pump. It's not clear whether it was the computer repairman or the fusion center that first jumped to this conclusion. A spokeswoman for the Illinois State Police, which is responsible for the fusion center, pointed the finger at local representatives of DHS, FBI and other agencies who are responsible for compiling information that gets released by the fusion center. "We did not create the report," said spokeswoman Monique Bond. "The report is



# ASIS COUNCILS



## Utilities Security Council

created by a number of agencies, including the Department of Homeland Security, and we basically are just the facilitator of the report. It doesn't originate from the [fusion center] but is distributed by the [fusion center]."

But DHS is pointing the finger back at the fusion center, saying if the report had been DHS-approved, six different offices would have had to sign off on it. "Because this was an Illinois [fusion center] product, it did not undergo such a review," a DHS official said. The report was released on a mailing list that goes to emergency management personnel and others, and found its way to Joe Weiss, managing partner of Applied Control Solutions, who wrote a blog post about it and provided information from the document to reporters.

The subsequent media blitz identified the intrusion as the first real hack attack against a SCADA system in the U.S., something that Weiss and others in the security industry have been predicting would happen for years. The hack was news to Mimplitz. He put two and two together, after glancing through his phone records, and realized the Russian "hacker" the stories were referring to was him. Teams from the FBI and DHS's Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT) subsequently arrived in Illinois to investigate the intrusion and quickly determined, after speaking with Mimplitz and examining the logs that the fusion center report was wrong and should never have been released. "I worked real close with the FBI and was on speakerphone with the fly-in team from CERT, and all of them were a really sharp bunch and very professional," Mimplitz said.

DHS investigators also quickly determined that the failed pump was not the result of a hack attack at all. "The system has a lot of logging capability," Mimplitz said. "It logs everything. All of the logs showed that the pump failed for some electrical-mechanical reason. But it did not have anything to do with the SCADA system." Mimplitz said there was also nothing in the logs to indicate that the SCADA system had been turned on and off.

He cleared up another mystery in the fusion report as well. The report indicated that for two to three months prior to the pump failure, operators at Curran Gardner had noticed "glitches" in their remote access system, suggesting the glitches were related to the suspected cyber intrusion. But Mimplitz said the remote access system was old and had been experiencing problems ever since it was modified by another contractor. "They had made some modifications about a year ago that was creating problems logging in," he said. "It was an old computer ... and they had made network modifications that I don't think were done correctly. I think that's why they were seeing problems."

Joe Weiss says he's shocked that a report like this was put out without any of the information in it being investigated and corroborated first. "If you can't trust the information coming from a fusion center, what is the purpose of having the fusion center sending anything out? That's common sense," he said. "When you read what's in that [report] that is a really, really scary letter. How could DHS not have put something out saying they got this [information but] it's preliminary?"

Asked if the fusion center is investigating how information that was uncorroborated and was based on false assumptions got into a distributed report, spokeswoman Bond said an investigation of that sort is the responsibility of DHS and the other agencies who compiled the report. The center's focus, she said, was on how Weiss received a copy of the report that he should never have received. "We're very concerned about the leak of controlled information," Bond said. "Our internal review is looking at how did this information get passed along, confidential or controlled information, get disseminated and put into the hands of users that are not approved to receive that information. That's number one." Source: <http://www.wired.com/threatlevel/2011/11/water-pump-hack-mystery-solved/>

### Security 'Chaos' Leaves Utility Grids Vulnerable, Report Says

*Government Computer News (11/15/11) Jackson, William*

A recent paper from Pike Research reveals that the lack of standards, inadequate spending and an aging infrastructure are making vital utility grids increasingly vulnerable to cyber attack. Though the report says that this vulnerability is a global problem, it also notes that there are multitudes of differing region infrastructures and security technologies, requiring region-specific definitions of threats as well as region-specific decisions regarding investments in security. Annual spending for this type of security is expected to climb to near \$750 billion by 2018 in North America alone. Spending is currently constricted by a lack of enforceable standards for security, though numerous guidelines exist. There are five trends in grid cyber security that the reports notes are promising: multi-factor authentication, application whitelisting, data encryption, control network isolation and security event logging and correlation.

Source: [Web Link](#)

### Congratulations Allan Wick

The FBI Denver Division is proud to announce Mr. Allan Wick, as the recipient of the Director's Community Leadership Award, for 2011. "The outstanding contributions demonstrated by Mr. Wick for service to his community are astounding. As a leader in Colorado's security industry, he demonstrates a strong and sustained commitment to building safer communities through crime prevention and



# ASIS COUNCILS



## Utilities Security Council

critical infrastructure protection. His outreach and leadership in Colorado and beyond is promoting lasting relationships with government, private sector businesses, academic institutions, state and local law enforcement, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. Mr. Wick has achieved extraordinary results within the programs he initiated and built for the future. His influence in the FBI InfraGard Program has developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters.”

InfraGard brings together representatives from the private and public sectors to help protect our nation’s critical infrastructure—both virtual and physical—from attacks by terrorists and criminals.

Article in the Denver Post: <http://blogs.denverpost.com/crime/2011/11/16/fbi-awards-security-expert-for-community-service/2732/>

### Illinois Water SCADA Reporting Shows Need for Analytical Competence

Sean McBride

*Guest author Sean McBride is the Director of Analysis and Co-founder of Critical Intelligence, a company that provides Cyber Situational Awareness and Threat Intelligence services for Industrial Control System Owner/Operators, Vendors and Government stakeholders.*

A pair of investigations, one by the Department of Homeland Security [1], and one by reporters from Wired [2], provided a conclusion to the Curran-Gardner Water District (Illinois) hacking incident. In short, the suspected intrusion from a Russian IP address was legitimate traffic from a SCADA engineer on travel in that country. The log-in did not seem to be related to the failure of a pump under the system’s control.

The story originally broke on November 17, when Joe Weiss, an outspoken ICS security professional, noted having received a report from a government body that described a compromised water SCADA system. Over the following weeks numerous news outlets, including the BBC [3] covered the incident – which is now known to be a false alarm.

Several facets of the incident, its reporting and coverage, show the importance of developing sound analytical competence. First, and most obviously, the report, which came from the Illinois Statewide Terrorism and Intelligence Center, was unverified analysis. As a consumer of information, one must accept that when you receive analysis from a third party there may be errors and omissions, lack of expertise, logical fallacies, false assumption, and biases. The old adage still applies: “You can’t believe everything you read in the paper.” Of course, this challenge of discerning truth and error is compounded when information is provided by an “official” government source – which was the case here. Close examination of the Illinois report however, shows several reasons to call it into question:

The report was released on November 10, 2011 and provides extensive details of an event that reportedly occurred on November 8, 2011. That timeline seems unreasonable.

The report claimed that the intrusion “is the same method of attack recently used against the Massachusetts Institute of Technology (MIT) server” because “The water district’s attack and the MIT attack both had references to ‘phpMyAdmin’ in the log files of the computer systems.” This is inaccurate, showing a fundamental misunderstanding and lack of research. The compromised MIT server attacked other systems that exhibited the phpMyAdmin vulnerability– it was not the means of its own compromise. Moreover, it does not seem likely that the SCADA system would be running phpMyAdmin (though not impossible).

The report also states “It is believed the hackers had acquired unauthorized access to the software company’s database and retrieved the usernames and passwords of various SCADA systems, including the water district’s system.” This seems to conflict with the idea that the compromise occurred via phpMyAdmin. One possible way to sync the two named attack vectors is that the SCADA vendor was running phpMyAdmin and the SCADA vendor’s networks were compromised by that vulnerability – but that would probably have required analysis of the SCADA vendor’s logs in addition to the Curran-Gardner logs, and the report itself implies that the vendor’s logs have not been reviewed: “It is unknown at this time the number of SCADA usernames and passwords acquired from the software company’s database and if any additional SCADA systems have been attacked as a result of this theft.” Second, DHS’s (INL/Battelle) handling of the situation represents a continual squandering of taxpayer resources.

“Rules” for government engagement in the private sector seem to have been disregarded. It is my understanding that ICS-CERT or any other federal agency providing a public-private service can only intervene upon the request of an affected entity. In the Curran-Gardner case, ICS-CERT actively sought to contact the reportedly affected entity: “ICS-CERT would like to thank the Curran-Gardner Public Water District and the SCADA systems integrator (vendor) for their cooperativeness in pulling all available resources in order to conduct a thorough and exhaustive investigation” [1]. While this may seem like the right thing to do, it is, at a minimum, inconsistent with

previous statements that incident response requires “voluntary” participation with the government. Imagine that the DHS and FBI come calling, “We heard you had a problem...we are here to investigate. You need our help. Can we help?” This is hardly voluntary. Read more @: <http://www.digitalbond.com/2011/12/12/illinois-water-scada-reporting-shows-need-for-analytical-competence/>

### Other News

Thanks to Angeline Berryman for assisting in compiling our news items for this month’s report, and in properly formatting the final product. Angeline is a business major at the College of Southern Nevada.

### Your Editor’s Request

Please send topics of interest, announcements, work activities, professional development, chapter involvement, related business and government associations, et al, to me. With your participation in “The Current” we can develop a wonderful communications tool for the USC and ASIS International. Thanks.

Bob Hulshouser, CPP

A Monthly Newsletter of the ASIS International Utilities Security Council (USC)

(Editor’s Note: This newsletter is published for the use of USC members and other interested ASIS International security councils, working groups, leaders, members and staff. It is not an official publication of ASIS International. As such, the information and articles contained in this, and subsequent editions of “The Current”, should be considered as unofficial and for member interest and use as appropriate)



1625 Prince Street  
Alexandria, VA 22314-2818  
USA  
703-518-1447  
Fax: 703-518-1517  
Email: [councils@asisonline.org](mailto:councils@asisonline.org)