Strengthening Cyber Security

CENTER ADVISES UTILITIES

BY ALAN PALLER

REMOTE ATTACKS ON SYSTEMS THAT control power production and distribution are no longer hypothetical events. At least four utilities have been subjected to extortion demands by criminals who used the Internet to infect the utilities' computers and caused or threatened power outages. Cyber attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities. These are criminal acts, but nation-states are actively targeting utility computers, as well, so that in time of war they can turn off their adversary's power.

While all this is happening, most executives in the power industry are in a state of denial. They are not informed by their security staffs that these attacks are happening or that they are vulnerable to such attacks. As a result, they discount the problem and overstate their security readiness. At least one industry leader did just that, lying, under oath, to a Congressional subcommittee looking into the problem, and got caught.

In recent months, some utility industry executives have begun discovering just how bad the problem actually is. The head of MI-5, the Security Service in the United Kingdom, personally invited the top executives of key power companies to a classified briefing on the current wave of attacks and what is likely to come next. Although the U.S. government has not been as forthcoming, preferring not to admit the failure of its programs to protect the critical infrastructure, a few U.S. executives are also learning about the problem through personal relationships with people who have access to the relevant data. Whenever top executives are awakened to the actual threat, they almost invariably ask three questions: What do we need to do? How much is enough? Whom can I trust to give me those answers?

NewsFlash

DOE FUNDING

www.energycentral.com

The Department of Energy is proposing to provide $43.1 million to fund geothermal research, development and demonstration projects over four years.

Steve Chalk, deputy assistant secretary for renewable energy, said the effort "will help us meet our aggressive departmental goal to prove the technical feasibility of enhanced geothermal systems by 2015."

The U.S. government has done a good job of providing answers to these three questions – good enough so they are being used by utilities in Europe and other countries around the world. The U.S. Department of Energy and the U.S. Department of Homeland Security have spent tens of millions of dollars on programs that identify the vulnerabilities in common control systems, determine how they can be exploited, and define the actions that the vendors and buyers of these control system can take to mitigate the risks. Best of all, they have put the answers in forms that utilities can put to work immediately and effectively.

One program is called the National SCADA Test Bed (NSTB), operated primarily by the Idaho National Laboratory outside Idaho Falls, and funded by DOE. NSTB's goal is to improve the resilience of control systems associated with energy sector critical infrastructure. It conducts detailed laboratory assessments of Supervisory Control and Data Acquisition/Energy Management System control systems, communications protocols, and third-party security products used in U.S. energy sector installations in order to understand vulnerabilities and develop recommended mitigation strategies for system vendors. The assessments are very deep; each of the 10 control system assessments employed more than 800 hours of cyber research effort. The control systems they studied are from vendors that supply more than 80 percent of the control systems used in the U.S. power industry. Idaho National Laboratory also conducted seven on-site assessments at electricity transmission, generation, and oil and natural gas facilities to better understand real-world

Subscribe Online to EnergyBiz

Autodesk: Leveraging Design to Improve Asset Information

Utility Industry Challenges

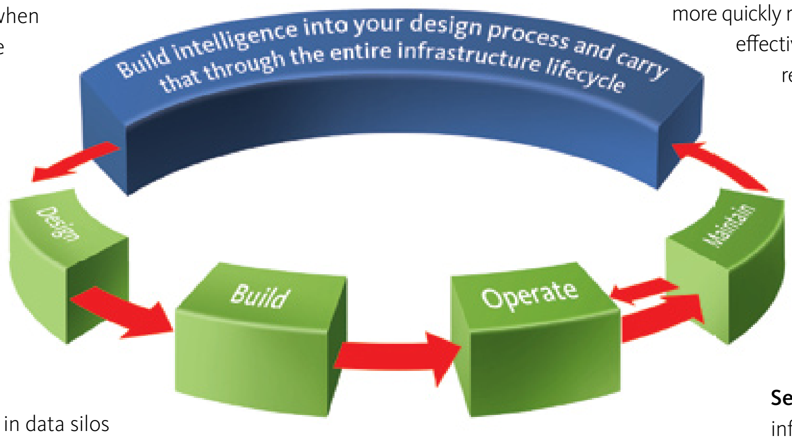
Utilities face relentless pressure to do more with less and maintain high reliability and customer service, all the while coping with aging assets, capital constraints, a rising demand for energy, and addressing sustainability.

Infrastructure: The North American Electric Reliability Corporation predicts that demand for electricity will increase 19 percent nationwide over the next 10 years while transmission capacity will grow by only 6 percent. In addition, surveys indicate that about half of all utility infrastructures in North America are more than 50 years old. This is an issue that is reoccuring across the world, and is estimated to cost $40 trillion over the next 25 years to refurbish infrastructure globally.

Efficiency: There is rising consumer interest and participation in energy efficiency measures and distributed energy resources, which adds to the complexity of grid design and optimization.

Knowledge Transfer: Utilities will have to cope with the retirement of experienced staff over the next decade—workers with valuable knowledge that will be difficult to replace.

However, even under such tough circumstances, utilities still can increase productivity and cost efficiencies by improving asset information. If asset information is accurate, timely, and available to all who need it when they need it, a utility can operate more effectively.


Build intelligence into your design process and carry that through the entire infrastructure lifecycle
Design
Build
Operate
Maintain

Asset Information Challenges

Unfortunately, for most utilities, it is not easy to access or share asset information across the design, build, operate and maintain infrastructure lifecycle. Often, the information resides in proprietary formats or in data silos throughout the organization. When design information is shared, it is often exchanged via paper format and is manually entered into an as-built system. Making design data available to those managing as-builts, responding to maintenance issues, or answering customer service requests usually requires either manually reconciling the data or converting it to the proprietary formats. Autodesk utility solutions improve business process and data quality by leveraging engineering design information across processes to build, operate and maintain asset lifecycle.

So, what if utilities could get accurate and consistent information quickly enough so they can maximize operational efficiencies, improve responsiveness, and increase quality of service?

The Autodesk Approach

By leveraging the Autodesk design tools utilities likely already have, they can build on that strong foundation. Autodesk solutions for utilities make it easy for all departments to integrate, access and share design and as-built information—in their business processes. This helps to eliminate waiting for reports or pieces of information from different departments and wondering how accurate and up-to-date the information is.

- Key data on every engineered asset – what they are, where they are, and how they are performing – is available instantly, without having to compile the information manually or convert it to another format.
- Every physical asset has a "single point of truth" associated with it.

With Autodesk solutions, utilities can extend the reach and value of infrastructure asset information, so they can more easily handle customer requests; more quickly respond to outages; and more effectively provide information for reporting, planning and analysis.

> "Autodesk solutions for utilities make it easy for all departments to integrate, access and share design and as-built information--in their business processes."

Autodesk utility solutions can improve efficiency and data quality by building intelligence into the design process and then leveraging that data across the entire asset lifecycle. With this, utilities:

See the big picture. Manage infrastructure safely and efficiently with greater access to information supporting decision analysis.

Do more with less. Turn out quality work quickly so they can:

- Build standardization into the engineering process
- Eliminate wasteful data re-creation processes
- Remove the silos and to create a single point of truth

Get the right information to the right people at the right time.

With Autodesk, utilities can leverage design to improve business process and data quality.

JOAN THARP, INGENUITY COMMUNICATIONS

autodesk.com/utilities

Autodesk is a registered trademark of Autodesk, Inc., in the USA and/or other countries. All other brand names, product names, or trademarks belong to their respective holders. Autodesk reserves the right to alter product offerings and specifications at any time without notice, and is not responsible for typographical or graphical errors that may appear in this document. © 2008 Autodesk, Inc. All rights reserved.

installations of the systems and provide mitigation strategies to vendors and asset owners. The team of cyber researchers, control systems engineers and network engineers at the lab is widely recognized as the world's most knowledgeable and effective center of excellence in cyber security of control systems.

The result of all these assessment programs is an unparalleled body of knowledge about vulnerabilities in control systems. To put that knowledge to work to protect the critical infrastructure, INL experts working at the Control Systems Security Analysis Center funded by DHS developed education courses that teach asset owners and operators how to secure these systems. They recently completed a very effective new program called the control system cyber red and blue team advanced training course giving students hands-on understanding of how the vulnerabilities are exploited, what attackers can do, and how users may be able to mitigate the risk.

Even more valuable than the training is the Idaho National Laboratory's innovative "Cyber Security Procurement Language for Control Systems document," available at www.msisac.org. Again with funding from DHS, the lab and New York State Office of Cyber Security worked together to translate the findings from assessment projects into very specific contract clauses that asset owners can employ to require the vendors of these systems to bake security into new control systems they are delivering.

We have a long way to go to even begin to protect our control systems effectively. Attacks are accelerating from both criminal organizations and malicious nation-states. But the work of Idaho National Laboratory, supported by the Department of Energy and the Department of Homeland Security, provides the outlines of a road map to real progress in reducing the risk.

Alan Paller is director of research at The SANS Institute, an organization involved in computer security issues.

The Green Circuits Project

FOCUSING ON TRANSMISSION AND DISTRIBUTION EFFICIENCY

BY ARSHAD MANSOOR

Arshad Mansoor

PHOTO COURTESY OF ELECTRIC POWER RESEARCH INSTITUTE

WE LIVE IN A WORLD WHERE THE demand for electricity continues to increase, not only as a result of normal load growth but also as a result of new loads like electric vehicles. It is becoming increasingly important to look beyond traditional generation for alternatives to meet supply needs including energy efficiency, demand management and renewable generation. As we look at opportunities for more efficient uses of energy, it is important to look at the entire supply chain. Transmission and distribution systems offer numerous opportunities for efficiency improvement.

While the industry is tasked by regulators to engage in end-use energy efficiency programs, few have considered options to reduce energy losses along the electricity delivery chain. In many cases, the efficiency gains that could be realized by reducing transmission-and-distribution losses or by improving plant operational efficiency can be in the same range as, or exceed, the potential of end-use efficiency savings.

The electric industry is currently spending approximately $2 billion per year in state and utility administered energy-efficiency programs in residential, commercial and industrial facilities. While there

Subscribe Online to EnergyBiz