Ensuring Cyber Security in Integrated Networks

The increasing complexity of intelligent, integrated networks means that safety and reliability are of paramount concern. By implementing cyber security measures at the management level, operators can ward off hacker attacks and secure the integrity of their networks.

By Rhea Wessel

For most people, the acronym CIA stands for a mysterious American governmental agency. For those in the cyber security business, however, it means something totally different: the Confidentiality, Integrity and Availability of data networks and computer systems.

These three cyber security principles are increasingly imperative for power plant operators and energy distributors as well. As networks coalesce into an IT-based smart grid, bad storms or fallen trees may become minor threats in comparison to potential attacks by data hackers.

In fact, one report says that the 2003 blackout in the USA, one of the worst in history, was partly due to a computer bug that stalled an energy provider's control-room alarm system. The blackout caused transport networks to fail; homes, businesses, and hospitals were without power for days; and public life was thrown into turmoil.

Experts are working to make sure this doesn't happen again, but they face sophisticated and growing challenges linked to the particular structure of energy provision networks.

Up to the 1980s, most power was provided by regional network operators using mainframe computing systems that were not linked to one another. Later, computer and power networks became increasingly intertwined, but computer networks continued to be operated using proprietary standards. Now, with open standards for computer networks in widespread use, power providers cannot run their power networks effectively without proper cyber security measures. They must ensure that viruses and worms cannot enter the system and impair their ability to control and oversee power plants and power networks.

"If control mechanisms were deactivated over the Internet, it would be like flying blind," says Konstantin Knorr, a professor of IT security at the Computer Science Department of the University of Applied Sciences in Trier, Germany. In addition, as the smart grid becomes reality, the business models of power companies are increasingly based on the security of the data – data that is needed for skillful management of production and consumption demands, which can change by the minute.

In fact, the entire operation and efficiency of the smart grid is based on data. It depends on noncompromised data provided by geographically dispersed energy producers and consumers with smart meters, each of whom might have an interest in manipulating data for their own advantage, as well as the ability to do so.

To meet this growing security challenge, governments and industry bodies in every region of the world have developed standards for the power industry. However, these standards vary

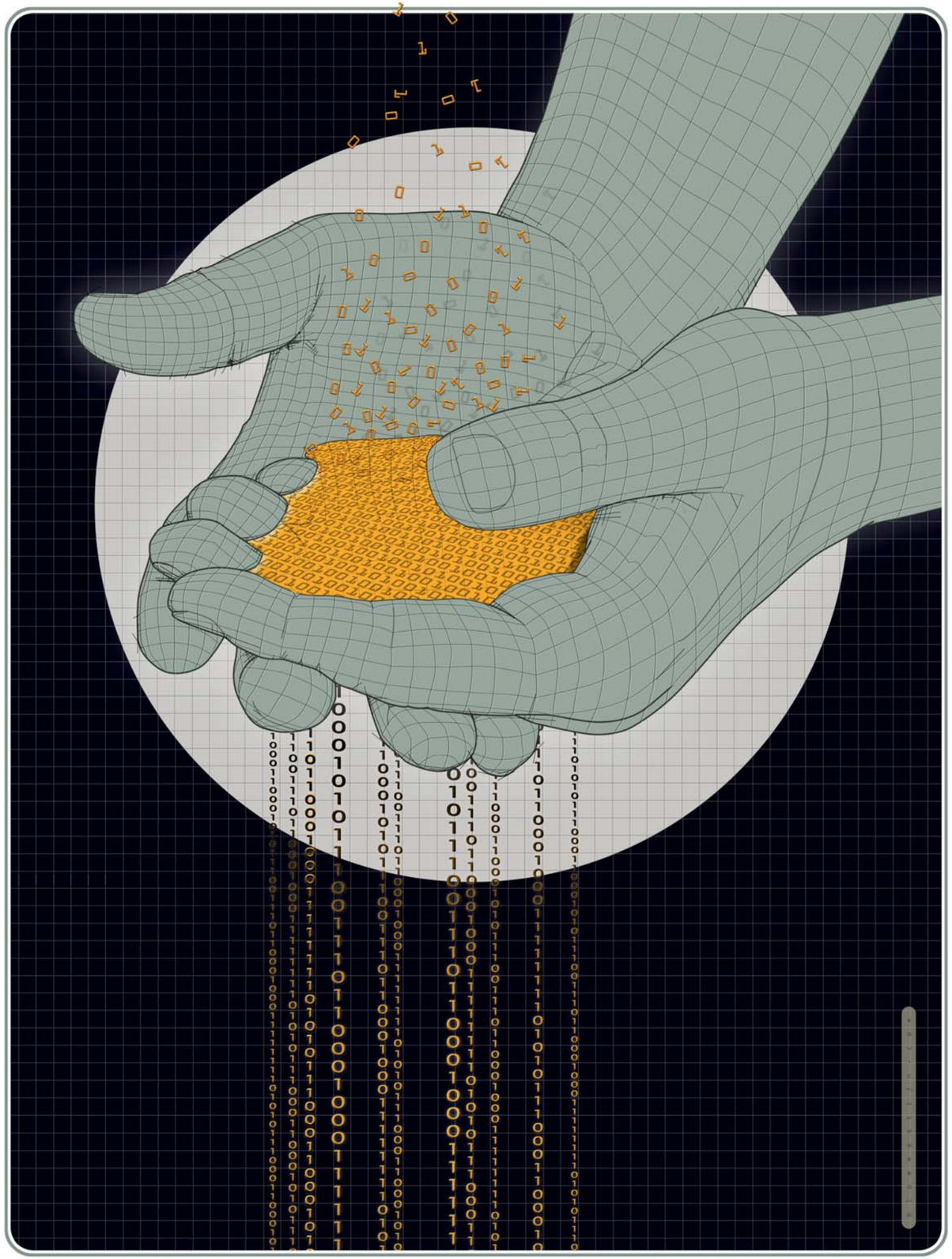


Illustration: Rhonald Blommestijn

> “If control mechanisms were deactivated over the Internet, it would be like flying blind.”
>
> Konstantin Knorr, professor of IT security, University of Applied Sciences in Trier, Germany

widely from continent to continent, and their application can be drastically different in each company.

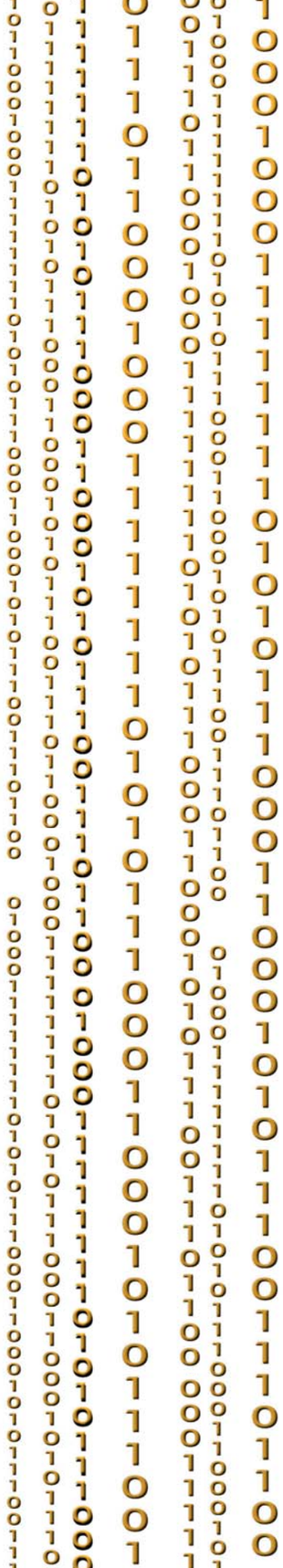
Developing a Cyber Security Policy

For instance, small power providers in Europe may have a single person in charge of data security, while larger ones have entire departments dealing with the matter. Meanwhile, the USA has implemented some of the world’s toughest requirements for cyber security in power networks in the aftermath of the September 11 attacks. The rules of the North American Electric Reliability Council (NERC) are legally binding and are designed to ensure the uninterrupted functioning of power assets, which are considered part of the critical infrastructure.
Still, even those power providers that have addressed the question of cyber security and have the latest technology may still be vulnerable, according to Knorr.
“In most power companies, the IT department is organizationally separated from the operations department and the administrative department. The operations guys are typically power engineers, the IT guys are computer experts, and those in the back office may work on marketing. These people often have different requirements of the computer network – one group is concerned about availability, while the other is worried about confidentiality,” says Knorr.

Such organizational hurdles are one reason why experts suggest that cyber security should be a matter for the highest levels of management at companies throughout the power generation and distribution supply chain. Another is the fact that each network is configured differently and has its own unique strong and weak points.

The Threat Analysis

Often, the first step toward developing and implementing an effective cyber security policy is to conduct a threat analysis that goes beyond what is provided by the power network supplier. This is critical, since divergences in IT network configurations and additions, such as patches, can affect a manufacturer’s original security design, says Thomas Brandstetter, the manager of the worldwide Hack-Proof Products Program at Siemens. Brandstetter and his team work to ensure that cost-efficient cyber security is built into each Siemens product.
To obtain a threat analysis, operators of power plants or power networks may choose to work with outside consultants or with the company that delivered the system, since the supplier will have the deepest understanding of the company’s equipment. The network is subjected to a threat analysis that is quite similar to the approach a hacker would take: First, consultants gather information about the network, they review it for potential vulnerabilities, and then they attempt



intrusions. Such an analysis may be executed as part of an acceptance test, or with due diligence even when a solution has already gone productive. With every network or plant delivered, Siemens outlines possible threat scenarios in system documentation and provides customers with templates that model safe networks, including specific recommendations about where to place firewalls or password-controlled interfaces. And customers can order targeted penetration tests as part of the acceptance process in order to confirm the cyber security of their systems.
In the USA, where security requirements are the strictest, Siemens also consults with its customers about making the best possible use of the security features it delivers with power plants, such as the SPPA-T3000 instrumentation and control system for power plants. It contains an integrated cyber security zone architecture, which creates zones, connects the zones, and ensures communication between those zones.

Cyber Security as an Ongoing Process

Once the threat analysis has been completed, the power plant operator or network provider identifies measures to be taken to reduce the risks, either alone or with the partner. These may be organizational changes, such as restructuring, employee training, or actual changes to network design or interfaces. Finally, to protect critical power infrastructure, IT networks must be managed continually and be subjected to routine maintenance and security checks.
For instance, remote connections must be monitored, the operation of security-relevant components of control systems should be verified, virus scans must be run, virus protection software should be updated daily, authorization protocols must be double-checked, and operators must have in place an emergency plan for running relevant control components.
However, during such maintenance, technicians must be particularly careful, Brandstetter cautions: “It’s critical that any changes to the system be tested intensively before implementation, to make sure they won’t have negative consequences for the control system and its availability.”
According to Brandstetter, ensuring the confidentiality, integrity, and availability of data networks in the face of cyber threats all comes down to one overarching principle: Maintaining cyber security must be seen as a continuous process, rather than a goal to be met at a particular finish line.

__Rhea Wessel__ is a freelance writer based in Frankfurt.

Cyber Security Precautions for Power Networks

The NERC standards for critical infrastructure protection include recommendations for cyber security in the following areas:

- Security Management Controls
- Personnel & Training
- Electronic Security Perimeter(s)
- Physical Security of Critical Cyber Assets
- Systems Security Management
- Incident Reporting and Response Planning
- Recovery Plans for Critical Cyber Assets

Further Information

www.siemens.com/energy

Biographies

In December 2009, **Konstantin Knorr** was appointed as a professor for IT security at the University of Applied Sciences in Trier, Germany. He focuses on the security of SCADA (supervisory control and data acquisition) systems, particularly those in energy generation and distribution. Previously, Knorr performed penetration testing, security monitoring services, and cyber security projects for the Siemens Computer Emergency Response Team (CERT).

Thomas Brandstetter leads the Hack-Proof Products Program at Siemens, which focuses on ways to integrate cost-efficient IT security into Siemens products. He is an expert on hacking prevention and security in energy infrastructure. Brandstetter has more than ten years of experience in practical IT security and has been working for the Siemens CERT since 2005.