by Patrick Le Fèvre

Is Your Smart Grid Secured?

As I have been involved with digital power since the early days of adding communications and intelligence to power supplies, I have frequently been asked about software security and if the power supply industry is prepared to address security issues. While there is very little chance that a hacker will reach a single digital point-of-load (POL) at the board level, the risk increases exponentially as we move upward in the value chain. In that chain, the smart grid is probably the highest and the most exposed to cyberattacks (Figure 1).

All over the world, governments, consortiums, and groups of experts are engaged in an amazing race to deploy security methods and protocols to make the smart grid safer.

As time passes, the number of renewable power sources is growing, the deployment of smart meters is rising, and many other communication links and automation circuits are being connected to the smart grid. So what is the situation in terms of security? Are we safe?

Risk Escalation

In 2007 in the Aurora Generator Test, the U.S. government demonstrated that, with only 21 lines of code, hackers could take control of a power plant and physically destroy a generator [1]–[3]. Since then, many cybersecurity breaches have taken place, such as the case in April 2016, when a water and electricity authority in Michigan became the victim of a ransomware attack and was forced to keep information technology (IT) systems locked down for a week. Examples such as these and many others indicate that the number of cyberattack cases reported to security authorities has been rapidly increasing [10]. Florida International University estimated that, during the first six months of 2015, more than 100 cyberincidents affected the infrastructure of the United States, and the energy sector had the largest number of attacks. Cyberattacks on the smart grid are a global threat and all countries are at risk, motivating power experts and networks managers to consider a global response and methodology to prevent any damages.

In February 2016, the U.S. Department of Homeland Security (DHS) issued an alert (IR-ALERT-H-16-056-01) that was based on a case that happened on December 2015 in the Ukraine [4]. It was a high-level alert to smart grid operators, motivating them to accelerate protection mechanisms and to develop preventive actions policies. The Ukrainian case combined multiple elements in the attack, including physical sabotage. In fact, the sophistication of the cyberattack reached a new level of intrusion, motivating the smart grid community to strengthen cooperation and efforts to accelerate sustainable security within the smart grid [5].

A Black Christmas for Ukrainians

On 23 December 2015 at 4:00 p.m. local time, the Ukraine region Ivano-Frankivsk was plunged into darkness for several hours and more than 220,000 customers lost power. In addition, the IT and communications systems of the electric companies were severely damaged by the attackers.

In this case, the attackers combined a large number of attacking tools: spreading phishing e-mails containing a variant of the BlackEnergy 3 and KillDisk malware programs and exploiting security holes in Microsoft Office documents to get into the IT network of the electric companies and inhibit the security agents in the firewalls (Figure 2). At the same time,

Digital Object Identifier 10.1109/MPEL.2016.2615780
Date of publication: 20 December 2016

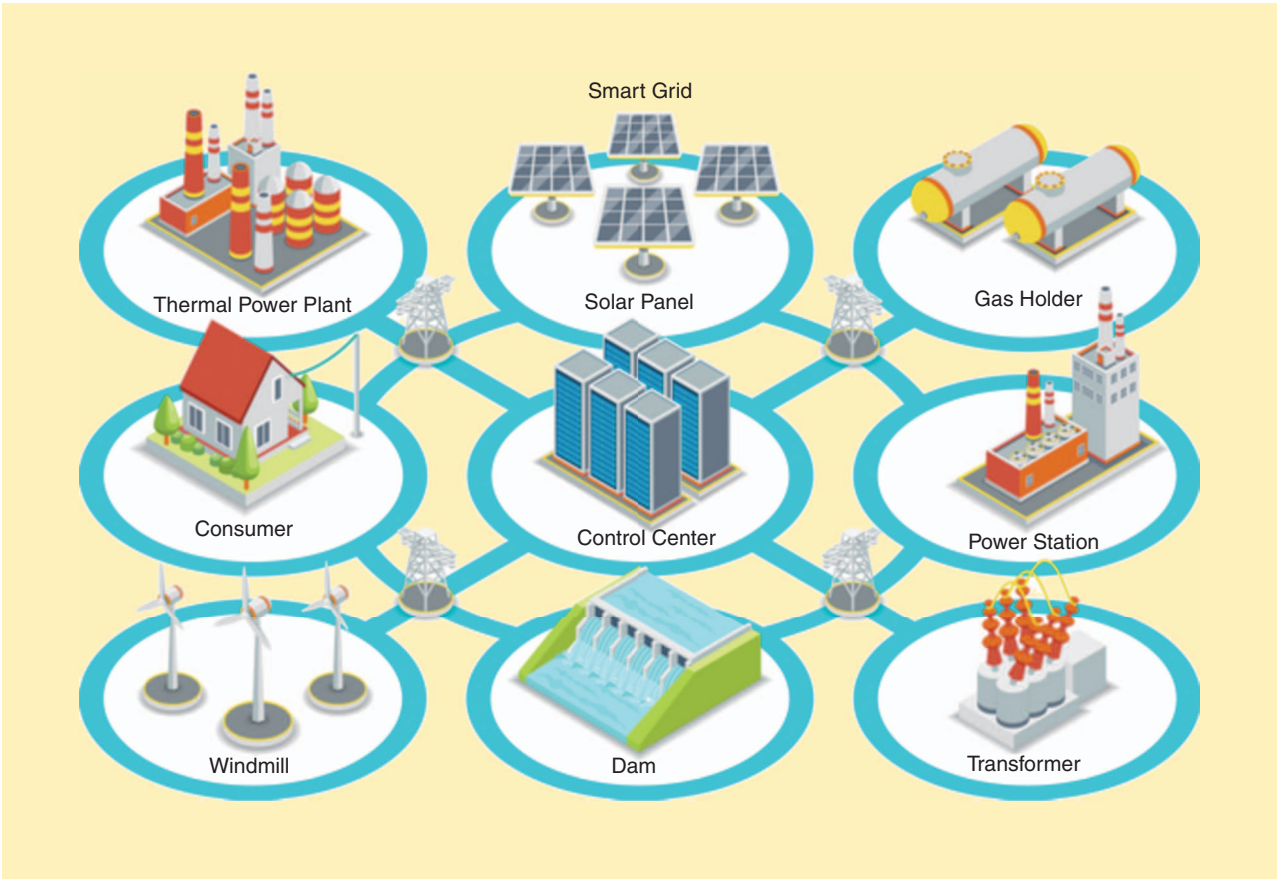

FIG 1 The smart grid network is very distributed and vulnerable to physical and cyberattacks. (Credit: MSSA/Shutterstock.)

The Ukrainian case is considered a real-life example of what could happen to larger networks.

FIG 2 Cybercriminals taking control of the smart grid is now a reality. (Image courtesy of Powerbox.)

they managed to break credential codes to access deeper levels of the system, controlling industrial communication busses such as the ones interconnecting uninterruptible power systems (UPSs) to the supervisory control and data acquisition (SCADA) systems.

SCADA systems are basically process control systems (PCSs) that are used for monitoring, gathering, and analyzing real-time environmental data. PCSs are designed to automate electronic systems based on a predetermined set of conditions, such as traffic control or power grid management. For the ones used to lower energy and board power systems, it is supersoftware-defined power architecture, which, considering the strategic role it plays, requires an extremely high level of security. After gaining control of the SCADA systems, the hackers accessed the electricity network, which allowed

them to shut down and severely damage equipment.

The Ukrainian case is considered a real-life example of what could happen to larger networks. The lessons learned from that case are part of ongoing smart grid security standardization projects in the United States, Europe, and Japan.

Making the Smart Grid Safer

The smart grid is an extremely complex architecture with a lot of areas for intrusions and attacks. Over the years, it has shifted from managing electricity distribution to becoming a super information and communication technology (ICT) machine. Michael McElfresh, adjunct professor of electrical engineering at Santa Clara University, California, summarized the situation very well [6], saying "Technological advances in grid operation have made the power grid increasingly vulnerable

Although the worldwide smart grid is slowly and steadily getting stronger and safer, the potential of threats remains high.

Smart Grid Overview Showing the Different Actors and Points of Interfaces Within the Grid

FIG 3 The complexity of the smart grid makes it very difficult to protect globally. (Image courtesy of Powerbox.)

to cyberattacks." He also stated, "The growth of the smart grid has created many more access points for penetrating grid computer systems—the Internet of Things (IoT) will only make this worse."

All over the world, governments, consortiums, and groups of experts are engaged in an amazing race to deploy security methods and protocols to make the smart grid safer. In the United States, the set of critical infrastructure protection (CIP) standards issued by the North American Electric Reliability Corporation became mandatory in 2007 for owners, operators, and users of the Bulk Electric System to ensure that certain assets on the grid critical to reliable operation are protected from both cyberattacks and physical damage [7]. It is going through a wave of new revisions, moving from CIP V3 to CIP V5—skipping V4, and accelerating V6! This revision cycle reflects the situation faced by the standardization organization, developing security standards in a fast-evolving world of threats [11], [12].

In Europe, despite a number of initiatives within the European network and information security community to establish frameworks and standard operating procedures, the E.U. level response to cyberincidents lacks consistency. However, projects such as the E.U.-funded Smart Grid Protection Against Cyberattacks are showing signs of progress [8]. Although the worldwide smart grid is slowly and steadily getting stronger and safer, the potential of threats remains high.

Conclusions

Because of the complexity and the variety of devices connected to the smart grid (Figure 3), power supply manufacturers will have to consider the security aspects when their products are integrated within a smart grid. Introduced at the Asia-Pacific Economic Cooperation in 2015, software-defined power architecture is deploying fast in the ICT industry; some systems already installed in data centers are connected to the smart grid and communicating through the SCADA system. In this loop, even if there is little risk that a hacker can send a command to a POL blasting local core processor, the risk for UPS and even the front-end rectifier to receive a fatal command is far greater. The Ukrainian incident has triggered the alarm for all of us involved in developing power systems connected to the smart grid. It is a signal that we should never forget about the final application and to be smart security innovators to power the smart grid with excellence.

The Ukrainian incident has trigged the alarm for all of us involved in developing power systems connected to the smart grid.

About the Author

Patrick Le Fèvre (patrick.le-fevre@prbx.com) is a graduate of the Paris Delépine-Bessière School in technical engineering. Currently, he is the marketing and communications director at Powerbox. He is a certified electronics engineer with 25 years in power electronics. He pioneered the marketing of new technologies such as digital power and technical initiatives to reduce energy consumption and has written and presented numerous white papers and articles at the world's leading international power electronics conferences. He is also involved in several environmental forums, sharing his expertise and knowledge of clean energy.

References

[1] P. Pederson. Project Aurora and the smart grid. [Online]. Available: https://www.whitehouse.gov/files/documents/cyber/Pederson%20Perry%20-%20Aurora%20and%20the%20Smart%20Grid.pdf

[2] CNN (2007, Sept. 26). Staged cyber attack reveals vulnerability in power grid. [Online]. Available: http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html?iref=topnews

[3] Internet Governance Project. (2009, Apr. 3). A more detailed look at the proposed Cybersecurity Act of 2009. [Online]. Available: http://www.internetgovernance.org/2009/04/03/a-more-detailed-look-at-the-proposed-cybersecurity-act-of-2009/

[4] U.S. Department of Homeland Security. Alert (IR-ALERT-H-16-056-01): Cyber-attack against Ukrainian critical infrastructure. [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[5] E-ISAC. Analysis of the cyber attack on the Ukrainian power grid. [Online]. Available: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[6] M. McElfresh. Can the smart grid survive a cyberattack? [Online]. Available: http://www.energypost.eu/can-smart-grid-survive-cyberattack/

[7] North American Electric Reliability Corporation. NERC website. [Online]. Available: http://www.nerc.com/

[8] The smart grid protection against cyber attacks (SPARKS) project. [Online]. Available: https://project-sparks.eu/

[9] E. Lacy. BWL in limbo from cyber attack. [Online]. Available: http://www.lansingstatejournal.com/story/news/2016/04/27/cyberattack-bwl-keeps-fbi-silent/83590820/

[10] B. Fowler. (2016, Oct. 22). Attacks on the internet keep getting bigger and nastier. [Online]. Available: http://www.khou.com/tech/attacks-on-the-internet-keep-getting-bigger-and-nastier/340203887

[11] U.S. Department of Energy. Cybersecurity for energy delivery systems. *Energy.gov*. [Online]. Available: http://energy.gov/oe/services/technology-development/cybersecurity-for-energy-delivery-systems

[12] U.S. Department of Energy. Cybersecurity for energy delivery systems (CEDS) fact sheets. [Online]. Available: http://energy.gov/oe/downloads/cybersecurity-energy-delivery-systems-ceds-fact-sheets

PEM