Smart Grid Security and Architectural Thinking

Security design should be an integral part of the first phase of developing smart grid architecture to maximize its benefits and minimize future risks

By Jeffrey S. Katz, IBM

Smart grid means automation of the electric power grid, and automation often means computerization, which can create new cyber security risks to a process if proper thought to the system design is not applied. When implementing a smart grid project, security issues and lessons to consider include source code security, security as risk management, and how to move beyond defensive behavior to proactive procedures.

The first step toward protecting the smart grid from security breaches involves risk analysis: In the event of a cyber security threat to the electric power system, what is at stake? The first risk is serious disruption to the electric grid, which the North American Electric Reliability Corporation (NERC) calls a critical national infrastructure. The NERC Critical Infrastructure Protection (CIP) guidelines list security concerns that must be addressed. Another significant risk is loss of system availability, and the possibility of losing control of certain aspects of the grid.

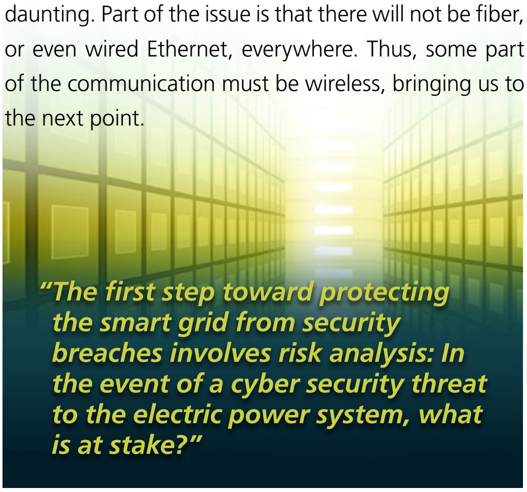
After these basics, consequences of a grid failure must be considered. One possible consequence is process interruption. For example, manufacturing processes could be jeopardized, leading to damage of production equipment or the product being manufactured. Such forced outages could be detrimental to petrochemical refineries, pharmaceutical manufacturing, and other industries using continuous processes. Significant equipment damage can also occur in situations where electricity supplies important cooling or heating functions.

While news and media scenarios tend to dramatize wide-scale electricity black outs, another risk—asset misconfiguration—is more insidious. In this scenario, settings on equipment are changed, and normal operational protections are removed. For example, if a protective relay, or a voltage tap is set to 130 VAC instead of 120 for a residential area distribution line. Loss of data and confidentiality is the most subtle consequence—and is more applicable as we move to advanced metering infrastructure (AMI) and 15-minute interval meter reads, increasing the likelihood of misuses that can lead to an invasion of privacy for individual residents. Another risk factor follows from NERC CIP, which has now instituted substantial financial penalties resulting from violations of its regulations.

Another very serious risk involves employee safety. When considering protective measures, some utilities identify safety as their first priority and reliability as second. Personal injury to employees is a prime concern because typically two-thirds of the staff are field crews. While most utility line personnel are trained to always assume a line is energized, sudden presence of voltage due to a line being re-energized from an unauthorized source can still be a threat.

Lastly, there is the risk of loss of customer and public trust, particularly given how difficult it would be for a utility to deny awareness of the existence of cyber security threats. This would be more problematic for utilities in the jurisdiction of public utility commissions, since outages that utilities could have reasonably protected themselves against could be perceived as violating their mission to protect the public.

Having framed the risk context, we now move to measures to mitigate those risks. As to security, perimeter defense alone is probably not enough. A diagram that shows a firewall, with intruders outside the wall and systems to be protected inside, is too simplistic for an undertaking as geographically distributed as the electric power grid. Its widespread nature makes drawing a logical boundary easy, but a physical boundary of protection is much more daunting. Part of the issue is that there will not be fiber, or even wired Ethernet, everywhere. Thus, some part of the communication must be wireless, bringing us to the next point.



"The first step toward protecting the smart grid from security breaches involves risk analysis: In the event of a cyber security threat to the electric power system, what is at stake?"

Radio frequency (RF) devices inherently require additional security considerations. This is relatively apparent given how easy it is to snoop on unsecured home wireless Local Area Networks (LANs) or older portable phones. While, as delivered, these devices have limited range, it doesn't take much expense to obtain an antenna with directional gain to pick up these signals from far away. Thus, the intrusion radius can be significant, as is illustrated by the practice of so-called "war driving"—a term derived from the classic hacker movie War Games, referring to the act of driving around with a wireless laptop to find unsecure wireless networks with which to connect. RF devices are also susceptible to denial-of-service attack by frequency jamming, or blocking received signals by wrapping the device in aluminum foil.

Being secure is not just about keeping the "bad guys" on the outside; it is also about making the systems inside less vulnerable. One has to maintain the philosophy that the internal systems will eventually be exposed to attack. Reducing vulnerability of internal systems includes ensuring:

- Each application validates its input for reasonability before processing;
- Each application has a way of announcing an exception—whether it is a security intrusion or simply a failing Intelligent Electronic Device (IED) sending bad input.

It is for the security system to decide why the abnormal event occurred.

Applications should not contain built-in weaknesses; however, any functional piece of software may still contain security holes. Some of us are aware that certain vendors publish lists of security patches. On occasion, patterns can be observed in the descriptions of these weaknesses—problems that were effectively, but not intentionally, in the source code. A program may have passed its functional testing, but security issues may still exist. There are actually software products that can scan and analyze source code, somewhat as a compiler does, looking for potential problems with array indices (e.g., buffer overflows) and other common conditions that may not have been checked. Beyond a locally written application having no detectable security flaws, there is the worrisome fact that a typical executable application (e.g. .exe file) contains much code the programmer didn't write. Such code comes not from a source (e.g. '.C' file), but from a multitude of pre-supplied libraries and linked-in objects. The provenance of such off-theshelf components may be worth knowing, or at least be certified as not a security risk. Such scrutiny of supplied software is "de rigueur" in certain financial and avionics applications, for example.

"In general, what is desired is a culture of security, not a culture of compliance with security regulations."

To further improve the smart grid security profile, attention to architectural tenets is needed beyond some of the tactical measures suggested above. These can be applied specifically to cyber threat reduction in general hardware or software architectures. One conventional precept is to "build for the end solution." In terms of the smart grid, the view on cyber security is that "security is risk management." Deployment of smart meters would probably slow down if a hacker-proof meter was developed at a cost of $1,000 per unit. Although there is risk both to the confidentiality of meter-reading data and even risk of individual remote disconnect, these must be put into the perspective of risk management. There is a cost associated with this risk. If the risk is not pervasive, as when an attack on the meter network does not penetrate to the substation control network, then security risk must often be weighed against cost. Risk reduction strategies, such as giving good consideration to whether the AMI network should have any connection to the SCADA network, should also be employed. Economic versus security trade-offs can be justified with risk analysis, assuming a secure overall architecture is employed.

Sometimes it is human nature to push difficult problems out of mind by assuming technology will be the saving factor, such as "put in a firewall and we're done." Similarly, people will buy a $300 alarm system with a $25 monthly monitoring fee. However, they seldom think to replace the 1-inch hinge screws in their wooden front door with 3-inch screws that go deep into the stud around the doorframe—a precaution that requires just a $5 purchase at the hardware store, assuming the homeowner already has a power screwdriver. A number of television commercials for premises alarm companies show a burglar kicking in the door, resulting in a quick response from the alarm company. But why is it so easy to kick in the door in the first place, creating the need for a high-tech alarm? This is the type of security thinking needed when considering the smart grid.

When looking at the smart grid holistically—power grid plus automation—security also overlaps with the dimension of reliability. A system that recognizes security threats may also capture events that result not from external threats but from internal mistakes, with human error being a more common occurrence. An effective security approach enhances reliability because some security failures might be people failures, while others might be equipment failures, might be due to natural causes or might be deliberate. In general, what is desired is a culture of security, not solely a culture of compliance with security regulations. In defending our electric grid, a security anomaly detection system that cries wolf once or twice is preferable to the alternative.

Some smart grid security issues are brought to the public's attention by the media in a context that can be embarrassing to utilities. In such cases, utilities should view these reports as a "heads up." For example, it is likely that somewhere in a smart grid there is the popular TCP/IP protocol commonly associated with the Internet. However, this does not mean the smart grid is connected to the vast public Internet. Often, however, it is interpreted that way, especially when all the facts and capabilities of the smart grid are not properly presented. Smart grid design should not directly involve the Internet. The vital parts of the smart grid need to be protected from any possibility of public access to reduce the likelihood of an external security breach.

Some of the points above already hint that security provisioning can significantly affect system design, and therefore should be part of phase one in the design of any successful project. The re-design cost can be too high, not only in terms of delays and cost, but also in terms of public trust. At the time of this writing, smart grid projects funded through the American Recovery and Reinvestment Act (ARRA) have a fixed deployment time and a public "lessons learned" reporting requirement. In the proposals, applicants are required to submit security and interoperability statements about the proposed project. These two requirements should help utilities understand best practices around smart grid security.

Once an incident occurs, the loss of trust makes a security retrofit, at any cost, less believable to the consumers. While security design should be in the first phase of a project, the time-worn phrase, "scope, schedule, and budget," can sometimes work against proper security design. Projects have schedules and budgets, while hackers have no such constraints. Therefore, long after the secure smart grid project is completed, cybercriminals may be working on new technologies to circumvent what has been done and acceptance tested. As a result, periodic security testing is required indefinitely and must be accounted for in ongoing operational budgets. This is really no different from buying a substation and budgeting for annual maintenance expense.

So far, we have addressed smart grid cyber security because it is in vogue. Thus comes the admonition not to overlook physical security. Consider high-resolution security cameras on substations. They would permit the use of image recognition software, which could automatically detect a human presence versus an animal within the fence. Some utilities have even considered using a dual purpose thermal camera for night situations. Besides looking for intruders, when thermal cameras are aimed at the transformer, hot spots can be detected in the image that might be of use to maintenance. Substation fences consisting only of chains may need heavy cable and secure padlocks (ones that can't be snapped shut and whose keys can't be copied just anywhere). Utilities with substations that use card key access control might think of linking their work order system to the card key access control computer. Just as a hypothesis, consider that in normal operation, a valid card key won't allow entry to a substation if there is no work order currently assigned to that substation. In such a case, the field technician would need to call in to confirm entry. In any kind of storm, emergency, or wide area problem, the valid card key would be accepted by the access control system to work without restriction.

Smart grid designers should also look to the CIO's office and some information technology best practices. For example, most enterprises do not allow

"The vital parts of the smart grid need to be protected from any possibility of public access to reduce the likelihood of an external security breach."

just any portable computer to be brought in, plugged into an Ethernet jack in an office, and connected to the corporate network. A similar strategy should be employed in the actual smart grid: connected IEDs must be pre-authorized to participate. This may take a bit more coordination in the repair or replacement process, but will reduce the possibility of device spoofing.

The phrase "connecting the dots" is often heard in post-facto discussions about security lapses. The smart grid will provide much more data about grid operations than the traditional grid. By using stream computing or complex event processing software, events on the grid may be categorized as operational, maintenance, or security. Correlating suspicious activity from all inputs then becomes part of the security detection methodology.

Another axiom that applies to grid security is "a chain is only as strong as its weakest link." Think of six vendors involved in the path from smart meter to back-end Meter Data Management System (MDMS). Each of these vendors could indicate, even certify or prove, that their component is secure. If it is no one's job to check the overall end-to-end security of the system, then six connected secure devices do not in themselves ensure a secure system. There are several reasons why a series of secure devices might not achieve the desired end-to-end security:

- Problems with the interconnections
- Problems with the communication link between each device
- Problems with the remote configuration process
- Problems with the remote firmware upgrade process
- Problems with secure application design—vetting of incoming data

It is therefore recommended that overall end-to-end security be an assigned responsibility on a project for the overall system integrator or another expert provider.

In conclusion, smart grid security involves an architecture that includes security from the beginning, consists of more than just protective devices such as firewall, and engages processes as well as products. A simple perimeter defense is not sufficient; monitoring, both for events and physical actions, is required to bring the benefits of smart grid with minimal risk to this vital part of the infrastructure of modern life.

To view references and sources please visit www.generatinginsights.com

About the Author

Jeffrey S. Katz is the Chief Technology Officer of the Energy and Utilities industry at IBM. He is involved with the application, development, and innovation of IBM products, services, technology and research for electric power companies and related organizations. Katz has worked on the industry's framework, Solution Architecture For Energy (SAFE), the IBM Innovation Jam workshops, the IBM Intelligent Utility Network initiative, and is the primary industry liaison with IBM Research.