OFFPRINT FROM STRATEGIC OUTLOOK 7

The Swedish Electricity Supply System:
How to Deal with Increasing Vulnerability

Maria Andersson and Lars Westerdahl

Society has become totally dependent on electricity. Without it, many daily activities could no longer be performed. The electricity supply system is vulnerable, however, and the ongoing transition to smart grids will make it even more so. Cyberattacks can be carried out even on the existing power grid. These attacks cause major disturbances to society, as was demonstrated by the recent cyberattack on Ukraine's power grid. These increased risks must be taken into account in the ongoing transformation of the Swedish electricity supply system.

The electricity supply system as a target for cyberattacks

Suspected preparations for cyberattacks on the Swedish power grid have recently been reported. Sweden's National Defence Radio Establishment (FRA) announced in January 2017 that it had detected suspicious activities and preparations. The 2015 cyberattack on the Ukrainian power grid began with emails being sent to several electricity distributors. The emails contained attachments with malicious code that made it possible for the attackers to pass through firewalls and into the control system. Hundreds of thousands of electricity customers lost power while the power grid had to be manually restarted, which took several hours.

The evolving power supply system

The Swedish power grid is evolving into a so-called smart grid. Smart grids are characterised by increased use of modern communications technology. Data is collected from more actors, which creates opportunities for detailed analyses of different states in the power supply system. These analyses can serve as a basis for more cost-effective pricing, improved demand forecasting and higher demand flexibility. Smart grids provide good opportunities to improve energy efficiency and reduce costs in the power supply system. However, the transition to smart grids also increases vulnerability to cyberattacks.

Traditional power grids distribute electricity in one direction and production is adapted to a standardised customer demand. From a historical perspective, electricity production has mainly taken place in large-scale power generation plants, such as hydroelectric or nuclear power stations. Smart grids can be seen as an upgrade on the traditional grid, where new technologies are installed to improve control and monitoring in all areas of the power supply system – the production, transmission and distribution systems – as well as with the customer. To make full use of the benefits of the new technology, several actors need to be able to communicate and interact. The new technology makes it possible to better balance electricity supply and demand. Smart grids can react better to demand flexibility and the variable electricity production of renewable energy sources such as solar and wind power in local energy systems. Another driving force behind the transition to smart grids is climate policy. Climate targets in the European Union and Sweden require reductions in greenhouse gas emissions. Key elements of achieving climate goals are an increase in the use of renewable energy sources and improved energy efficiency, both of which will benefit from the move to smart grids. In summary, the large-scale introduction of variable electricity production, energy efficiency measures and demand flexibility will create demand for improved monitoring, control and measurement in the grid – the technologies that characterise smart grids.

Increased vulnerability

The grid control system has traditionally been more or less isolated from the outside world. Developments in IT, however, as well as cheaper IT components mean that traditional electrical components and vendor-specific solutions are being replaced in control systems with hardware and software components as well as communication protocols that were initially developed for ordinary office systems. This has resulted in control systems and office systems being able to communicate

FOI Memo 6204
Approved by: Lena Bartholdson

Offprint from Strategic Outlook 7
November 2017

with each other. For the electricity providers, this has meant a potential increase in the availability of up-to-date information on what or how much is produced. This information can be used, for example, to charge the customer more accurately.

This interconnection of systems has not only created an increased need for communications. Interconnected systems also increase the exposure of production, transmission and distribution systems to an environment that they were not designed to handle. Increased internal communication will increase the complexity of the power supply system. At the same time, however, increased exposure to the Internet will leave systems open to hostile intentions. An antagonist, that is, a conscious attacker who wants to steal information, prevent access to systems or exploit such systems for their own interests, is something that did not previously need to be considered to any great extent.

Correctly implemented security functions are difficult to get past. This means that attackers rely instead on *phishing* and *spear phishing*, which aim to trick a person sitting at a computer in the target organization into opening a prepared attachment or clicking a link to a prepared web page. If the person opens the attachment or clicks the link, the attacker has passed the firewall and entered the network. Based on such a foothold, an attacker can move on to the main goal.

The need for structured security work

The risk of vulnerabilities increases in complex systems with multiple actors. In such an environment, structured security work between actors is required to achieve adequate protection for the entire power grid. Each actor needs to work systematically on security issues for their own system throughout the lifecycle of the system. Security is not a product that is installed once, but rather the result of continuing work.

The aim of security work is that a system should be able to contribute to the operation even if antagonists try to attack it. This is achieved by a combination of training for staff, administrative measures and technical solutions. Continuous security work is particularly important for control systems, given that they usually have a long service life, sometimes of up to 20 years, and high availability requirements. This is in comparison with office-based IT systems, which are usually replaced every three to five years.

A system is designed to handle known vulnerabilities. As the system is maintained and adjusted, new vulnerabilities may arise, for example through increased exposure. A system that is not maintained from a security perspective will deteriorate over time.

Security analysis

Infrastructure systems such as power supply systems are rarely developed by a single system owner. Several actors interact within the power supply system, and the system consists of several subsystems with interdependencies. Changes in these subsystems do not occur at the same time, which means that new and old subsystems will need to exchange information. The subsystems may also have dependencies between them.

Building IT systems in an environment where there are multiple systems with different owners places great demands on the interfaces between the systems for enabling communication. Each actor must ensure the functioning of its subsystem and identify the risks to which the subsystem is exposed. It is therefore important that subsystem owners share a common view of the threat situation in which their systems will operate. When a new system is to be introduced, security analysis is an important tool for identifying which security functions are needed and the procedures required to support them.

However, since the security of a system will deteriorate over time, security work does not end when the system is put into operation. IT systems contain weaknesses that are detected as the system is used and corrected by *patching*. If patching is not performed, the system will contain known weaknesses.

A managed system will constantly change. This means that continuous security analyses need to be conducted. The functionality assigned to a system after it has been put into operation needs to be examined as carefully as new functionality is examined during system development.

To prevent cyberattacks

The foundations of and prerequisites for the security of a system are installed during system development and reinforced through maintenance work. However,

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Phone: +46 8 5550 3000
Fax: +46 8 5550 3100
https://foi.se/en.html

active security work is also required during the system's operation, including pre-emptive and follow-up activities over time. Increased security is achieved through technical solutions, administrative procedures and supportive management.

Administrative procedures provide structure for security work. Structured security work, however, must focus not only on the functionality that the system will deliver, but also on the functionality of the system. This means that the system owner must know what has been installed in the system, and either support all of its functionality or remove any unnecessary functionality. Maintaining control of maintenance work, including of installed updates, is part of security work.

In collaborative systems, for example in power grids where there are several actors, it is even more important to actively monitor your own networks. The security functions provided during the development phase are designed to handle the threats that existed when the system was developed. New threats may have occurred to a system that has been in operation for a while. Existing security solutions cannot always detect or handle these new threats. It is therefore important to pay attention, for example, to changes in patterns of communication in the network. Monitoring is required to detect illicit activities on the network, but staff members are also needed to follow up logs and alarms. Monitoring includes logging, intrusion-detection systems and anti-virus programs.

To handle cyberattacks

Whether the aim is information theft, prevention of access or to utilize system functionality for the attackers own purposes, once detected an attack needs to be addressed. How this should be done depends on the type of functionality that the system is delivering. For an information system that has no hard real-time requirements, the system can be shut down for a while in order to manage the intrusion. For a system that supports critical infrastructure such as power grids, however, this is not always possible. In such cases, the attack must be handled while the system continues to support the activities of the organization.

The key to handling an attack effectively is preparation. A crisis group established around a number of key individuals with good knowledge of the business and a large network of contacts will be an important resource in such a situation. The group must be prepared. It should have reviewed a number of possible scenarios and drawn up action plans, contact lists, and so on. Dealing with cyberattacks need not be the sole purpose of such a group. It could also act as a "general troubleshooter" within the organization.

Larger organizations could establish a Computer Emergency Response Team (CERT), a specific group highly skilled in handling IT problems. Its task would be to restore a system that had suffered an attack as quickly and efficiently as possible, while also ensuring that the same problem could not occur again. A CERT is expensive, which means that there tend to be industry cooperation or national functions established as external resources that can support smaller organizations by providing technical skills and knowledge of known threats.

Smart grids increase the exposure of control functionalities, which provides a larger attack surface. However, this attack surface does not necessarily lead to greater demands on other security functions in the system. On the other hand, there may be greater priority placed on the ability to detect intrusions and to handle incidents. An increasing number of actors in the power supply system also place a higher priority on the coordination of security issues.

The new power supply system requires both new and old security solutions

There are several strong drivers behind the transition to smart grids. These are likely to speed the transition. Both intensive and structured security work are essential during the transition phase, and this work should continue throughout the entire lifecycle of the power grid. Active security work, where people, administrative practices and technologies interact, is a necessity for long-life IT systems. This means that active safety work is important for as long as the system is in operation.

The attack on the Ukrainian power grid in 2015 is a good reminder of this need. Although electricity supply was lost for only a few hours, the attack was in preparation for several months. It is common for cyberattacks to go undiscovered for several months, sometimes years, depending on the attacker's goal. In Ukraine, the attack began with a targeted phishing

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Phone: +46 8 5550 3000
Fax: +46 8 5550 3100
https://foi.se/en.html

attack to get a foothold in the networks. A long period of surveillance of the networks followed, to find a way from the initial entry computer to the actual target system. It is during this period when active security work, including monitoring, might have detected the attack.

Industry-based and national monitoring functions cannot be more effective than the tasks they are given. The Swedish power grid, like much other critical infrastructure, is made up of several actors. It is important that incidents are reported to an organization capable of maintaining an overview.

The events in Ukraine also taught another important lesson: manual recovery functions are still important. Technicians were forced to revert temporarily to manual functions in order to restore electricity distribution.

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Phone: +46 8 5550 3000
Fax: +46 8 5550 3100
https://foi.se/en.html