Grid security for intelligent power supply networks

Power Utilities are operating critical infrastructures and as such their highest priority is to ensure a cost effective and reliable supply of energy. New challenges have fundamentally changed the nature of how power grids are operated today. These challenges include the integration of renewable and decentralized energy sources, the need for continuous grid optimization, and the inclusion of increasing numbers of consumers becoming producers of electrical power. Information and communication technologies (ICT) are increasingly pervading the grids, and the growing number of interfaces is generating new security risks for our power supply grids. Consequently, grid security has become one of the biggest and most important challenges for power utilities.

As a reliable strategic partner to the energy industry, Siemens’ Energy Management Division offers energy providers and grid operators the right solutions for mastering these challenges. One of the challenges is product security – and Siemens products comply with all standards and satisfy diverse country-specific regulatory requirements for grid security. Siemens also supports its business partners with consulting services for all aspects of this matter.

Siemens participates in the key standardization committees to incorporate the latest technologies and knowledge into its standards and products. Siemens offers an all encompassing approach to security, based on the following key factors:

- Confidentiality: encrypted communication between individual devices and systems;
- Integrity: protect devices against malware;
- Data protection: encrypted data storage with regulated access rights;
- Availability, the most important requirement for these systems.
An appropriate security solution requires a comprehensive strategy. As part of the strategy, Siemens defines security measures reflecting a holistic approach to cyber security, and encompassing the so called “3 P”:

- People and organizations: those who are running the company;
- Processes: those used by the people and organizations to fulfill the business needs;
- Products and systems: the underlying infrastructure to support the business needs.

**A basis for trust: a solid foundation for security**

Grid security is a highly sensitive area that requires a partner who can be trusted. As a technology partner, Siemens understands how products, systems, and solutions interact with the underlying processes and people. As a globally structured company, it has a leading smart grid portfolio and the knowledge and extensive experience in both intelligent power supply networks and grid security for intelligent power supply networks.

Siemens experts are represented in the relevant international standardization organizations to further improve the standard of security for smart grids. They also advise supervisory authorities on technical and process-related matters. Its company-wide Cyber Emergency Response Team (CERT) gives Siemens a global overview of emergent threats that impact, for example, the grid security of power supply networks.

Siemens is founding member of the EE-ISAC sharing platform for cyber security in the energy supply industry. EE-ISAC, the European Energy Information Sharing & Analysis Center (www.ee-isac.eu), is the first international sharing platform for cyber security issues. Here both public and private groups exchange information on matters of security as a means of better protecting Europe’s energy infrastructure against cyber-attacks. The sharing platform will soon acquire the status of a company under civil law, with Siemens as a founding member. The current stakeholders in the information-sharing platform include European energy providers such as Alliander, EDP, Enel and EVN, as well as technology and service companies such as Accenture, Security Matters, Siemens and Viasat. Institutes from the University of Louvain, the Delft University of Technology and the University
of Gdansk are also involved, alongside the non-profit organizations European Union Agency for Network and Information Security (ENISA), National Cyber Security Centrum (NCSC) and European Network for Cyber Security (ENCS). Additionally Siemens acts as a technology partner of ENCS.

**End to end Network security: network protection with integrated grid security**

The goal of all security efforts is to obtain a system that is accessible at all times and is not corrupted. Siemens offers grid security solutions incorporating products and systems. This concept ensures increased protection against cyber-attacks and reliable grid availability. The security architecture is based on a combination of different measures that are defined in the relevant global standards. Key examples are IEC 62443, IEC 62351, and ISO/IEC 27000. As part of a Siemens security plan for smart grids, the integration of encryption and communication components enables a higher level of security in system-critical devices, because it provides end-to-end data encryption along transmission links.

**Continuous monitoring: access management and strategies**

A robust security strategy must factor in the human element, because incidents are often triggered by the misuse of access privileges. That is why Siemens relies on a powerful authentication and authorization system in its solutions. Based on the principle of minimal allocation of rights, users are only given the access privileges that they need for their work. Access management in the operation of a smart grid involves different security rules than those used for traditional IT systems. These rules must permit operational availability while also meeting requirements like role-based access controls. By combining central access management for SCADA systems (supervisory control and data acquisition) with a smart grid infrastructure that will also work interoperable in systems involving different manufacturers (multivendor systems), Siemens’ solutions can offer a single sign-on system that will integrate in any existing IT security environment.

**Keeping the grid under control: monitoring, recording, and evaluation**

Energy providers and grid operators must keep an eye on all of the processes within a smart grid. They must constantly analyze them in order to receive immediate
indications of potential cyber security threats. Energy providers and grid operators can investigate any incidents that occur. A security information and process management solution also lets operators stay informed at all times about the current security status of their smart grid. Continuous analysis of network events can identify attacks and risks.

Closing security gaps: dealing with malfunctions and managing security patches

If a security event occurs that impacts the system, energy providers and grid operators must be prepared to intervene. The solutions offered by Siemens’ Energy Management Division for dealing with these incidents are seamlessly combined with Siemens’ security patch management service. This is a service in which Siemens experts draw on the company-wide Cyber Emergency Response Team (CERT) to search for new software vulnerabilities throughout the world and identify relevant security patches from third-party suppliers in order to establish compatibility or to provide updates as swiftly as possible for the products and systems in their smart grid portfolio. When it comes to security patch management, Siemens distinguishes between critical and non-critical updates, which are made available for selected systems and installed by the user upon request, in accordance with the level of urgency. Only relevant and tested patches are deployed on critical infrastructure as guided by customer policies.

Grid security at Siemens: practical examples

**BSI-compliant IT solution for smart metering:** Siemens has added application software components to its EnergyIP smart grid application platform especially for the German smart metering market. This means that Siemens is providing power utilities with a central IT solution for managing smart meter gateways and process-encrypted and signed meter data on energy consumption. This solution enables energy providers to connect smart measurement systems comprising a smart meter gateway and smart basic meters to their central IT system. In terms of data protection and data security, the IT solution satisfies the requirements set forth by Germany’s Federal Office for Information Security (BSI) in its technical guideline for smart energy, TR-03109.
Secure meters from Siemens’ development programs: The electricity meters developed by Siemens come with authentication in the form of certificates. Charging information is encrypted for the entire length of transmission between the meters and the metering service provider’s central IT system. The encryption procedure works with an algorithm based on elliptic curves as they represent the current technology.

VPN feature integrated: The Sicam A8000 series of compact remote terminal units, designed for operations in diverse contexts ranging from substations to renewable energy parks and micro grids, offers an integrated VPN feature (virtual private network) based on IPsec (internet protocol security). The IPsec tunnel, originating from within the device ensures end-to-site encryption and integrity of IP-based communication between the A8000 series and supervisory control and monitoring systems. HTTPS (Hyper Text Transfer Protocol Secure) makes secure engineering over a web browser possible. For browser-based access, Sicam A8000 devices support on-board role-based access control, with user accounts that can be either locally managed or centrally in a Radius server (Remote authentication dial-in user service). Communication between the device and the Sicam Toolbox II configuration tool is encrypted with transport layer security (TLS). A built-in crypto chip optimizes the encryption and stores the key material securely.

Smart grid remote-control unit for decentralized electricity generators: In collaboration with Sicam SGU, Siemens has a communications-capable field device in its portfolio that allows a communications connection to be established between distributed energy resources and a grid control or energy management system. When it is used as an input/output (I/O) unit, power providers and municipal utilities can control and monitor decentralized power generation systems and consumers using the smart grid remote-control unit. Siemens manages the data security function required for all applications involving its remote control unit. A connection with a closed VPN (virtual private network) computer network based on IPsec (Internet protocol security) enables encrypted data transmission. When used without a wireless mobile module, transport layer security (TLS) – the integrated encryption protocol for secure Internet data transmission – provides end-to-end data security for OpenADR communication (Open Automated Demand Response).
Integrated cyber security for digital security devices: The protection devices in the Siprotec 5 series are suitable for use in both medium- and high-voltage switchgear, where communication between the Siprotec 5 and the Digsi 5 configuration tool is TLS-encrypted to enable the necessary security. In addition, the protection devices are equipped with integrated protection of the firmware that protects against tampering by malicious parties. The firmware contains a digital signature that is validated before it is loaded onto the device. A built-in crypto chip optimizes encryption in the Siprotec 5 protection devices and stores the key material securely.

Encrypted communication and access protection in station control technology: Communication between the Sicam PAS station automation system with its network control center is encrypted via the secure version of the IEC 60870-5-104 and DNP3 TCP protocol in accordance with security standard IEC 62351. For role-based access control of the human machine interface, the local Sicam SCC operating and monitoring system supports flexible user/rights management, including central management of user IDs, passwords and roles via Microsoft Active Directory Domain Controller.

Cyber security for industrial systems: Siemens energy automation solution certified. Siemens has had a typical energy automation solution comprised of both hardware and software components certified in accordance with IT security specification WIB 2.0 (working-party on instrument behavior). This specification has now been incorporated into the international standard IEC 62443. The security standard specifies requirements not just for individual products and systems but also for the entire energy automation solution – from product creation to engineering and commissioning through to operations, service and maintenance. Together with the German association for technical Inspection, TÜV Süd, Siemens is currently working on an IEC 62443 certification as an evolution of the WIB 2.0 certification. With this certification process, Siemens satisfies its industrial customers’ desire for the products and systems used in their power supply solutions to comply with the latest cyber security guidelines.

Solutions for grid security for intelligent power supply networks are part of the Siemens Division Energy Management’s product portfolio. As a product supplier, system integrator, and solution and service provider, the Division offers power supply companies and industry cost-efficient, reliable, and intelligent solutions for
the transmission and distribution of electrical power. The portfolio ranges from products and systems for low-voltage and distribution networks and smart grid and energy automation solutions to high voltage transmission systems. With a presence in more than 100 countries, the Siemens Division earned approximately €11.9 billion in sales and €570 million in profit and employed just fewer than 53,000 employees worldwide last fiscal year, which ended on September 30, 2015.

For further information on Siemens’ Energy Management Division, please see www.siemens.com/energy-management

Contact for journalists
Dietrich Biester
Phone: +49 9131 7-33559; E-mail: dietrich.biester@siemens.com

Follow us on Twitter at: www.twitter.com/siemens_press

Siemens AG (Berlin and Munich) is a global technology powerhouse that has stood for engineering excellence, innovation, quality, reliability and internationality for more than 165 years. The company is active in more than 200 countries, focusing on the areas of electrification, automation and digitalization. One of the world’s largest producers of energy-efficient, resource-saving technologies, Siemens is No. 1 in offshore wind turbine construction, a leading supplier of gas and steam turbines for power generation, a major provider of power transmission solutions and a pioneer in infrastructure solutions as well as automation, drive and software solutions for industry. The company is also a leading provider of medical imaging equipment – such as computed tomography and magnetic resonance imaging systems – and a leader in laboratory diagnostics as well as clinical IT. In fiscal 2015, which ended on September 30, 2015, Siemens generated revenue of €75.6 billion and net income of €7.4 billion. At the end of September 2015, the company had around 348,000 employees worldwide. Further information is available on the Internet at www.siemens.com.