Grid security for intelligent power supply networks

The highest priority for operators of critical infrastructure, including electrical power supply grids, is to ensure a reliable, secure, and cost-efficient energy supply. 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 network optimization, and the inclusion of increasing numbers of consumers who are electricity producers. 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. Grid security has become one of the biggest and most important challenges for energy supply companies.

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 so as to incorporate the latest technologies and knowledge into its standards and products. A comprehensive security approach is routine in solutions from Siemens, integrating the following key factors:

- **Confidentiality:** for example, encrypted communication between individual devices and systems
- **Integrity:** for example, to protect devices against malware
- **Authentication:** for example, to protect against unauthorized access of local operation systems
- Authorization: for example, communication only with identified participants
- Data protection: for example, encrypted data storage with regulated access rights.
- Availability, the highest requirement for systems.

An appropriate security solution requires a comprehensive strategy. Siemens bases its solution on collaborations in partnership with energy providers and grid operators and on monitoring mechanisms that protect the network in various areas.

**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 people and processes. 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 can 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). Siemens also is technology partner of ENCS.

**Expanded 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 that can be incorporated in products and systems. This concept ensures increased protection against cyber attacks and reliable network infrastructure availability. The security architecture is based on a combination of different measures that are defined in the relevant global standards. Examples are IEC 62443, IEC 62351, and ISO/IEC 27000, which are also recommended by international regulatory authorities such as NERC (North American Electric Reliability Corporation). 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 rights. That’s why Siemens relies on a powerful authentication and authorization system in its solutions. Based on the principle of minimal allocation of rights, users are given only the access rights 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. Their central access management for SCADA systems (supervisory control and data acquisition) and a smart grid infrastructure that will also work interoperably in systems involving different manufacturers (multivendor systems) mean that 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 closely related to Siemens’ security patch management. This is a service in which Siemens experts draw on the company-wide Cyber Emergency Response Team (CERT) to search for new threats throughout the world and identify relevant security patches from third-party suppliers in order to create 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 used for critical infrastructure.

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 energy 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.

The Sicam CMIC small remote-control device for local substations operates using an integrated VPN (virtual private network) computer network based on IPsec (internet protocol security). HTTPS makes secure Web engineering possible. Additional Sicam CMIC provides assistance regarding RADIUS for the central management of users and roles for access authorization per web interface. Communication between the remote-control device and the Sicam Toolbox II configuration tool is also encrypted. A built-in crypto chip optimizes the encryption and saves the key material.

Smart grid remote-control unit for decentralized electricity generators: In collaboration with Sicam SGU, Siemens has marketed a communications-capable field device 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, electricity providers and municipal utilities can control and monitor decentralized electricity generation systems and consumers using the smart grid remote-control unit. Siemens manages the data security function required for all applications involving its new 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.

Integrated IT 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 encrypted to enable the necessary security. In addition, the protection devices are equipped with integration protection for the firmware that protects against
manipulation by third parties. The firmware contains a digital signature that is tested before it is loaded onto the device. A built-in crypto chip optimizes encryption in the Siprotec 5 protection devices and saves the key material.

**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. Role-based access control at the local Sicam SCC operating and monitoring system supports central management of user IDs and passwords via Microsoft Active Directory Server.

**IT security for industrial systems: Siemens energy automation solution certified.**
Siemens has had a typical energy automation solution comprising 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 as parts 2 to 4. The security standard certifies not just individual products and systems but also the entire energy automation solution – from product creation to engineering and commissioning through service and maintenance. With this certification process, Siemens satisfies its industrial customers’ desire for the products and systems used in their electricity supply solutions to comply with the latest IT security guidelines. Together with the German association for technical Inspection South, TÜV Süd, Siemens currently is working on an IEC 62443 certification as a further development of the WIB 2.0 certification.

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