SIEMENS

www.siemens.com/gridsecurity

Cyber Security

Global solutions for energy automation

Answers for infrastructure and cities.

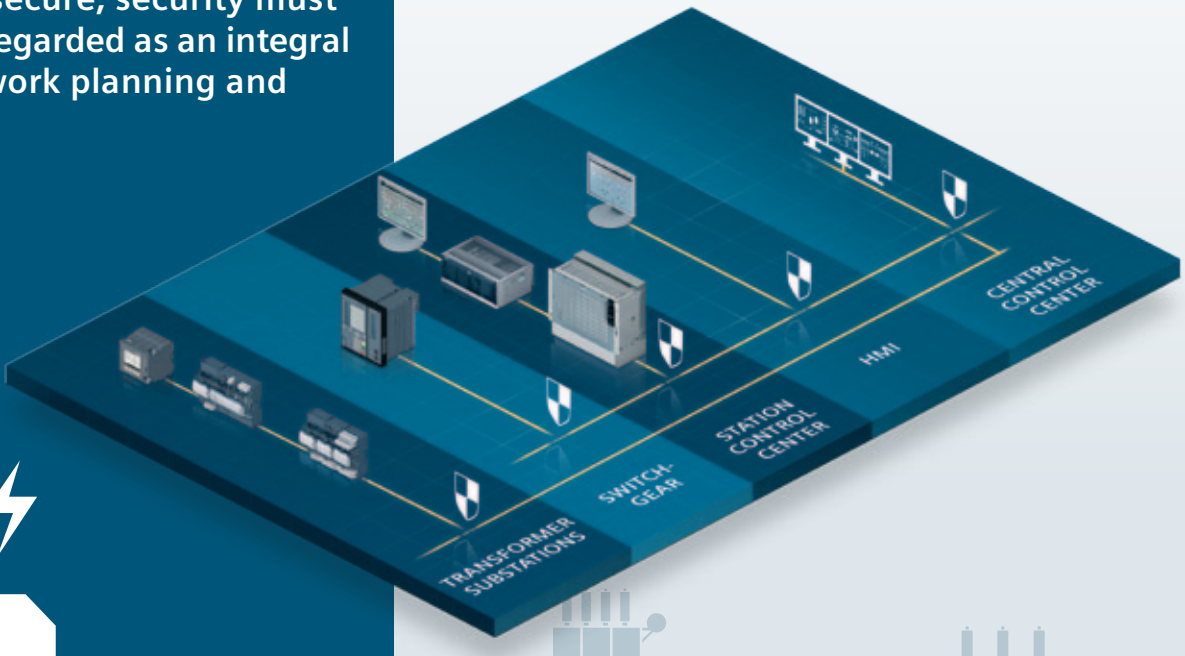
Cyber Security: Security from the very start

More and more, we are networking our systems and standardizing communication protocols and operating systems. And although these trends simplify processes and ensure efficiency in operation, they also leave our networks vulnerable.

How can we effectively protect the power supply against attacks? First and foremost, by planning security ahead of time. For a network to be secure, security must already be regarded as an integral part of network planning and design.

The best way to arrive at a complete, cost-effective system solution is by making security an integral part of the earliest planning stages. Such a solution integrates security into all phases of the development process. In the end, it includes precisely those security features that are absolutely necessary – no more and no less – thereby eliminating the need for expensive and time-consuming upgrades.

Siemens offers products, systems and solutions that are specially designed for energy automation. Right from the start, they meet the highest security requirements – including those of the BDEW white paper (German Association of Energy and Water Industries) and NERC CIP (North American Electric Reliability Corporation, Critical Infrastructure Protection).



Siemens Energy Automation: Security on every level

Our products: integrated security

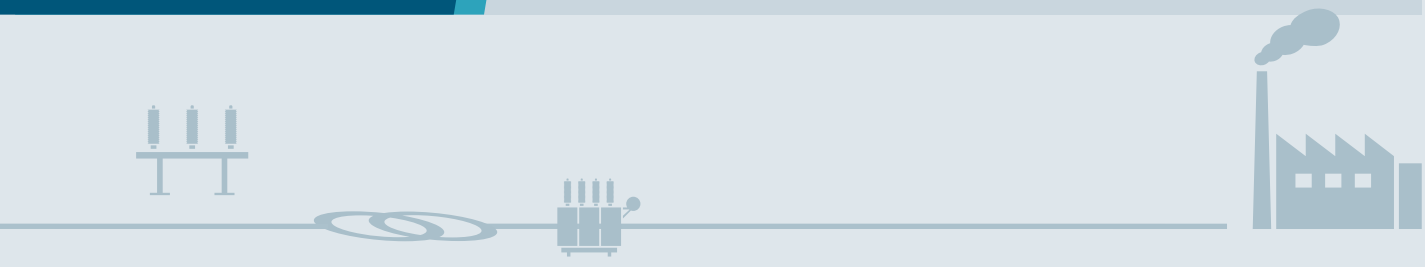
- Software and firmware integrity protection
- Encryption and secure communication
- Centralized user management support for station automation and local operator terminals
- Compliance with the IEC 62351 security standard

Our systems and solutions: end-to-end security

- Tested security architectures
- Recommendations for network components
- Security updates
- Virus protection

Our expertise and services: for security into the future

- Standardized patch management
- Contribution in the creation of international security standards such as IEC 62351
- Participation in national and international panels on security in the Smart Grid
- Secure development process
- Consulting services for everything relating to cyber security



Products, systems, and expertise: Security in every detail

Our products: integrated security

Strict guidelines have been established in the industry to increase security in energy automation systems. Siemens products support the implementation of these guidelines with effective and appropriate security functions that are integrated right from the start.

Access control

If you already have centralized user management with Microsoft Active Directory, you can simply integrate HMI systems such as SICAM SCC or station automation systems like SICAM PAS. You can quickly grant authorizations and modify or revoke them at any time, thus ensuring that only authorized persons can access your plant.

Our systems and solutions: end-to-end security

The more comprehensively IT security in energy automation systems is viewed, the more efficient and cost-effective the solutions will be. Siemens offers global concepts for an efficient security architecture in your plant.

Secure system design

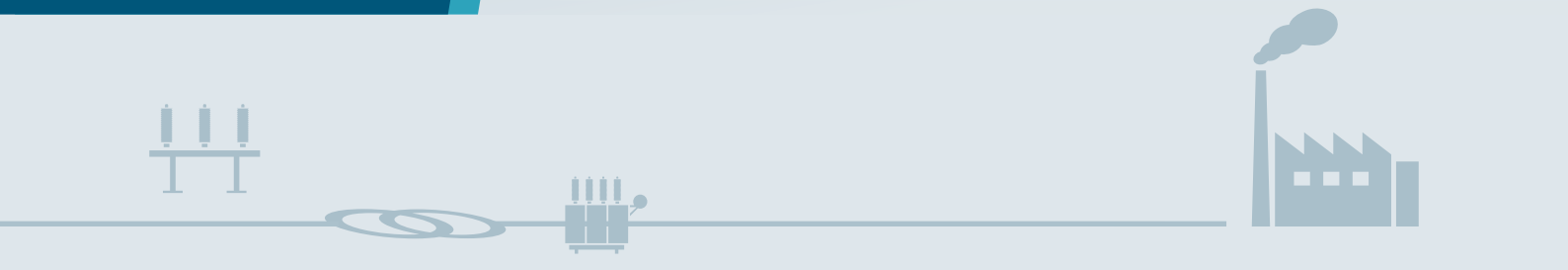
Thanks to many years of experience and worldwide expertise, our components, architectures, and safeguards have been thoroughly tried and tested. You can rely on our guidelines for securely expanding your infrastructure, or for "hardening" your system – in other words, eliminating all components that are not absolutely necessary. Last but not least, we advise

Our expertise and services: for security into the future

In order to stay ahead of the game in the field of IT security, Siemens employees undergo regular training. This means that the latest requirements are always taken into account in development. You can rely on our decades of experience.

Secure standards

Siemens shapes the industry. Our experts serve on national and international committees, drafting regulations and developing standards. This is where we bring our expertise to bear – for example, in the International Electrotechnical Commission (IEC) or the EU's Smart Grid Taskforce.



Secure authentication in DIGSI 5

Encrypted communication with SICAM PAS

Encryption and secure communication

Siemens systematically integrates information security into all automation and networking. Confidential data such as passwords are always stored in an encrypted form. We also protect communication using, for example, SIPROTEC 5 and DIGSI 5 parameterization software. The latest authentication methods ensure that protection devices accept only encrypted connections coming directly from DIGSI 5. In the other direction, the software unambiguously identifies the devices by a certificate. Nothing could be more secure.

From station automation to the control center and bay controllers – we also offer encryption to IEC 62351 for other communication channels in the power supply system. For example, in the case of SICAM PAS, the automation system optionally encrypted information via the IEC 60870-5-104 and DNP3i protocols.

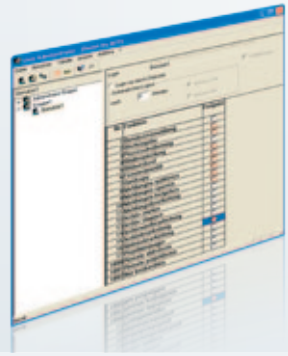
Firmware, software, and data integrity

Firmware files for SIPROTEC 5 or SIPROTEC 7SC80 contain a digital signature that the device checks each time a new firmware version is loaded. Thus Siemens ensures that only approved firmware versions are run – and effectively protects against manipulated or defective software.

you on current topics such as remote access to your plant. Here again, forward-looking security concepts are of primary importance.

Operational security

How to reduce security risks in daily plant operation? With a centralized approach, using the "principle of least privilege" to keep plant access to an absolute minimum. Siemens supports you in implementing a suitable user management system.



Convenient user management for SICAM SCC

Tailored consulting

How effective are your security technologies? Have individual components become outdated? What measures would make your plant more secure? Check your plant for security vulnerabilities on a regular basis. Siemens supports you – in this and in redesigning or reconfiguring your IT security.

Dependable services

Whether your automation and IT infrastructure is well-established or newly designed, it is unique. Siemens always plans and carefully evaluates the integration of a product from start to finish. To guarantee operational security over the long term as well, we offer a software and firmware update service. We also actively inform you as soon as we learn of new security vulnerabilities and security updates that are available for you.

Business continuity and disaster recovery

Arm yourself against the unexpected: The redundancy concepts of Siemens products and solutions guarantee that your plant will continue to operate when individual components or subsystems fail. We also assist you in developing disaster and recovery plans. Getting your plant up and running as soon as possible after a security incident occurs – that is our goal.

Published by and copyright © 2013:

Siemens AG
Infrastructure & Cities Sector
Smart Grid Division
Energy Automation
Humboldtstr. 59
90459 Nuremberg, Germany
www.siemens.com/gridsecurity

For more information,
please contact our
Customer Support Center.
Phone: +49 180 524 84 37
Fax: +49 180 524 24 71
(Charges depending on the provider)
E-mail: support.ic@siemens.com

Order No. IIC1000-G220-A164-X-4A00 | Printed in Germany | AL=N ECCN=N
Dispo 6200 | c4bs No. 768
HL 12127555 WS 01131.0