

Totally Integrated Energy Automation

Simplify your IT security

Think reliable



Power Transmission and Distribution

SIEMENS

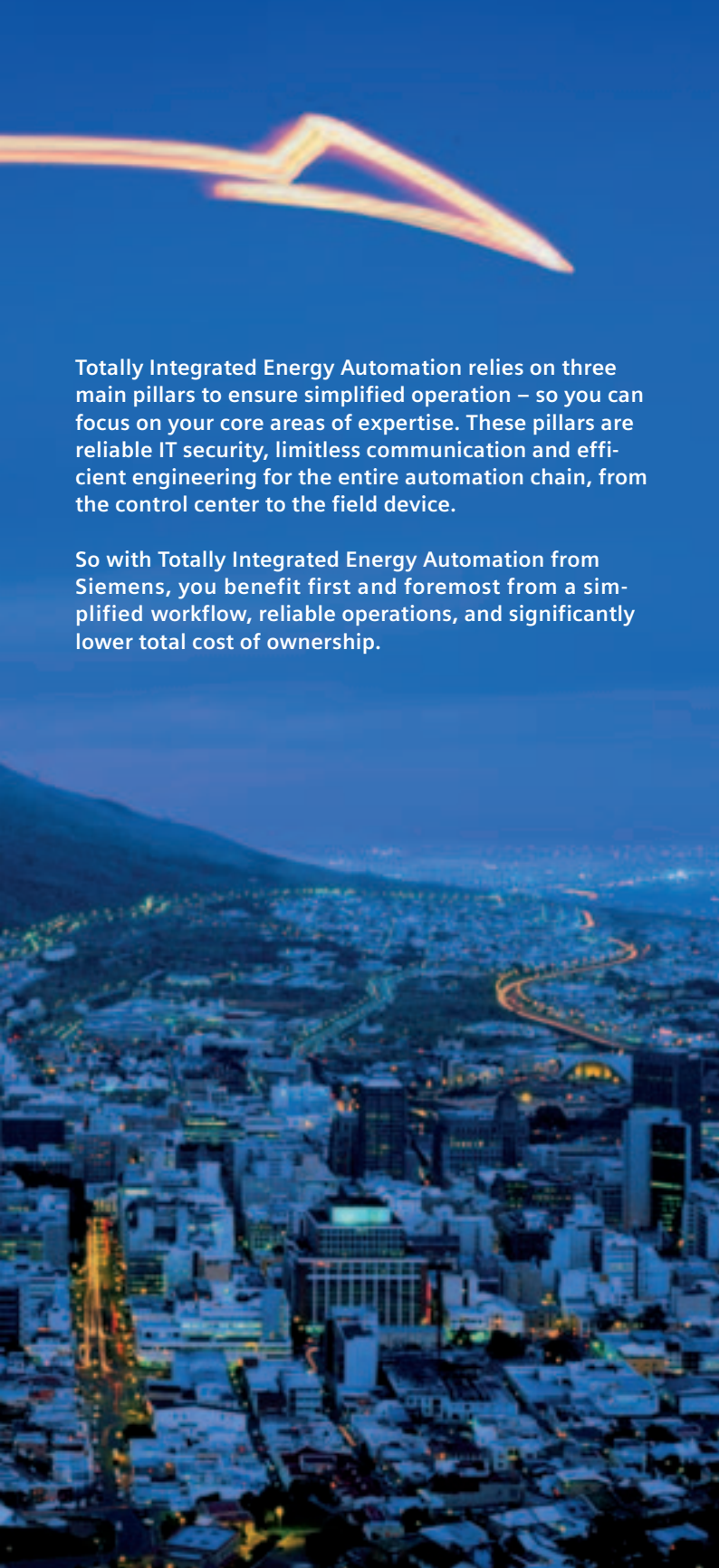
A man in a suit and glasses stands on a hillside at night, reaching his right hand towards a glowing, curved arc of light that stretches across the sky. Below him, a city is illuminated with lights, and mountains are visible in the background under a dark blue sky.

Reliable IT security for energy automation that simply works

Imagine your plant availability as an equation with many variables. One important variable is reliable IT security in the form of protection against unauthorized access, physical attacks, operator errors, or internal or external threats.

But what ultimately counts for you is the outcome – in the form of energy automation that simply works. And that's exactly the philosophy behind Totally Integrated Energy Automation. Our end-to-end solutions combine all the variables for you into a single transparent equation – to ensure maximum plant availability.

With Totally Integrated Energy Automation, we deliver an IT security concept that not only ensures the confidentiality and integrity of your data, but especially its availability.



Totally Integrated Energy Automation relies on three main pillars to ensure simplified operation – so you can focus on your core areas of expertise. These pillars are reliable IT security, limitless communication and efficient engineering for the entire automation chain, from the control center to the field device.

So with Totally Integrated Energy Automation from Siemens, you benefit first and foremost from a simplified workflow, reliable operations, and significantly lower total cost of ownership.










A view of your entire plant at all times

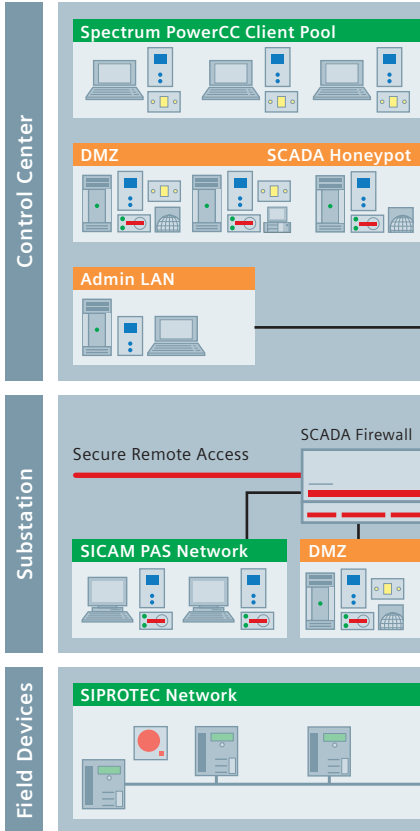
If you consider your plant as a whole, the individual parts resemble a chain. And when it comes to IT security, it's clear that your automation chain is only as strong as your weakest link. Totally Integrated Energy Automation delivers seamless IT security to ensure the continuous availability of your plant. Our holistic approach guarantees a universally high standard of security throughout the entire automation chain.

Zone-by-zone protection

The graphic representation of the security network, the so-called network blueprint, depicts the infrastructure and architecture of your plant. This is our basis for clear segmentation, which we use to precisely analyze the risk for every link in your automation chain, without losing sight of the effects on the plant as a whole.

We divide your network into manageable zones so we can equip them with precisely the right level of IT security – the level necessary and practical both for protecting the data in these zones and ensuring problem-free operation of the plant.

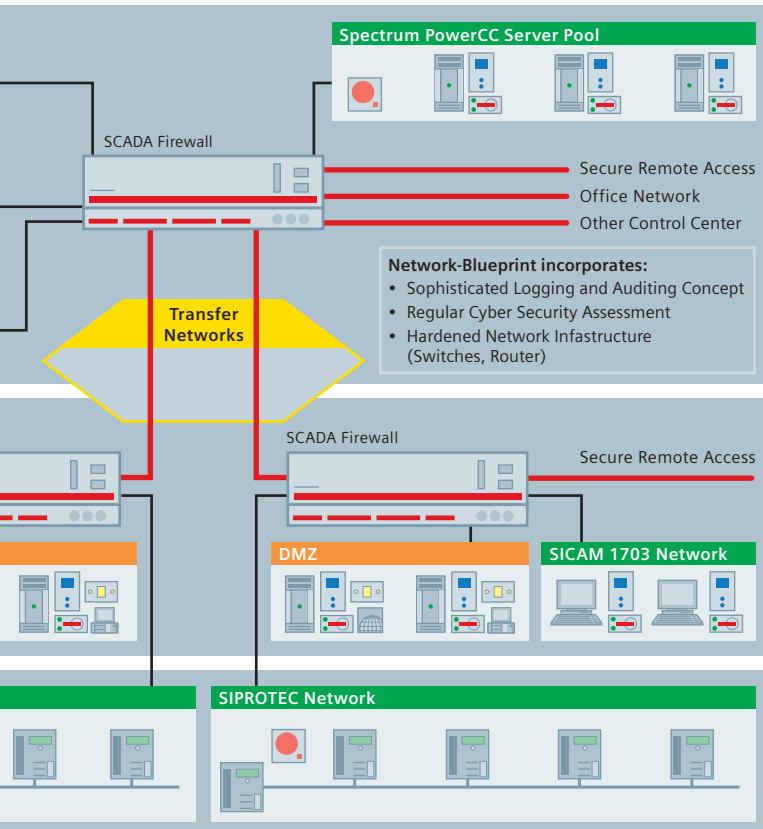
- Trusted Network 
- Semi-Trusted Network 
- Untrusted Network 
- Hardened Host 
- VPN Tunnel 
- Host-based Intrusion Prevention System 
- Network-based Intrusion Detection System 
- Web Server 
- Anti Virus 



End-to-end security among all interfaces

With the spread of the Internet and increasing networking at your plant, today every interface poses a potential IT security risk. You need a simplified way to assess these risks. So with Totally Integrated Energy Automation, Siemens pursues an IT security philosophy that simply offers you protection.

To achieve this, we rely especially on homogenization through standard, transparent processes for authentication, authorization, intrusion detection and prevention, malware protection, effective patch management for 3rd-party components, standardized logging, and continuous security tests.



Continuously hardening applications

Secure products are the essential foundation for a secure network. That's why we continually harden our applications against attacks and weak points. We do this through individualized risk analyses and regular tests, including specific tests for 3rd-party components, with a defined package of IT security test programs designed to identify weak points (test suite).

In-house CERT as an expert partner

Siemens has its own in-house Computer Emergency Response Team (CERT). An organization of this kind that discusses IT security-critical topics and issues up-to-date warnings is usually only operated by universities or governments for the information of users across the industry. Our in-house CERT has been in existence for 10 years, during which it has issued warnings about security risks and offered approaches for solutions that are specifically geared to the company's areas of expertise.

In its capacity as an expert partner, the Siemens CERT creates rules for secure coding and programming of our products, for example, and continuously further trains our programmers. The CERT carries out deliberate hacker attacks to assess the products for weak points. And the team also collects and distributes reports on weak points and upgrade notifications for 3rd-party components and links them to recommendations, concrete proposals and implementation regulations.

This institution gives us an important advantage in terms of expertise – from which our customers can also benefit. And the best testimonial for our CERT is the solid IT security of the Siemens global corporate network.

With Totally Integrated Energy Automation, we consider your plant as a whole





By continually hardening our products, we ensure a seamlessly high standard of IT security

Applying standards effectively

Standards are designed to offer you quality, increased long-term IT security and investment protection. There are hundreds of IT security standards now in existence, but only some of them are really necessary and useful for your plant.

Drawing on our many years of experience in the market, we can select the standards and guidelines that protect your network reliably and effectively from the many different security standards available. That includes advising you on which IT security standards you need to comply with both internationally and at regional level.

As a global company represented in approximately 190 countries, we have extensive expertise and experience, accumulated over many years, with different IT security regulations and standardization measures at the international level.

Risk analyses: facing the challenges

An important first step for successful IT security management is the assessment of existing security risks.

We register and evaluate these risks with individualized risk analyses. Using these analyses, we classify the risk potential and develop corresponding recommended actions for you. In the security concept, the measures must be matched to the value of the data to be protected. If there are too many measures, the result is high costs and lack of flexibility, while too few measures leave open major security gaps.

Our risk analyses offer you a transparent, informative and complete comparison of risk and costs, giving you the best-possible basis for deciding on further measures.



Implementing an “IT security gene”

Our goal is permanent, long-term IT security for your plant. That’s why secure products and infrastructures alone are not enough. With Totally Integrated Energy Automation, Siemens implements the needed security procedures to ensure that IT security is fully established end to end, and guaranteed throughout the plant’s entire life cycle.

IT security grows in the development process

The holistic approach of Totally Integrated Energy Automation means more than just keeping an eye on your entire plant. For us, complete IT security also means that the security of our products is already integrated in the complete development process – and not just later in the test phase.

IT security guidelines for development, handling of processes, service and other functions ensure that IT security is a continuous part of all processes. Examples of this include security briefings for product management before a product is developed or programmed in the first place. Programmers work according to defined guidelines for secure coding, as stipulated by the Siemens CERT. For effective patch management, updates of 3rd-party security products such as firewalls are

Our products are certified according to carefully selected IT security standards



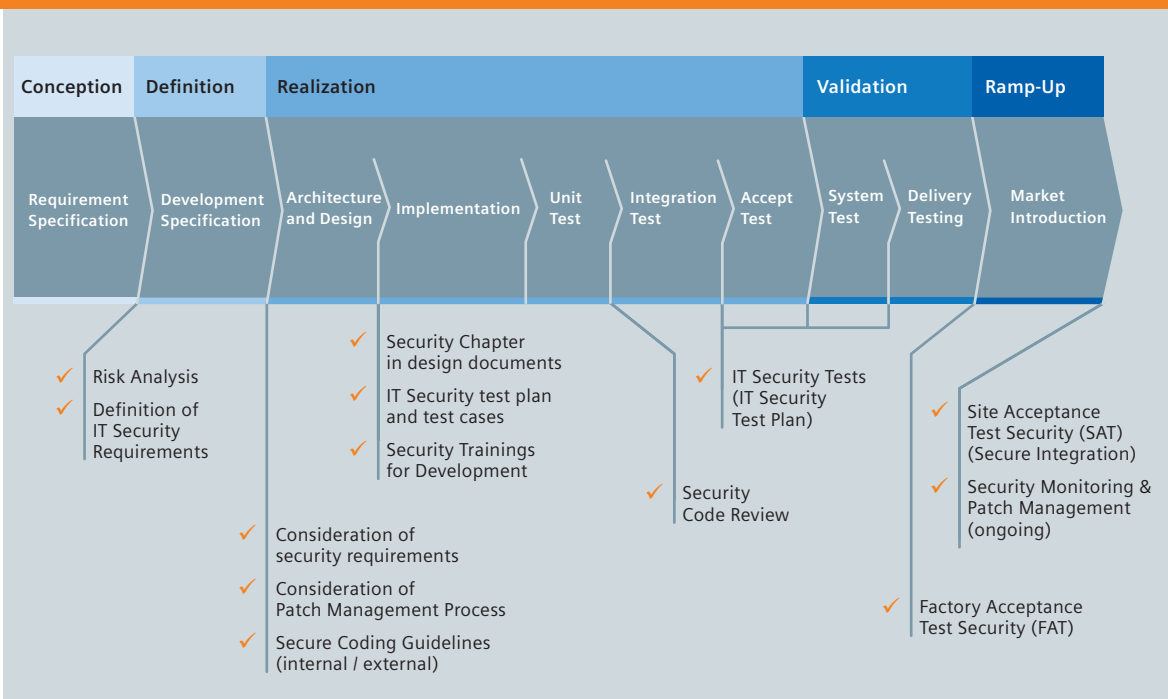
already tested during the development process for our products. Continuous penetration tests of all relevant products are specified in a test plan. And these steps also include defining and creating a security test environment and suitable test cases.

With these measures, we subject our products to an objective and critical certification process that allows us to ensure and control IT security on the basis of suitably selected standards. As a result, the IT security of our products is always reproducible and transparent, and naturally is continuously being improved.

Integrating IT security into your daily operations

The security of a plant directly depends on how securely the operator handles it. And a high level of security can only be achieved through close cooperation between the manufacturer and operator.

We’ve observed great potential for optimization in plants when security concepts are implemented continuously in the daily plant operations. For this, too, we support you with our extensive experience, advising you, for example, on the selection and evaluation of 3rd-party components.



IT security is an integral part of the entire development process

We offer a very wide range of helpful tools that allow users to benefit from IT security as a standard part of the daily operations at their plant. We implement standardized security processes, for example, for updates and system backups. At the same time, we provide you with efficient tools for administering access in your plant network. This includes effective management of rights as well as secure logging tools. Automatic compiling of logs or creation of log files are not only legally mandated – they can help determine at a later time how damage to a system came about.

The principle of simplicity and transparency

Naturally, these are only a few of the services we provide. With Totally Integrated Energy Automation, Siemens offers holistic solutions – intelligently coordinated and harmonized – for energy automation. Only a company like Siemens has a complete portfolio of perfectly matched solutions, and the expertise, to see the bigger picture while highlighting just those parts that are important for you.

With Totally Integrated Energy Automation, we always follow the principle of simplicity and transparency, because guidelines and standard processes are the best basis for IT security. This reduces operator errors and thus safeguards the availability of your plant in the long term.





For you, energy automation with Siemens means...

- you benefit from the experience of the largest installed base in the world,
- you are able to contact us quickly – we have representatives in approximately 190 countries,
- we keep you on the cutting edge of technology with our innovations in research and development,
- you can select from a comprehensive range, from single product to turnkey solution,
- you can simply focus on your core areas of expertise.

An aerial night photograph of a city, likely San Francisco, with its lights glowing against a dark blue sky. Overlaid on the image are several bright, glowing orange and yellow light trails that form a large, abstract, looping shape in the upper half of the frame. The text 'Your contact for Totally Integrated Energy Automation' is centered within this shape. Two thin red lines point from the text towards the light trails.

Your contact for Totally
Integrated Energy Automation

Siemens AG
Power Transmission and Distribution
Energy Automation
P.O. Box 48 06
90026 Nuremberg
Germany
www.siemens.com/energy-automation

For more information, contact our
Customer Support Center.
Phone: +49 180/524 70 00
Fax: +49 180/524 24 71
(Charges depending on provider)
E-mail: support.energy@siemens.com
www.siemens.com/energy-support

Order No.: E50001-U300-A112-X-7600
Printed in Germany
Dispo 06200
6100/6985 SchöDM 102834 WS 11073.0

The information in this document contains general descriptions of the technical options available, which do not always have to be present in individual cases.
The required features should therefore be specified in each individual case at the time of closing the contract.