Cyber Security for HVDC & FACTS

Cyber Security Services

Introduction

Cyber threats are increasing with serious consequences for companies and communities worldwide. Critical infrastructure like power transmission systems become increasingly the focus.

Information technology (IT) systems are the foundation of all of today's critical processes in most companies. This leads to significantly increased risks of being attacked by hackers or viruses. There can be serious consequences if these attacks result in data loss, the theft of confidential data, or even a complete system failure.

At the time of installation the system has by design a high level of security. Yet cyber security is not a onetime task. It is an ongoing endeavor during the complete systems life time to constantly fight new cyber threats and continuously keep the system security on a high level.

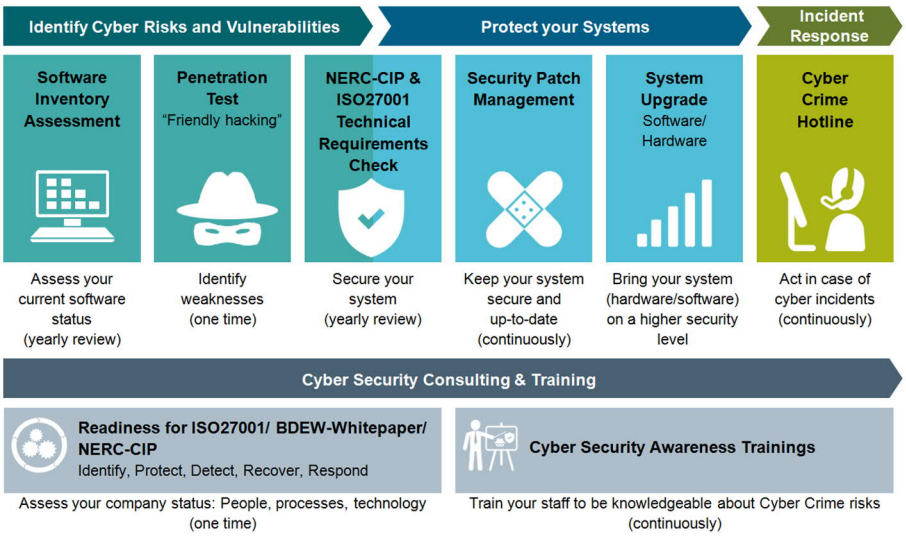
Features

Siemens has developed a comprehensive cyber security service portfolio for HVDC and FACTS to support customers.

1. Identify cyber vulnerabilities
   - Software Inventory Assessment: The basis for any effective cyber security activities is to know the installed software
   - Penetration test, sometimes called "friendly hacking", helps to reveal security weaknesses from a simulated hacker perspective
2. Protect your systems
   - The "technical requirement check" comprises many technical security aspects including system hardening, defense-in-depth, malicious code prevention (anti-virus software), secure event monitoring & central logging, system access control & account management, remote access, backup & recovery, and further topics
   - Security Patch Management: Identifying, tracking, testing and implementing a security patch management program
   - System upgrade: When software reaches end of life time
3. Respond to cyber incidents
   - Cyber crime hotline with support from Siemens cyber experts when cyber incidents happen
4. Consulting and training
   - Consulting for implementation of international cyber security standards
   - Cyber security awareness trainings

Benefits

The cyber security services for HVDC & FACTS support system operators in their effort of professionally managing security vulnerabilities and keeping their systems continuously on a high security level.



Cyber Security Service Portfolio for HVDC and FACTS

Security Patch Management
Keep your system updated and protected

Security Patch Management
A security patch is a piece of software designed to resolve security vulnerabilities in systems. Security patches may be released during the complete life cycle of the software.

It is important for system operators to know about existing security patches in order to evaluate and mitigate the associated security risks. Testing and installing security patches is an important element in closing existing security vulnerabilities. Security patch management is essential for effective cyber security.

Scope of delivery
The Security Patch Management service is built up in three levels and helps the customer to keep the software secure:

- **Bronze:**
  Monthly newsletter on available security patches relevant for customers' systems; information only, no testing
- **Silver:**
  Testing of security patches - on the Siemens generic testbed and/ or on a customer specific replica
- **Gold:**
  Installation of tested security patches on site of the operational system during scheduled yearly outages

The three levels build up on each other. The silver level includes the bronze level service. Gold includes both silver and bronze levels.

Technical details of testing
According to international standards and best practices, security patches should be evaluated and tested in a test environment.

Siemens has developed a generic HVDC and FACTS baseline testbed which is used for testing of security patches. The testbed provides an efficient way of testing the software compatibility. Customers will be regularly informed about the testing results.

While the generic testbed comprises typical baseline system configurations, the generic testbed setup does not include all customer specific system configurations. Customers interested in having tests performed on an exact system environment need a customer specific replica. A replica is a copy of the operational HVDC/FACTS system components. Siemens then performs the tests on the customer specific replica. If the replica is located at the customer's premises it can also be used by the customer for additional purposes like trainings and system operation simulations.

End of life time of software
After the end of life time of the software typically no security patches are issued by the software vendor. In that case a system modification or upgrade to a current software version should be considered to be able to continuously ensure the security of the system.

ISO27001 Certification
ISO27001 is a leading international standard for information security management systems. Siemens Customer Service at the EM division in Erlangen, Germany has received the ISO27001 certification since 2017.

Siemens
Gas and Power GmbH & Co. KG
Service Power Transmission
Humboldtstr. 64
90459 Nuremberg, Germany

Customer Support Center

Phone: +49 (911) 433 78 78
E-Mail: support.energy@siemens.com