A HOLISTIC APPROACH TOWARDS A SECURE POWER SYSTEM

# Cybersecurity Consulting

## At a Glance

Local governments around the world are taking regulatory action against the prevailing threat of cyber security attacks. To give but one example, the German IT Security Act was issued on June 12, 2015.

The rising need for protection against potential cyber security attacks arises from an increased interconnection of operational technology (OT) as well as growing demands with respect to data processing supported by the integration of the operational technology with information technology (IT).

The term critical infrastructures designates organizations or institutions with high importance for their communities. Outages or disturbances affecting these critical infrastructures will lead to lasting shortages of supply, significant impact on the society and economy.

In Germany, operators of critical infrastructures are obliged to follow legal requirements such as the IT Security Catalog, which requires the implementation and certification of an Information Security Management System (ISMS) and taking appropriate measures to protect critical infrastructures.

## The Challenge

The protection of a power system has different priorities compared to traditional IT environments. In IT, the highest priority is always on confidentiality. In operational technologies, availability is more relevant. A system must be available in order to protect systems and humans from harm at any price. With the merge of operational technology and information technology, the power systems are facing risks from known and new threats.

SIEMENS

A cyber-attack against these infrastructures can have severe consequences for the system operator:

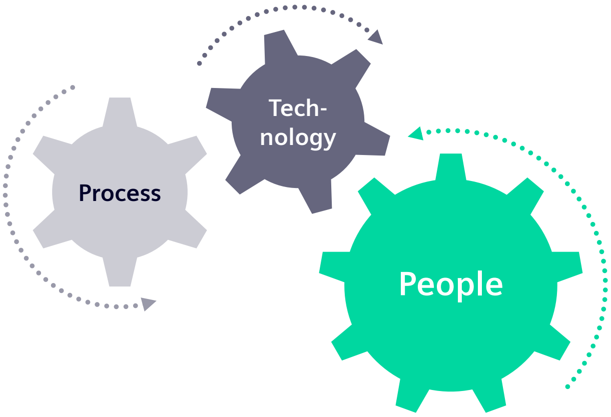
- Human harm or loss
- Degradation or disruption of operation
- Breaches of legal or contractual requirements, financial loss
- Loss of know-how or licenses
- Loss of reputation, customers and market share

An Information Security Management System defines rules and processes for steering, controlling, maintaining and optimizing cyber security within an organization, but it does not clearly define which aspects should be covered in a protection concept and how it can be applied to an operational environment such as a substation.

## Our solution:

Siemens' consulting approach considers all elements of a company:

- **People**
  Awareness and understanding of cyber security needs and requirements
- **Processes**
  Requirements regarding products/systems, operations and organization, covering the complete life cycle
- **Technology**
  Supports the fulfillment of processes and achievement of the protection goals: availability, integrity, confidentiality



As people work with processes, supported by technology, any security assessment needs to consider all of these three elements.

The methodology used in Siemens' consulting approach is based on the NIST framework which follows international security standards and recommendations (IEC/ISO27k, IEC 62443, BDEW Whitepaper, NERC-CIP).

Applying this methodology to a power system operator, the following cyber security functional areas are relevant:

- **Identify**
  Understanding the business context, the resources that support critical functions and the related cyber security risks
- **Protect**
  Protection of critical infrastructure services, e.g., energy supply by safeguarding the critical assets of an overall system
- **Detect**
  Identification of occurrences of cyber security related events
- **Respond**
  Taking action against the detected cyber security related event. It supports the ability to contain the impact of a potential event
- **Recover**
  Creating plans for resilience and restoration of business essential services that were impaired due to a cyber security incident

Our consulting approach is based on the well-proven Compass® method by following a clearly structured process. Results can be derived quickly. These results are the basis for creating high customer value.

The Compass method includes the following phases:

- **Orientation:**
  Comprehensive and objective analysis of the current security status in the process environment
- **Destination:**
  Definition of the aspired security level and proposition of concrete measures
- **Routing:**
  Roadmap including profitability analysis and recommendations for implementation
- **Navigation:**
  Continuous customer support during the implementation of security measures

The approach and the methodology are applied with the domain knowledge of Siemens experts working in the energy management domain. This guarantees that appropriate measures are defined and applied during the process.

The Compass method includes the following phases:

- **Orientation:**
  Comprehensive and objective analysis of the current security status in the process environment
- **Destination:**
  Definition of the aspired security level and proposition of concrete measures
- **Routing:**
  Roadmap including profitability analysis and recommendations for implementation
- **Navigation:**
  Continuous customer support during the implementation of security measures

The approach and the methodology are applied with the domain knowledge of Siemens experts working in the energy management domain. This guarantees that appropriate measures are defined and applied during the process.

### ISMS implementation example

An Information Security Management System (ISMS) defines the principles and rules within a company to achieve consistent information security.

The first step in implementing an ISMS, is to understand the business context and to identify the critical business processes and assets.

Based on gap and risk analysis, a protection concept and implementation plan has to be carried out where associated business risks are addressed in all NIST functional areas.

**Published by**
**Siemens AG**

Smart Infrastructure
Grid Software
Humboldtstrasse 59
90459 Nuremberg, Germany

For the U.S. published by
Siemens Industry Inc.
100 Technology Drive
Alpharetta, GA 30005, United States

For more information, please use our web contact form.

SIGSW-B10034-00-7600
AL=N, ECCN=N

Subject to changes and errors.

The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations may be trademarks or product names of Siemens AG or other companies whose use by third parties for their own purposes could violate the rights of the owners.