IT security
in telecontrol technology
Why security is more important now than previously

Coordinated cyber attacks on station technology are no longer merely construed horror scenarios, but instead are already part of our reality. For the supply network operators, this state of affairs entails enormous risks for both supply stability and the possible associated claims for damages, as well as for their public reputation. Strong enough reasons, therefore, to focus on information security today rather than tomorrow.

But what specifically does this mean? An optimally protected system preserves the confidentiality, integrity, authenticity and availability of data and information and prevents unwanted interventions. However, the challenges that IT experts face in attempting to ensure this are growing steadily: The attackers are becoming more and more professional, legal requirements are becoming increasingly specific, and – last, but not least – different interest groups have to be taken into account. Notwithstanding the required increase in security, the practicability of the systems for operating and maintenance personnel also always needs to be kept in mind.

Ideally, therefore, a supply system is based on a network infrastructure that allows both secure connections with strong encryption and high functionality and convenience for everyday business applications. A future-proof infrastructure must also be able to provide continuous and detailed monitoring in order to identify risks and derive protection measures. The practice-oriented solution to this challenge can only be a holistic security concept that enables continuous further development and updating.

Basic concepts of IT security

In order to gain a fundamental understanding of the different threat scenarios as regards IT security, the basic concepts should be explained. Four aspects are key here:

1. **Confidentiality**
   - No unauthorised persons may read the data

2. **Integrity**
   - Unauthorised persons may not change the data

3. **Authenticity**
   - The data really does come from the assumed source

4. **Availability**
   - Access to the data must be guaranteed for authorised persons
**Powerful hardware - series5e**

With its improved immunity and isolation concept, the series5e product family is already able to skilfully handle the complex current and future security and practical requirements. The continuously increasing demands on IT security measures are leading to a significant increase in the performance requirements for components. Each net-line product with series5e technology offers higher performance thanks to the 32-bit RISC processor with floating point unit and 1GB memory: Running at 1,200 MIPS, the hardware is three to five times more powerful than the previous series5+ generation. The improved performance has a positive impact in particular on network communication via IEC 61850 and process point treatment according to IEC 60870-5-10x standards, and also enables the use of state-of-the-art encryption algorithms. The overall system was based on a modern Linux kernel which allows for greater flexibility and easier maintainability of firmware, especially with respect to IT security.

**setIT configurable software**

Advanced security functions have been seamlessly integrated into the user interface of our setIT configurable software:

- The default settings of new stations now default to the secure protocols FTPs/HTTPs
- User management with individual role based access control (RBAC)
- Access to service functions in the station can be temporarily activated via a system command from the control centre
- The station configuration can be encrypted using a project-specific system password.
- VPN encryption via IPsec with IKEv2
- The new database format .sdbx allows the entire project database to be encrypted
- Simple definition of advanced firewall rules: Services are granularly activatable and can be limited to various network interfaces
- Number of possible process data for FW-5000, FW-50 and BCU-50 increased to 20,000 (series5e)
- Central recording of security-relevant operating events with SYSLOG
- Back-up function with freely selectable storage location for saving configuration data

**Thorough testing**

In order to verify the effectiveness of our ongoing improvements in the area of IT security, we have our telecontrol systems checked by external specialists at regular intervals.

GAI NetConsult GmbH recently carried out a check to ensure that the requirements of the BDEW Whitepaper are met. The result:

‘From the point of view of IT security, there are no concerns with respect to the tested units in the tested configuration for productive use in networks with increased security requirements.’

**Selection of services and functions in setIT**

FW-5-GATE-4G with series5e technology

Firewall with connection settings via VPN in setIT
Our IT security expert Markus Dewerny has been with SAE IT-systems since 2002. Previously, he was a client himself. As a former project engineer, he not only knows the systems and technology inside out, but also understands the concerns and problems of the clients at first-hand. In 2017 he took over the position of Information Security Officer at SAE to advise and train customers on security issues. In coordination with the IT-EDV department, he also coordinates our administrative security, such as measures to secure our IT systems and the data transfers to and from third parties.

### Internal IT security: ISMS

In addition to requirements-based hardware and software products, SAE also offers all key services, from project planning to system commissioning. Since IT security calls for a holistic view of all system components, processes and framework conditions, our security-related consultancy prior to a project is an effective and efficient investment. Typically, the following will be covered/provided:

- **Superordinate, conceptual advice**
  
  Questions in this context:
  - How can a network be sensibly planned and set up?
  - How do measures in the network harmonize with measures taken outside the network?
  - How are access restrictions set up?
  - How should networks be segmented?
  - How is the connection to the control centre secured?

- **Advice on technology's actual security mechanisms**

  Clarification of specific questions, for example:
  - How strong can the encryption be set?
  - Which transmission procedures or encryption algorithms are supported?
  - How does the firewall work in the units?
  - How can it be ensured that assigned passwords are secure?
  - How can a sensible path between usability and security be found?

The last question in particular poses great challenges for our clients and can only be answered individually. In the past, the main focus was on functionality, and security matters were of secondary importance. Today, there must be a reasonable balance between function, handling and security, taking into account the legal requirements, the recommendations of the German Federal Office for Information Security (BSI) and the current risk situation.

### Internal IT security: ISO 27001 certification

As a supplier for operators with critical infrastructures, we are taking the threat of hacker attacks seriously. To further increase security, we have decided to seek, with the help of our International Chamber of Commerce-approved Information Security Officer and external security experts, ISO 27001 certification.

### What role does telecontrol play in the security of your network infrastructure?

Telecontrol and substation automation technology is often located at central points of the communication network. The units have different interfaces to other services and manufacturers, to different components and to the physical process. Transmission is also often to different control centres run by several operators. Telecontrol technology is therefore always part of an overall system.

What is key in information security is knowing the following: ‘**A chain is only as strong as its weakest link.**’

Two core challenges derive from this:

1. **It is always necessary to consider the entire network with all its components, physical conditions and processes in operation.**

2. **Each individual component (including the telecontrol technology) must meet the required security level.**

With these requirements in mind, we are continuously developing our hardware, software and related services in order to provide our customers with secure and practical solutions.

### IT security in telecontrol technology

Telecontrol and substation automation technology is often located at central points of the communication network. The units have different interfaces to other services and manufacturers, to different components and to the physical process. Transmission is also often to different control centres run by several operators. Telecontrol technology is therefore always part of an overall system.

What is key in information security is knowing the following: ‘**A chain is only as strong as its weakest link.**’

Two core challenges derive from this:

1. **It is always necessary to consider the entire network with all its components, physical conditions and processes in operation.**

2. **Each individual component (including the telecontrol technology) must meet the required security level.**

With these requirements in mind, we are continuously developing our hardware, software and related services in order to provide our customers with secure and practical solutions.
**Practical solutions**

Secure connections, high user-friendliness, ongoing security analyses – on the basis of these requirements, we have developed a comprehensive security concept that enables practically-oriented further developments:

**System autonomy and transparency**

In a network dependent on external services, network security is not entirely in the hands of the user. When dependencies are reduced, this not only increases the autonomy of the network but also its security. Our clever solution is to use an in-house NTP server for time synchronisation as an alternative to an internet service. In addition, our security concept provides for the continuous and detailed monitoring of the network infrastructure with regard to stability changes, accesses and access attempts. To this end, the telecontrol technology sends relevant data to a Syslog server, which enables the central recording of the operating events of many stations and the evaluation of these messages. Depending on the type and the equipment of the Syslog server, alarms may be generated to report, for example, a high number of incorrect password entries, an update outside operating hours or other unusual events. These observations can be used to derive the causes of current stability fluctuations and to quickly identify potential hazards.

**Connectivity options for telecontrol**

Our security concept recommends a VPN gateway as the connecting component. This enables the central control of many stations via just one telecontrol master station. Our telecontrol components allow various connection techniques, such as the use of any internet connection, an external router, as well as a cellular or LAN connection. We also recommend redundant connections to secure the connection. We design solutions for utility companies with different requirements. Therefore, various products can also be integrated into the security concept on the hardware side: for example, the field device types net-line FW-5, net-line FW-50 and net-line FW-5-GATE-4G shown here. Thanks to series5e technology, these products have been converted to a new, future-proof platform.

**VPN, encryption and firewall**

A secure connection requires a secure VPN encryption protocol and a mechanism for key exchange. IPsec can be activated in the setIT configurable software both on protocol version 1 (IKEv1) and on protocol version 2 (IKEv2), described in RFC4306. It should be noted that it is not only the stations on site that should be protected against external accesses of any kind, but also the configuration database itself. The new database format .sdbx enables the encryption of the entire project file with the secure AES-256 algorithm. This encryption is also recommended as security by the BSI for cryptic processes. setIT also allows the further definition of advanced firewall rules, with certain services able to be activated as well as limited to different interfaces. It is also possible to make precise settings that allow more flexibility. In summary, our concept allows diverse and secure connection options via VPN and a high degree of functionality. The security of our clients and the supply networks has spurred us on to supplement our portfolio with security-related advice and to develop this security-optimised connecting concept.

© SAE IT-systems GmbH & Co. KG Subject to technical modification.
IT security in telecontrol technology