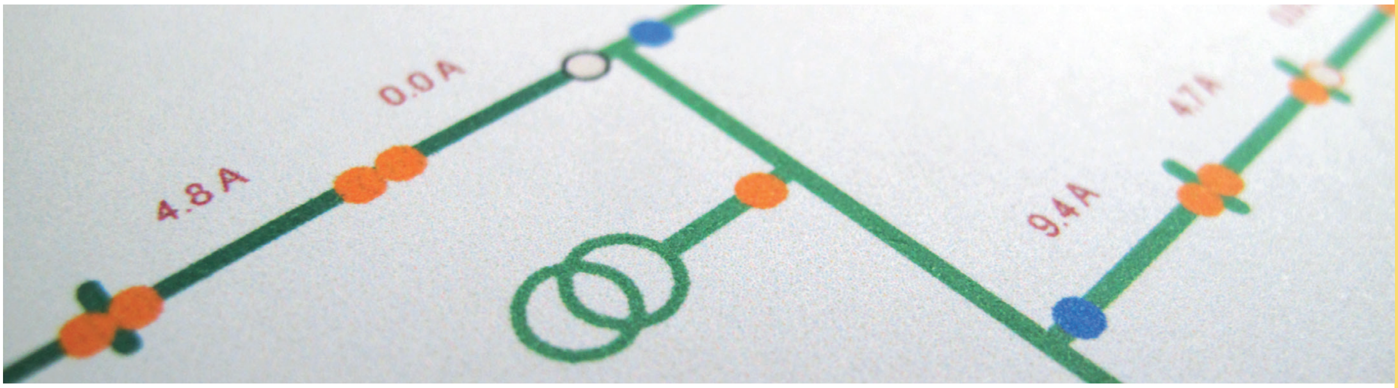
VIVAVIS

DECODING THE FUTURE



IT Security in Network Control Centres

Always on the safe side: with solutions and services from VIVAVIS

VIVAVIS services for IT security – Protection for your power grids according to EnWG
Have you made an analysis of your IT systems‘ weak points yet? The answer is “No“? Then it’s high time you did!

According to the German Energy Act (EnGW), § 11 section 1a, “telecommunication and electronic data processing systems must be suitably protected against threats.” In this context, the Federal Network Agency (BNetzA) has issued a catalog of security requirements.

We support you in the introduction of the IT security catalog and offer you ready-made solutions for the implementation of the stipulated measures in accordance with DIN ISO/IEC 27002 and 27019.

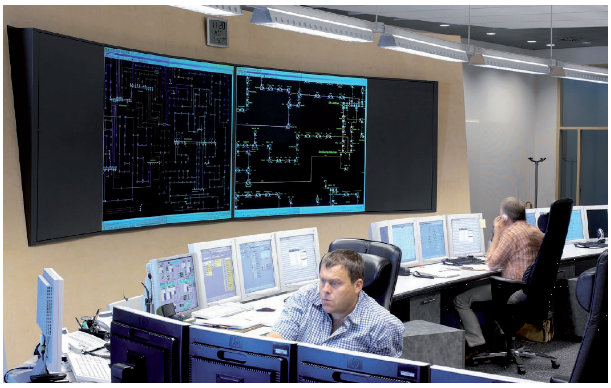
Services from VIVAVIS
Based on the recommendation of the BDEW white paper and the respective standards from the ISO 27000 series, our group member, Systema Gesellschaft für angewandte Datentechnik mbH, runs an IT security check for your control centre. This security check focuses particularly on the central IT systems.

The resulting report includes an assessment of the security status and a customer-specific catalog of measures to eliminate vulnerabilities.

VIVAVIS Products: Security from a single source
VIVAVIS products and the internal development and maintenance processes ensure a high degree of security with a view to the demands of the BDEW white paper.

This was recently confirmed by an assessment made by a renowned IT security firm.

For instance, the **VIVAVIS HIGH-LEIT SCADA** system (versions 2013 and later) automatically creates the user roles Administrator, Auditor, Operator and Data Display during installation.

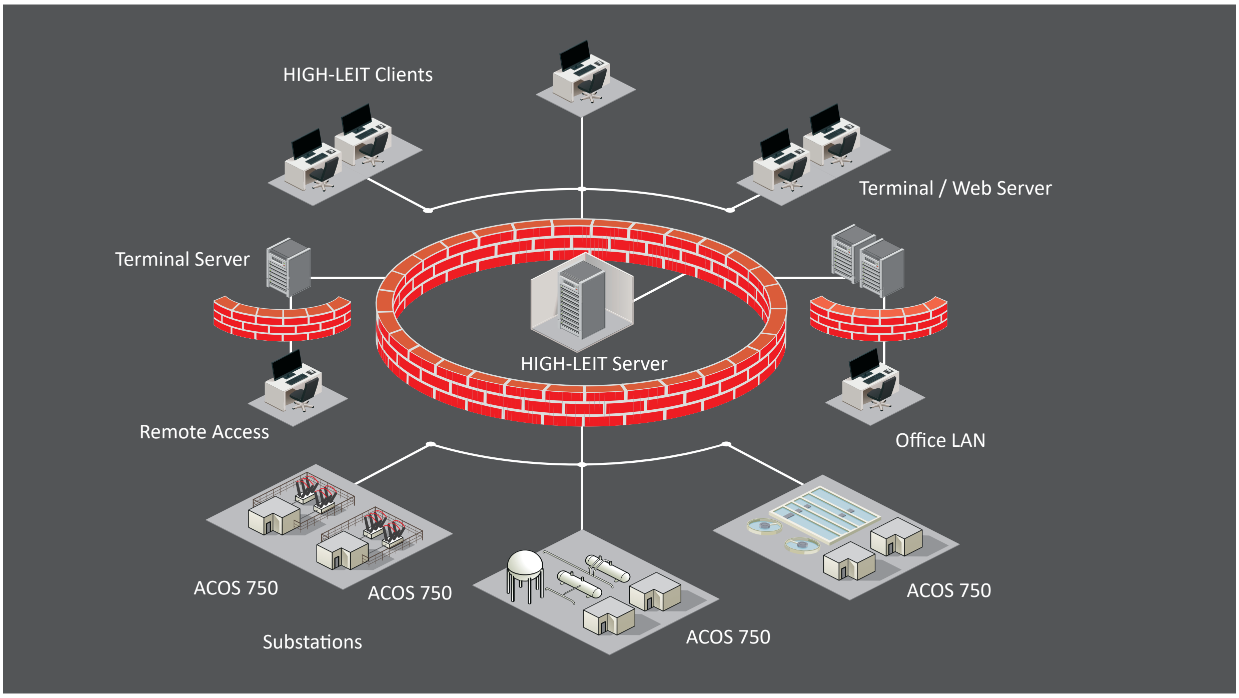


A password policy ensures the strength and validity of passwords. All securityrelevant incidents are stored in a separate Event Log and can be transmitted to a central alarm management by means of Windows Eventlog.

The RTUs of the ACOS 7 series can encrypt all communication links (end-to-end encryption) by means of a certificate-based OpenVPN. Ethernet services and ports that are not required can be deactivated in the RTU. Additionally, it is possible to integrate a dynamic firewall.

The ACOS ET engineering tool supports the following user roles: Administrator, Auditor, Operator and Data Display. Moreover, ACOS ET carries out an integrity check of all project files and stores them in encrypted form.

All security-relevant incidents are recorded in the ACOS ET Event Log and can be stored (optional) in Windows Event Log.



The VIVAVIS Basic Package
To upgrade your VIVAVIS HIGH-LEIT SCADA system to an up-to-date security level, we offer you a basic package which includes the following services:

- Central Windows server update service for the distribution of operating system patches
- Basic hardening of all servers and desktop computers
  (Windows 2008 Server R2/Solaris 10 or Windows 7, or later)
- Configuration of Windows BitLocker for hard disk encryption in mobile terminals
- Configuration of IPSec encryption of the communication between the MMI and the server
- Basic hardening of all network components (deactivation of unused ports, port security)
- Change of default passwords for BIOS, operating systems, databases and applications
- Setup of redundant servers for domain controller AD (Active Directory) server
- Assessment of network structure and network segmentation
- Conversion to a secure service access in accordance with the BDEW White Paper
- Implementation of a reliable backup strategy Preparation of an emergency concept
- Services for updates to current HIGH-LEIT versions (for older versions)
- Setting up of an anti-virus scanner with up-to-date signatures

We consult with you to decide upon the individual and detailed contents of the basic package, taking into account your specific requirements and the existing system concept.

These measures serve as a basis for the subsequent cyclic security maintenance measures.

Services around IT security

The keeping-up of a defined security level requires continuous activities which we carry out in close cooperation with you and which are laid down in a service agreement.

The annual services include:

- Administration of a separate computer at VIVAVIS for secure maintenance access
- Regular check of redundancy concepts
- Security check of all external access paths (terminal server, web server, process interface)
- Testing of backup mechanisms and of the stored backups of VIVAVIS HIGH-LEIT

The monthly/multi-monthly services include:

- Testing of operating system patches against the installed HIGH-LEIT version
- Upload of operating system patches (remote or local)
- Testing of patches of 3rd party products (e.g. Oracle) against the installed VIVAVIS HIGH-LEIT version
- Upload of patches for 3rd party products and system components (remote or local)

(Status: 10.02.2021, Subject to modification)