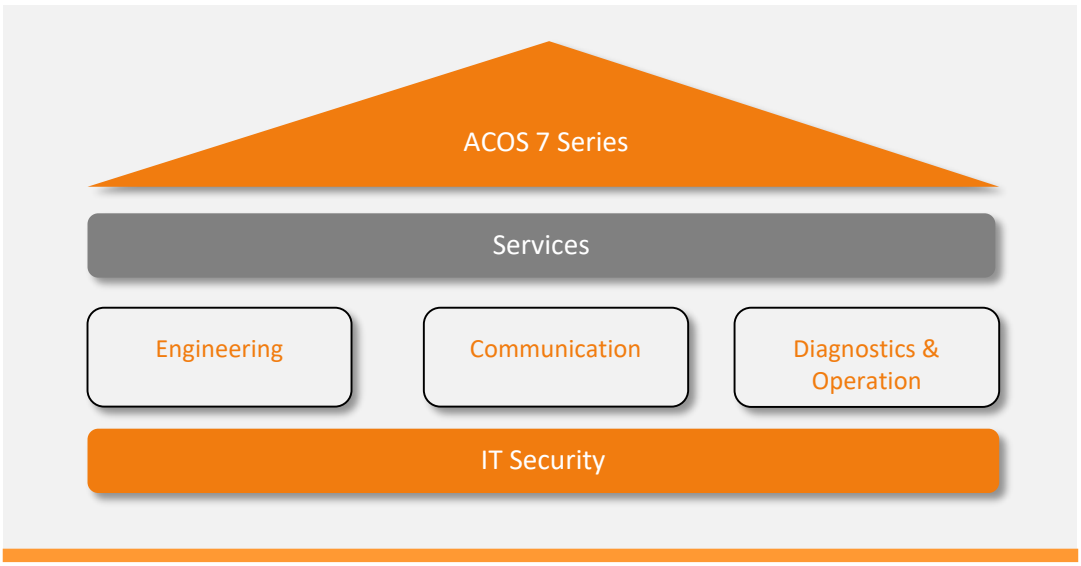

The ACOS 7 Series - Three Pillars of Security in Telecontrol Applications

The acquisition, transmission and processing of telecontrol data is vital for the operation of critical infrastructures, and measures to ensure IT security are of paramount importance. With our ACOS 7 series, you can be sure to be on the safe side – in all areas.

Secure Engineering with ACOS ET

ACOS ET offers not only different **user roles and rights**, but also enables users to authenticate themselves locally or centrally (e.g. via Windows AD).

Encryption of project data is essential, as well as the secure transmission of configuration data to the RTUs which is also based on certificate-based authentication. Additionally, sets of parameters and firmware update packets are checked for their integrity.

Secure Communication

For the encryption of data transmission via network-based telecontrol protocols via public or private network infrastructures, the devices from the ACOS 7 series enable the establishment of secure connections based on **certificate-based authentication** or **preshared keys**, through using **OpenVPN** or **IPSec.**
Furthermore, they also enable **end-to-end encryption** for private networks in accordance with IEC 62351-3.

Authentication to network components takes place in accordance with IEEE 802.1X. A **device firewall** monitors data transmission. All these measures protect the devices against possible attacks.

Diagnostics and Operation

Diagnostics of RTUs takes place via ACOS ET or the integrated web server, the latter of which also has **different user roles and rights**.

For diagnostic purposes, we recommend to set up different **zones or segmentation** across the respective VLANs. Logging of security-relevant events takes place on the basis of Syslog. Additionally, it is possible to poll information by means of SNMPv3. Furthermore, we offer intelligent patch management solutions.

The devices from the ACOS 7 series can be **individually parameterized** according to your requirements. Apart from our hardware, we also offer a **comprehensive portfolio of services**.

Tested and Approved

By the way**:** our ACOS 7 series was tested by **an independent software and consulting** company which confirmed that ACOS 7 provides **adequate protection** for networks requiring a **high level of protection!**

Morever, IDS GmbH is certified acc. to **ISO 27001**!

072018

IDS GmbH • Nobelstr. 18 • D-76275 Ettlingen • T +49 (0) 72 43/2 18-0 • F +49 (0) 72 43/2 18-1 00 • info@ids.de

The Three Pillars of Security

ACOS 7 Series

Tested and Confirmed *by an independent Software and Consulting Company*

Services

Engineering with ACOS ET

- ✓Different user roles and rights
- ✓Authentication: locally or centrally (e.g. via Windows AD)
- ✓Encryption of project data
- ✓Secure transmission of parameterization data to the RTUs (certificate-based)
- ✓Monitoring of parameter sets and firmware update packets for integrity

Communication

- ✓Encryption of data transmission via network-based telecontrol protocols
- ✓OpenVPN or IPSecbased on certificate-based authentication or preshared keys
- ✓End-to-end encryption acc. to IEC 62351-3
- ✓Authentication of network components acc. to. IEEE 802.1X
- ✓Device firewall for controlled data transmission and for protection against attacks

Diagnostics and Operation

- ✓Diagnosis of RTUS by means of ACOS ET or via an integrated web server with different user roles and rights
- ✓Establishment of differen t zones / segmentation via VLANs
- ✓Logging of security-specific events via Syslog
- ✓Polling of information by means of SNMPv3
- ✓Patch management

IT Security

(ISO 27001)

072018

IDS GmbH • Nobelstr. 18 • D-76275 Ettlingen – GERMANY • T +49 (0) 72 43/2 18-0 • F +49 (0) 72 43/2 18-1 00 • info@ids.de