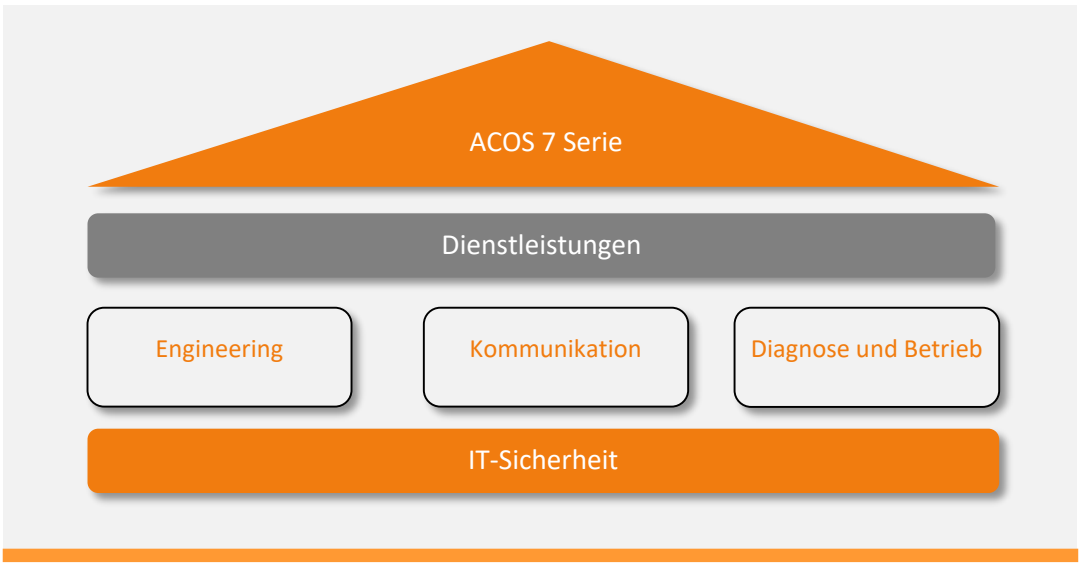

Die drei Sicherheitssäulen der Fernwirktechnik: Bauen Sie auf die ACOS 7 Serie

Für den Betrieb kritischer Infrastrukturen im Bereich der Energieversorgung ist die Erfassung, Übertragung und Verarbeitung von Informationen über die Fernwirktechnik unerlässlich. Maßnahmen zur IT-Sicherheit sind dabei fundamental. Mit unserer ACOS 7 Serie sind Sie in allen Bereichen abgesichert.

Sicheres Engineering mit ACOS ET

ACOS ET bietet nicht nur **unterschiedliche Benutzerrollen und -rechte**, sondern auch die Möglichkeit, sich entsprechend lokal oder zentral (z. B. über Windows AD) zu authentifizieren.

Die **Verschlüsselung von Projektdaten** ist dabei unerlässlich, wie auch die gesicherte Übertragung der Konfigurationsdaten zu den Fernwirkgeräten, die ebenfalls auf zertifikatsbasierter Authentifizierung beruht. Zusätzlich werden Parametersätze und Firmware-Update-Pakete auf Integrität geprüft.

Sichere Kommunikation

Um die Datenübertragung über netzwerkbasierte Fernwirkprotokolle durch öffentliche oder private Netzwerk-Infrastrukturen zu verschlüsseln, bieten die Geräte der ACOS 7 Serie die Möglichkeit, mittels **OpenVPN** oder **IPSec** gesicherte Verbindungen auf Basis **zertifikatsbasierter Authentifizierung** oder **Pre-Shared Keys** aufzubauen. In privaten Netzwerken kann zudem eine **Ende-zu-Ende-Verschlüsselung** gemäß IEC 62351-3 zur Anwendung kommen.

Die Authentifizierung gegenüber Netzwerkkomponenten erfolgt gemäß IEEE 802.1X. Eine **Gerätefirewall** kontrolliert den Datenverkehr. All diese Funktionalitäten schützen die Geräte vor möglichen Angriffen.

Diagnose und Betrieb

Die Diagnose der Fernwirkgeräte erfolgt über ACOS ET oder den integrierten Web-Server. Dieser verfügt ebenfalls über **unterschiedliche Benutzerrollen und -rechte**.

Für die Diagnose empfiehlt sich der Aufbau entsprechender **Zonen und Segmentierung** über entsprechende VLANs. Die Protokollierung sicherheitsrelevanter Ereignisse erfolgt auf Basis von Syslog. Zusätzlich können Informationen mittels SNMPv3 abgefragt werden. Außerdem bieten wir Ihnen intelligente Patchmanagement-Lösungen an.

Die Geräte der ACOS 7 Serie lassen sich **individuell** nach Ihren Anforderungen **konfigurieren**. Neben der Hardware bieten wir Ihnen auch **umfassende Dienstleistungen** an.

Geprüft und für gut befunden

Übrigens: Ein **unabhängiges Software- und Consulting-Unternehmen** attestierte der ACOS 7 Serie einen **angemessenen Schutz** für Netze **mit erhöhtem Schutzbedarf!**

Außerdem sind wir **ISO 27001**-zertifiziert!

Stand 04/2018

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

Die drei Sicherheitssäulen auf einen Blick

ACOS 7 Serie

Geprüft von einem unabhängigen Software- und Consulting-Unternehmen

Dienstleistungen

Engineering mit ACOS ET

- ✓Unterschiedliche Benutzerrollen und -rechte
- ✓Authentifizierung lokal oder zentral (z. B. über Windows AD)
- ✓Verschlüsselung von Projektdaten
- ✓Gesicherte Übertragung der Konfigurationsdaten zu den Fernwirkgeräten, zertifikatsbasiert
- ✓Überprüfung der Parametersätze und Firmware-Update Pakete auf Integrität

Kommunikation

- ✓Verschlüsselung der Datenübertragung über netzwerkbasierte Fernwirkprotokolle
- ✓OpenVPN oder IPSec auf Basis zertifikatsbasierter Authentifizierung oder von Pre-Shared Keys
- ✓Ende-zu-Ende-Verschlüsselung gemäß IEC 62351-3
- ✓Authentifizierung an Netzwerkkomponenten gemäß IEEE 802.1X
- ✓Gerätefirewall für kontrollierten Datenverkehr und Schutz vor Angriffen

Diagnose und Betrieb

- ✓Diagnose der Fernwirkgeräte über ACOS ET oder über integrierten Web-Server mit unterschiedlichen Benutzerrollen und -rechte
- ✓Aufbau entsprechender Zonen bzw. Segmentierung über entsprechende VLANs
- ✓Protokollierung sicherheitsrelevanter Ereignisse auf Basis von Syslog
- ✓Abfrage von Informationen mittels SNMPv3
- ✓Patchmanagement

IT-Sicherheit

(ISO 27001)

Stand 04/2018

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