Leitfaden

E – 005 – DE Kopplungen zu Leit- / Automatisierungssystemen

TE – EE Elektrotechnik

Anwendungsbereich:	Europa, Nordamerika Werke und Standorte der K+S AG und der K+S Minerals and Agriculture GmbH
Fachgebiet:	Elektrotechnik
Ursprungssprache:	Deutsch
Veröffentlichung:	Intranet, Extranet
Anwender:	K+S Mitarbeiter, Lieferanten und Kooperationspartner
Ersatz für Dokument:	neuer LF
Letzte Prüfung:	29.10.2025
Autor:	Alexander Röll
Abteilung:	TE-EES

Inhaltsverzeichnis

1 Geltungsbereich

Dieser Leitfaden stellt die Mindestanforderungen für die Kopplung und den Datenaustausch zu Leit- / Automatisierungssystemen dar.

Mit diesem Leitfaden werden einheitliche Mindestanforderungen veranlasst, um OT System wie insbesondere Prozessleitsysteme vor unbefugten Zugriff zu schützen. Zudem soll die Datenintegrität und -Vertraulichkeit der Anlagen-/ Betriebsdaten hiermit gewahrt werden.

Die grundlegenden Anforderungen wurden von der Arbeitsgruppe „IT-Sicherheit in der Automatisierungstechnik“ erarbeitet.

2 Mitgeltende Normen, Richtlinien

Es sind die nachfolgend aufgeführten VDE-Bestimmungen, harmonisierten EN – Normen , IEC - Empfehlungen und EU - Richtlinien in der jeweils gültigen Fassung einzuhalten.

IEC 62443 Cybersecurity in der Industrieautomatisierung

- Teil 1: Allgemeine Grundlagen
- Teil 2: Sicherheitsanforderungen für Betreiber und Dienstleister
- Teil 3: Sicherheitsanforderungen an Automatisierungssysteme
- Teil 4: Sicherheitsanforderungen an Automatisierungskomponenten
- Teil 5: Evaluationsmethodik

NIS-2 Richtlinie der EU

3 Automatisierungsstrategie

K+S verfolgt eine durchgängige und einheitliche Strategie zur Automatisierung und Digitalisierung.

Ein Datenaustausch sowie eine Datenschnittstelle zwischen den Leit- / Automatisierungssystemen auf der OT-Seite und den MES und ERP Systemen auf der IT-Seite ist dafür notwendig.

Falls eine solche Kopplung bereits vorhanden ist, so ist diese auf Einhaltung der in diesem Leitfaden beschriebenen Anforderungen zu überprüfen und bei Abweichungen unverzüglich anzupassen.

4 IT-Sicherheit

Die in der Richtlinie „IT/OT Sicherheit in der K+S Gruppe“ beschriebenen Anforderungen sind als Basis-Schutz zwingend einzuhalten.

5 OPC-Schnittstelle und Datensicherheit

Zur Kopplung der OT/IT Systeme ist der Schnittstellenstandard OPC-UA zu verwenden.

Die vom OPC-Server bereitgestellte Informationen sind auf das für die jeweilige MES bzw. ERP-Anwendung benötige Maß zu reduzieren.

Die von MES- bzw. ERP-Anwendungen benötigten Informationen dürfen lesend (read only) vom OPC-Server abgefragt und bereitgestellt werden.

Ein schreibender Zugriff ist im Bedarfsfall auf definierte Variablen des Leitsystems gestattet. Dies bedarf einer vorhergehenden Absprache/Freigabe durch den OT-Systemadministrator.

Die Informationen müssen verschlüsselt mittels sicherem Algorithmus übertragen werden, insbesondere sind hierfür die nachfolgenden Einstellungen am OPC-Server vorzunehmen:

- Security-Policy: AES256-SHA256
- Security-Mode: Sign&Encrypt
- Authentifizierung: User-Name + Passwort und Zertifikat

6 Netzwerktrennung / Firewallkonzept

Die Kopplung erfolgt über ein mehrstufiges Firewallkonzept sowie eine demilitarisierte Zone (DMZ) zwischen den Bereichen der OT und IT. Die DMZ ist unabhängig auf einem eigenen Hostsystem bzw. Hardwaresystem aufzusetzen.

Diese Architektur umfasst mindestens:

- eine IT-Firewall (zum Corporate Netzwerk)
- eine demilitarisierte Zone (OT-DMZ) inkl. eigenem Host
- eine interne OT-Firewall (zum Schutz der OT-Systeme) vom Typ Clavister NetWall300 (Neubeschaffung) oder Palo-Alto (Bestandssystem)
- die eingesetzten OT-Firewalls müssen mindestens über die folgenden Funktionen verfügen:
  - Intrusion Detection & Prevention System (IDS/IPS)

- Anti-Virus System (AV-Scanner)
- Application Layer Gateway für die zur Kopplung benötigten Protokolle, wie z.B. OPC, E-Mail, Druckdienst, etc.
- Statusüberwachung per SNMP
- Unterstützung parallel redundanter Betrieb

Sollte diese Kopplung noch nicht vorhanden sein oder diesem Standard nicht entsprechen, so ist als erster Schritt eine Netzwerkgrundplanung vorzunehmen. Diese ist durch einen spezialisierten OT-Dienstleister / -Kontraktpartner vorzunehmen und mit den jeweiligen Fachabteilungen der IT und OT abzustimmen.

7 Best Practice Beispiele

Netzwerkschema kleiner Standort:
Siehe großer Standort, wobei im Rahmen einer Risikobewertung ggf. auf eine redundante Ausführung der Firewalls verzichtet werden kann.

Netzwerkschema großer Standort: