

Leitfaden IT Sicherheit von PLT-Systemen auf Betriebsstätten WVER

Die Entwicklungen der Prozessleittechnik und der Unternehmensstruktur der letzten Jahre lassen eine isolierte, lokale Bedienung und Beobachtung einer Automation nicht mehr als zeitgemäß erscheinen.

Ein Zusammenwachsen der Physikalischen Plattformen, der Office IT und der PLT ist als großer Kostenvorteil zu werten. Allem voran sind in diesem Fall Standardisierungen mittels Windows/Intel und TCP/IP/Ethernet gemeint.

Komponenten und Dienstleistungen sind beherrschbarer und schneller verfügbar als früher. Diese Entwicklung birgt aber auch Gefahren in sich. Probleme der Office IT wie Schadsoftware und Sabotage sind nun auch in der Produktionsebene präsent.

Daher sind bei Neuanschaffungen und Migrationen von Leitsystemen folgende Richtlinien zu beachten:

1. Die SPS-Ebene ist physikalisch vom Intranet zu trennen

- Eigener Switch.
- Eigenes IP-Netz zur separaten Netzwerkkarte des PLS-Servers.
- Kein Eintrag des Standardgateways in der SPS.
- Der Kennwort-Schreibschutz der SPS ist zu aktivieren.
- Der IP-Schutz (falls vorhanden) ist zu aktivieren.
- Sollten Steuerungen über das Netz umgesetzt werden, so muss verschlüsselt werden und der IP-Schutz muss aktiviert sein

2. Der PLT-Server/Client

- Die Hard- und Software wird durch das zentrale Sachgebiet IT/PLT projektiert und beschafft.
- Der lokale PLT-Server verfügt über 2 Netzwerkkarten:
- Eine für das Intranet und eine für das SPS-Netz.
- Der lokale PLT-Server verfügt über mindestens 2 baugleiche Festspeichersysteme welche ohne RAID betrieben werden.
- Standorte mit Schichtbetrieb-Besetzung werden mit redundanten Systemen ausgestattet.
- Einbindung in den zentrale n Active-Directory-Service (ADS) der IT/PLT.

- In der Firewall (zentrale Vorgabe der ADS) aktivierte Ausnahmen werden von der IT-Sicherheit vorgegeben.
- Anforderung Betriebssysteme: mindestens Windows 11 oder Windows 2025
- Server (unter Beachtung der Kompatibilität des Leitsystemlieferanten).
- Der zentrale Anti-Virus des WVER mit mindestens täglicher Aktualisierung ist zu installieren.
- Betriebssystem-Updates sind automatisiert zu installieren.
- Client: Die Installation der OS-Updates erfolgt automatisch. Sollte ein Neustart erforderlich sein, wird dieser vom Betriebspersonal durchgeführt. Erfolgt dies nicht, so wird nach Ablauf einer vorgegebenen Zeit der Neustart automatisch ausgeführt.
- Server: Die Installation der OS-Updates erfolgt durch die zentrale Fachgruppe der IT/PLT. Sind Neustarts erforderlich so werden diese in Absprache mit dem Betriebspersonal durchgeführt.
- Anwendungsupdates werden anlassbezogen in Absprache mit dem Betriebspersonal durch das zentrale Sachgebiet IT/PLT installiert.
- Netzfregaben sind nur mit ADS-Userkonten vorzunehmen.
- Das Jeder-Konto mit Vollzugriff wird nicht verwendet. Netzfregaben werden ausnahmslos durch das zentrale Sachgebiet IT/PLT vorgenommen.
- OPC-DA DCOM-Berechtigungen sind nur auf die ADS-Konten zu legen welche einen Zugriff benötigen.
- Der Gastzugriff bleibt gesperrt.
- Administratoren-Kennwörter haben mindestens 8 Stellen und beinhalten ein Sonderzeichen.
- Das lokale und zentrale Administratoren-Kennwort der PLT-Anwendung und deren OS sowie der dazugehörigen Logfiles ist nur der zentralen Administration des UB 3.8 und dem Fachbereich IT bekannt.
- Der Wartungszugriff erfolgt ausnahmslos über den VPN-Zugang der WVER-IT (FB 2.5). Ein VPN-Account ist durch den Dienstvorgesetzten zu beantragen.
- Bei externen Dienstleistern erfolgt die Beantragung über den UB 3.8. Eine direkte Einwahl in das WVER-Intranet unter Umgehung der WVER-Sicherheitssysteme ist untersagt!
- Der Zugriff mittels Remote-Viewer-Tools mit Administratorenrechten ist nur von ausgewiesenen Usern oder IP-Adressen möglich.
- Einen Wartungszugriff einer Fremdfirma muss vorher erfragt und terminiert werden.
- Installationen von Software, insbesondere Remoteapplikationen sind von der IT/PLT-Leitung im Vorfeld zu genehmigen.

- Bei Lieferung von Hard- und Software verpflichtet sich der Auftragnehmer dahingehend, dass die Komponenten frei von Funktionen sind, welche der Vertraulichkeit, Integrität und Verfügbarkeit zuwiderlaufen. Dies bezieht sich auf
- Funktionen zum unerwünschten Aus- oder Einleiten von Daten sowie dem Manipulieren von Daten oder der Ablauflogik von Funktionserweiterungen.
- Beim Start der Leitsystemsoftware ist das OS und die AnlaufEinstellungen des Leitsystems so zu konfigurieren, dass ein Zugriff auf die OS-Ebene gesperrt ist (Kiosk-Modus).
- Personelle Veränderungen müssen durch die Personalabteilung des WVER an die Fachgruppe IT/PLT und den FB 2.5 mitgeteilt werden.

3. Bedienung von Prozessbildern

- Die Bedienungsberechtigung der lokalen Prozessbilder wird vom UB-Leiter/Abwassermeister geregelt. Hierbei sind die User-Gruppen der Administratoren, der Bedienungsberechtigten und der Beobachter bereits vorgegeben.
- Alle Benutzerkonten müssen personalisiert sein und den KRITIS-Kennwortrichtlinien des WVER entsprechen.

4. Webbilder

- Ein Zugriff auf Prozessbilder mit der Möglichkeit Anlagenprozesse zu verändern und außerhalb des lokalen Standortnetzes erfolgen müssen von der Dezernatsleitung genehmigt werden.
- Ausgenommen sind Beobachtungszugriffe.
- Parametrierbuttons der Trends und Alarmfenster welche nicht temporär sind müssen deaktiviert werden.
- Funktion und Quittierbutton's müssen auch im Beobachtermodus mit ADS-basierenden Berechtigungen versehen sein.

5. Datensicherung

- Die Sicherung der Betriebsdaten erfolgt im Minutentakt auf ein zentrales Speichermedium der Verwaltung des WVER und wird von dort im 24 h Takt auf ein weiteres räumlich getrenntes Speichermedium gespiegelt.
- Vollsicherungen der lokalen Systeme werden wöchentlich erstellt und zentral gesichert. Quartalskopien werden auf einem zentralen NAS-System gesichert.
- Bei lokalen Änderungen der SPS/PLS-Programme ist umgehend das zentrale Sachgebiet IT/PLT zu benachrichtigen bzw. die aktuelle Programmversion der Backup-Administration zwecks zentraler Sicherung zu übergeben.

- Die zentrale Fachgruppe IT/PLT ist zur Einhaltung von IT-Standards und Datenschutzbestimmungen verpflichtet und weisungsbefugt gegenüber internen wie externen Dienstleistern in der Ausführung ihrer IT-bezogenen Tätigkeit.

6. WLAN

Bei Einsatz von WLAN-Techniken sind folgende Sicherheitseinstellung zu beachten

- WPA3 Schlüssel 32-stellig Groß/Kleinschreibung sowie mind. 2 Sonderzeichen
- MAC-Filter der kommunizierenden Endgeräte ist einzurichten
- SSID als Unsichtbar deklarieren
- WLAN-Router Passwort 32-stellig Groß/Kleinschreibung
- sowie mind. 2 Sonderzeichen (darf nicht gleich dem WPA3 Schlüssel sein)

7. Messtechnik

Änderungen an der Messtechnik welche zentral aufgezeichnet werden ist umgehend der IT/PLT zu melden.

Hier drunter fallen insbesondere folgende Punkte:

- Änderung des Messbereiches
- Ausfall der Messung oder Stilllegung
- Umbenennung der Messeinrichtung
- Änderung des Messortes

8. Beschaffung

- Die Beschaffung von PLT Hard- und Software ist durch die DA00_1205 geregelt und erfolgt über die zentrale Fachgruppe IT/PLT oder wird von dort aus freigegeben.