Siemens
Industry
Online
Support

**ANWENDUNGSBEISPIEL**

# WinCC OA Konzept für eine Abwasser- und Wasser-aufbereitungsanlage

Leitfaden zur sicheren Projektierung

SIEMENS

# Rechtliche Hinweise

### Nutzung der Anwendungsbeispiele

In den Anwendungsbeispielen wird die Lösung von Automatisierungsaufgaben im Zusammenspiel mehrerer Komponenten in Form von Text, Grafiken und/oder Software-Bausteinen beispielhaft dargestellt. Die Anwendungsbeispiele sind ein kostenloser Service der Siemens AG und/oder einer Tochtergesellschaft der Siemens AG („Siemens"). Sie sind unverbindlich und erheben keinen Anspruch auf Vollständigkeit und Funktionsfähigkeit hinsichtlich Konfiguration und Ausstattung. Die Anwendungsbeispiele stellen keine kundenspezifischen Lösungen dar, sondern bieten lediglich Hilfestellung bei typischen Aufgabenstellungen. Sie sind selbst für den sachgemäßen und sicheren Betrieb der Produkte innerhalb der geltenden Vorschriften verantwortlich und müssen dazu die Funktion des jeweiligen Anwendungsbeispiels überprüfen und auf Ihre Anlage individuell anpassen.
Sie erhalten von Siemens das nicht ausschließliche, nicht unterlizenzierbare und nicht übertragbare Recht, die Anwendungsbeispiele durch fachlich geschultes Personal zu nutzen. Jede Änderung an den Anwendungsbeispielen erfolgt auf Ihre Verantwortung. Die Weitergabe an Dritte oder Vervielfältigung der Anwendungsbeispiele oder von Auszügen daraus ist nur in Kombination mit Ihren eigenen Produkten gestattet. Die Anwendungsbeispiele unterliegen nicht zwingend den üblichen Tests und Qualitätsprüfungen eines kostenpflichtigen Produkts, können Funktions- und Leistungsmängel enthalten und mit Fehlern behaftet sein. Sie sind verpflichtet, die Nutzung so zu gestalten, dass eventuelle Fehlfunktionen nicht zu Sachschäden oder der Verletzung von Personen führen.

### Haftungsausschluss

Siemens schließt seine Haftung, gleich aus welchem Rechtsgrund, insbesondere für die Verwendbarkeit, Verfügbarkeit, Vollständigkeit und Mangelfreiheit der Anwendungsbeispiele, sowie dazugehöriger Hinweise, Projektierungs- und Leistungsdaten und dadurch verursachte Schäden aus. Dies gilt nicht, soweit Siemens zwingend haftet, z.B. nach dem Produkthaftungsgesetz, in Fällen des Vorsatzes, der groben Fahrlässigkeit, wegen der schuldhaften Verletzung des Lebens, des Körpers oder der Gesundheit, bei Nichteinhaltung einer übernommenen Garantie, wegen des arglistigen Verschweigens eines Mangels oder wegen der schuldhaften Verletzung wesentlicher Vertragspflichten. Der Schadensersatzanspruch für die Verletzung wesentlicher Vertragspflichten ist jedoch auf den vertragstypischen, vorhersehbaren Schaden begrenzt, soweit nicht Vorsatz oder grobe Fahrlässigkeit vorliegen oder wegen der Verletzung des Lebens, des Körpers oder der Gesundheit gehaftet wird. Eine Änderung der Beweislast zu Ihrem Nachteil ist mit den vorstehenden Regelungen nicht verbunden. Von in diesem Zusammenhang bestehenden oder entstehenden Ansprüchen Dritter stellen Sie Siemens frei, soweit Siemens nicht gesetzlich zwingend haftet.
Durch Nutzung der Anwendungsbeispiele erkennen Sie an, dass Siemens über die beschriebene Haftungsregelung hinaus nicht für etwaige Schäden haftbar gemacht werden kann.

### Weitere Hinweise

Siemens behält sich das Recht vor, Änderungen an den Anwendungsbeispielen jederzeit ohne Ankündigung durchzuführen. Bei Abweichungen zwischen den Vorschlägen in den Anwendungsbeispielen und anderen Siemens Publikationen, wie z. B. Katalogen, hat der Inhalt der anderen Dokumentation Vorrang.
Ergänzend gelten die Siemens Nutzungsbedingungen (https://support.industry.siemens.com).

### Securityhinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen einen Bestandteil eines solchen Konzepts.

Die Kunden sind dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Diese Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und nur wenn entsprechende Schutzmaßnahmen (z.B. Firewalls und/oder Netzwerksegmentierung) ergriffen wurden.

Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter https://www.siemens.com/industrialsecurity.

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Produkt-Updates anzuwenden, sobald sie zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter https://www.siemens.com/cert.

# Inhaltsverzeichnis

# Abkürzungen

| | |
|---|---|
| ADSL | Asymmetric Digital Subscriber Line |
| ATV | Abwassertechnische Vereinigung |
| DMZ | Demilitarisierte Zone |
| DNP3 | Distributed Network Protocol |
| EPS | Endpoint Security |
| GSM | Global System for Mobile Network |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| IAD | Industrial Anomaly Detection (Industrielle Anomalieerkennung) |
| IPSec | Internet Protocol Security |
| IWLAN | Industrial Wireless Local Area Network |
| PPTP | Point-To-Point Tunneling Protocol |
| KVM | Keyboard Video Mouse |
| L2TP | Layer 2 Tunneling Protocol |
| NMS | Netzwerkmanagementsystem |
| RADIUS | Remote Access Dial In User Service |
| RDP | Remote Desktop Protocol |
| SPS | Speicherprogrammierbare Steuerung |
| RTC | Real Time Clock (Echtzeituhr) |
| RTU | Remote Terminal Unit (Fernbedienungsterminal) |
| SCADA | Supervisory Control and Data Acquisition |
| SIEM | Security Information Event Management |
| SPAN | Switched Port Analyser – Portspiegelung |
| SSL | Secure Sockets Layer |
| TLS | Transport Layer Security |
| TPS | Threat Prevention Subscription |
| TRA | Threat and Risk Analysis (Bedrohungs- und Risikoanalyse) |
| UMC | User Management Component |
| UMTS | Universal Mobile Telecommunications System |
| VPN | Virtual Private Network |
| WLAN | Wireless Local Area Network |
| WinCC OA | SIMATIC WinCC Open Architecture |
| WSUS | Windows Server Update Service |
| ABA | Abwasserbehandlungsanlage |

# 1. Vorwort

Dieses Dokument soll Systemintegratoren dabei helfen, wasser- und abwassertechnische Anlagen sicherer zu planen.

Das SCADA-System SIMATIC WinCC Open Architecture (WinCC OA) ist als offenes System konzipiert und lässt sich daher den unterschiedlichsten Kundenbedürfnissen flexibel anpassen. Die Systemsoftware bietet dem Projektierungsingenieur bei seiner Aufgabe einen hohen Freiheitsgrad, was auch für die Gestaltung der Geschäftslogik und der Visualisierung gilt.

Erfahrungsgemäß fallen spätere Modernisierungen oder Anlagenerweiterungen viel leichter, wenn das Automatisierungsprojekt von Anfang an und soweit möglich als „konform mit SIMATIC WinCC Open Architecture (WinCC OA)“ aufgesetzt wird. Dies bedeutet, dass Anwender bestimmte Grundregeln beachten müssen, um sicherzustellen, dass die vorgesehenen Systemfunktionen in der Zukunft eine optimale Bedienerfreundlichkeit bieten.

Dieses Handbuch dient als Kompendium, das die Produktdokumentation für SIMATIC WinCC Open Architecture (WinCC OA) und die Automatisierungsgeräte ergänzt. Die grundlegenden Schritte zur Projekterstellung und Parametrierung werden in Form von Anweisungen beschrieben.

Die Richtlinie bezieht sich unmittelbar auf die empfohlene Methodik (Defense-in-Depth nach IEC 62443), die auf den Ergebnissen weitreichender praktischer Erfahrung beruht. Die Beschreibung behandelt die Arbeit am Projekt und die Parametereinstellungen der darin enthaltenen Komponenten, aber nicht die Anwendung selbst.

# 2. Sicherheitsstrategien

Angesichts einer zunehmenden Anzahl von Angriffen (Schadsoftware, unbefugter Zugriff, Dienstblockade, Manipulation usw.) ist der Schutz von Automatisierungs- und Datensystemen gegen Attacken und Manipulation oberste Priorität für fast jedes System und Projekt. Die Digitalisierung als der dominierende Branchentrend wird zudem bewirken, dass die Anzahl vernetzter Systeme und damit die Anzahl potentieller Schwachstellen weiterhin wächst.

Anlageningenieure und Betreiber müssen mit hoher Priorität den Schutz von Automatisierungs- und Leitsystemen gegen Manipulation und Schadsoftware forcieren, um Verfügbarkeit und Qualität zu sichern – bei gleichzeitiger Erfüllung nationaler und internationaler Anforderungen.

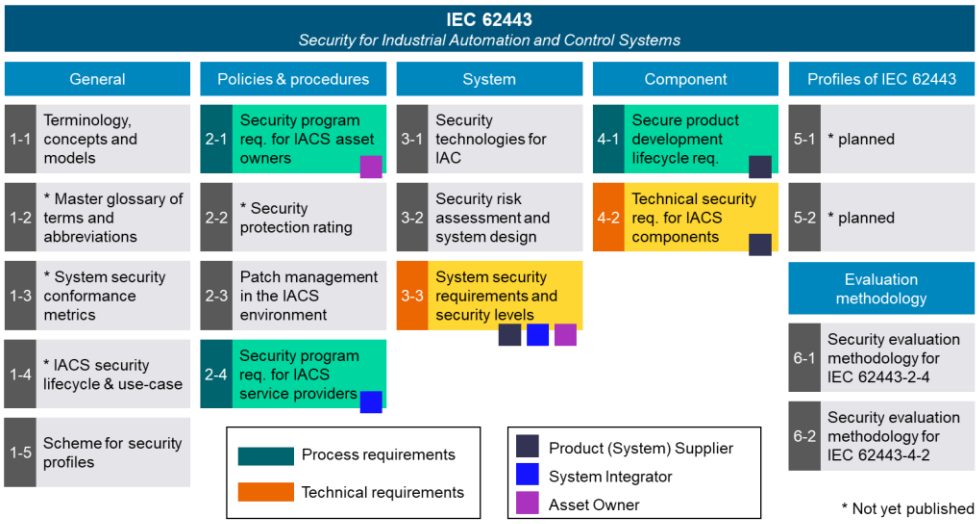
Aufgrund der enormen Vielfalt von Angriffen und der Komplexität in der Prozessindustrie ist es oft nicht leicht, Risiken und Bedrohungen zu identifizieren und die richtige Sicherheitsstrategie anzuwenden.

Gute, regelmäßige und gut geschützte Datensicherungen, eine wirksame Strategie für die Cybersicherheit, einschließlich der Isolierung kritischer Systeme mittels geeigneter Software, Installation der neuesten Sicherheitspatches und der Einsatz einschlägig geschulter Mitarbeiter sind von zentraler Bedeutung.

## 2.1. Norm IEC 62443 – Übersicht

Industrielle Sicherheit im Sinne neuerer Richtlinien sollte als Lebenszyklusthema behandelt werden. Um dem Bedarf für eine höhere Sicherheit von Systemen gerecht zu werden, müssen Betreiber alle Phasen des Lösungslebenszyklus betrachten, von der Entwicklung der Systeme bis zu ihrem Ersatz am Ende der Nutzungsdauer. Laut Normenreihe IEC 62443 besteht der Lebenszyklus aus fünf Phasen: Produkt- oder Systementwicklung, Spezifikation, Integration und Inbetriebnahme, Betrieb und Instandhaltung und Außerbetriebnahme. Eine Übersicht der Norm ist im folgenden Bild dargestellt:

Bild 2-1: Übersicht über IEC 62443

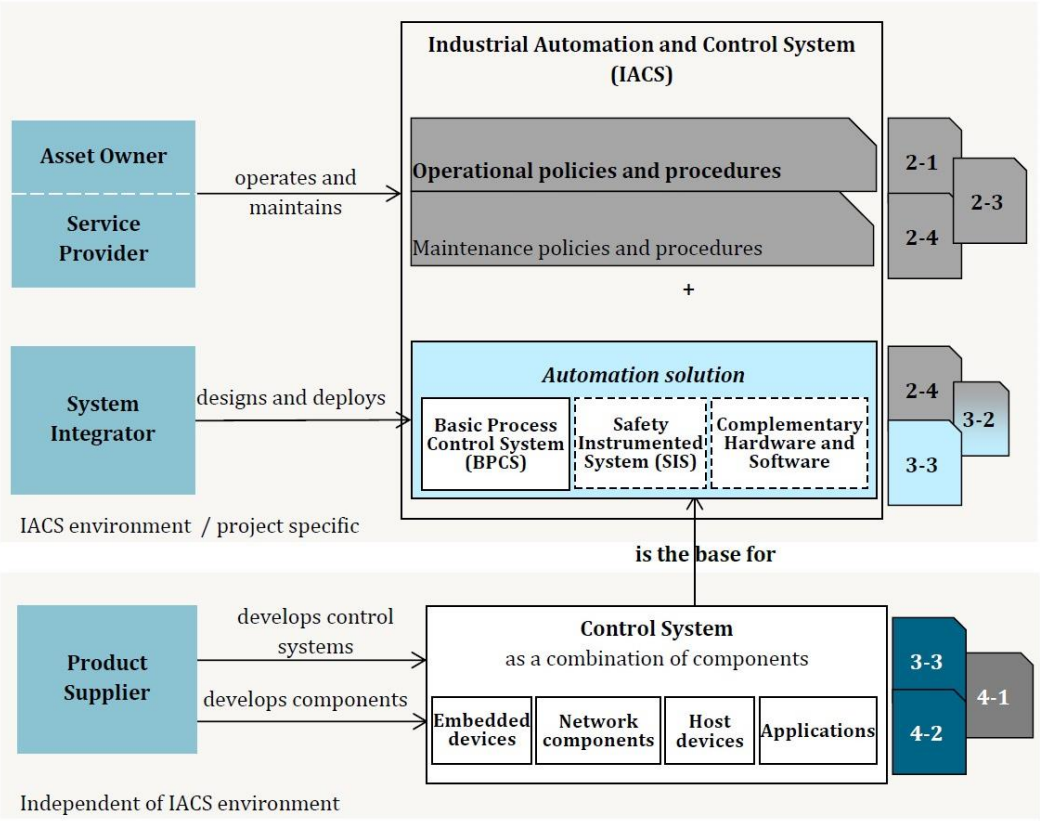


Mit jeder dieser Phasen ist eine klare Verantwortung und ein primäres Ziel verknüpft, und Sicherheitsthemen müssen zwischen verschiedenen Rollen und Anspruchsgruppen koordiniert und kommuniziert werden (Bild 2-2):

- Produktlieferanten implementieren im Rahmen des Produktentwicklungsprozesses Sicherheitsmaßnahmen wie Authentifizierung, sichere Kommunikationsmöglichkeiten oder robuste Kommunikations-Stacks in den Komponenten (z.B. IEC 62443 Teil 4-1).
- Systemintegratoren gewährleisten eine sichere Auslegung, die den Anforderungen je nach Exposition, Bedrohungen, Auswirkungen sowie der physischen und technischen Betriebsumgebung entspricht, wie vom Anlagenbetreiber vorgegeben. Der Systemintegrator definiert und appliziert die sichere Konfiguration und führt eine Verifizierung und Validierung durch. Systemintegratoren benötigen Sicherheitsinformationen über die Komponenten des Produkts, um die Komponenten sicher projektieren zu können.
- Anlagenbetreiber übernehmen den sicheren Betrieb und die Instandhaltung, hierunter fallen zum Beispiel die Benutzerverwaltung und die Handhabung von Berechtigungen, und spielen regelmäßig Sicherheitspatches auf.

Diese Rollen müssen zusammenarbeiten, um über den gesamten Lebenszyklus eines Systems eine angemessene Sicherheit zu erreichen. Ein Mangel an adäquaten Informationen oder eine unterschiedliche Interpretation von Sicherheitsthemen konterkariert die gemeinsamen Anstrengungen der verschiedenen Beteiligten.

Bild 2-2: Rollen nach IEC 62443

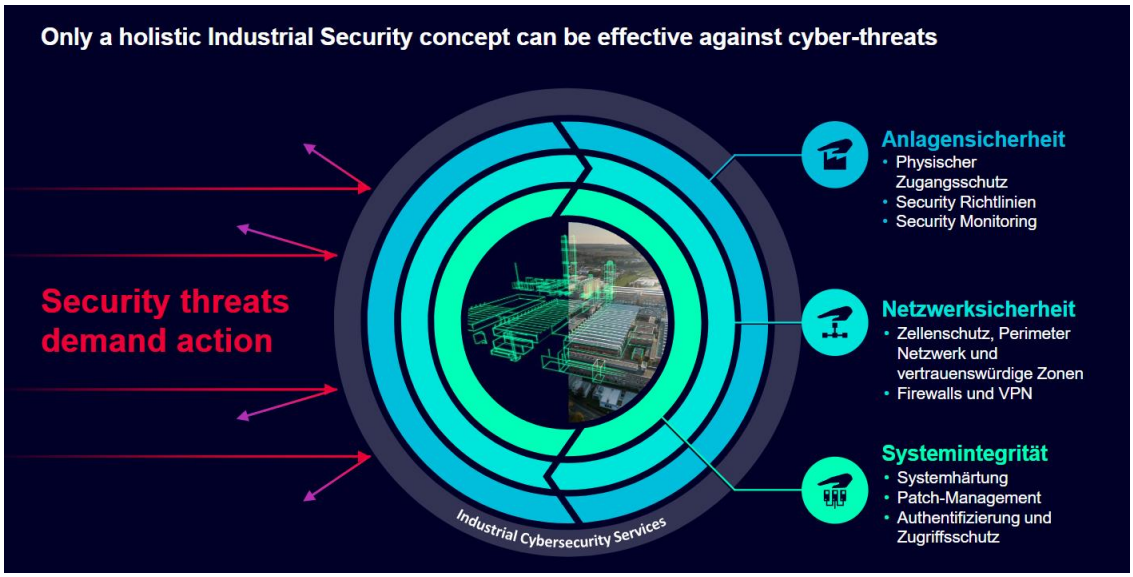


## 2.2. Sicherheitskonzept „Defense-in-Depth“

Ein alles überspannender Schutz industrieller Einrichtungen gegen Cyberattacken muss auf allen Ebenen gleichzeitig gewährleistet sein, von Gesamtbetrieb bis zum Einzelarbeitsplatz, von der Zugriffssteuerung bis zum Kopierschutz. Die Norm IEC 62443 empfiehlt daher das Konzept „Defense-in-Depth“ als Plan für einen umfassenden Schutz.

Ein Automatisierungs- und Leitsystem mit Defense-in-Depth-Abwehr muss über mehrere Schutz- und Aktionsebenen verteidigt werden, was bedeutet, dass Anlagenbetreiber und Lösungsanbieter vielfältige und sehr unterschiedliche Sicherheitsthemen bearbeiten müssen. Hierbei reicht die Bandbreite von der Anlagensicherheit und Netzwerksicherheit bis zur Systemintegration und zu organisatorischen Maßnahmen.

Bild 2-3: Defense-In-Depth




### 2.2.1. Anlagensicherheit

- Physische Sicherheitsmaßnahmen:
  Kontrolle des physischen Zugangs zu Flächen, Gebäuden, einzelnen Räumen, Schalt- und Steuerschränken, Geräten, Maschinen, Kabeln und Drähten. Die physischen Sicherheitsmaßnahmen sind auf der Ebene der Sicherheitszellen und der verantwortlichen Personen angesiedelt. Ebenso wichtig ist die Umsetzung des physischen Schutzes auch an entfernten Einzelplatzsystemen.
- Sicherheitsmaßnahmen auf Organisationsebene:
  Hierzu gehören Sicherheitsrichtlinien, Sicherheitskonzepte, Sicherheitsregeln, Sicherheitskontrollen, Risikoanalysen, Risikobewertungen und Risikoaudits, Maßnahmen zur Sicherheitsaufklärung und Schulungen.

### 2.2.2. Netzwerksicherheit

- Unterteilung in Sicherheitszellen:
  In einer umfassend abgesicherten Netzwerkarchitektur ist das Steuerungsnetzwerk in verschiedene aufgabenbezogene Ebenen unterteilt.
  Zu diesem Zweck sollten Techniken der Perimeterzonierung angewandt werden. Das bedeutet: Systeme, die im Perimeternetzwerk (demilitarisierte Zone, DMZ) eingerichtet sind, werden durch eine oder mehrere Firewalls (Front-Firewall und Back-Firewall oder Three-Homed Firewall) von anderen Netzwerken (z.B. Internet, Büronetzwerk) abgeschirmt. Diese Trennung ermöglicht den Zugriff auf Daten im Perimeternetzwerk, ohne dass gleichzeitig der Zugriff auf das interne, zu schützende Netzwerk (z.B. das Automatisierungsnetzwerk) erlaubt werden muss. Hierdurch lässt sich das Risiko von Zugriffsverletzungen deutlich senken.

- Absicherung der Zugangspunkte zu den Sicherheitszellen:
  Es gibt jeweils nur einen einzigen Zugangspunkt zu einer Sicherheitszelle (sollte durch Firewall realisiert werden) zur Authentifizierung von Benutzern, verwendeten Geräten und Anwendungen, für die richtungsbasierte Zugriffssteuerung, die Zuweisung von Zugriffsberechtigungen und die Erkennung von Eindringversuchen.
  Der so realisierte einzige Zugangspunkt bildet den Hauptzugangspunkt zum Netzwerk einer Sicherheitszelle und dient als erster Punkt der Steuerung von Zugriffsrechten für eine Netzwerkebene. Externe Pumpstationen oder Regenwasserbecken stellen also im Musterkonzept eigene Sicherheitszellen dar.

- Absicherung der Kommunikation zwischen zwei Sicherheitszellen über ein „unsicheres" Netzwerk:
  Bei Einsatz der Perimeterzonierungstechnik und Kommunikation über die Zugangspunkte sollte immer eine zertifikatbasierte, authentifizierte und verschlüsselte Kommunikation praktiziert werden. Hierfür eignen sich Tunnelprotokolle wie L2TP (Layer 2 Tunneling Protocol), IPSec (IPSecurity) und OpenSSL (Open Transport Layer Security und Secure Sockets Layer). Weitere Optionen für die sichere Kommunikation sind der Einsatz von Protokollen, die durch serverbasierte Zertifikate abgesichert sind, wie z.B. RDP (Remote Desktop Protocol), oder die Verwendung einer über HTTPS veröffentlichten Website. In diesem Fall findet die Kommunikation über die Firewall hinweg mit Technologien wie Transport Layer Security (TLS) oder Secure Sockets Layer (SSL) statt.

### 2.2.3. Systemintegrität

- Systemhärtung:
  Nachträgliche Änderungen am System mit dem Ziel, es widerstandsfähiger gegen Angriffe zu machen

- Benutzerverwaltung und rollenbasierte Bedienerberechtigungen:
  Aufgabenorientierte Bedien- und Zugriffsberechtigungen (rollenbasierte Zugriffssteuerung)

- Patchmanagement:
  Patchmanagement ist die systematische Vorgehensweise beim Installieren von Aktualisierungen auf Anlagensystemen.

- Erkennung und Abwehr von Schadprogrammen:
  Einsatz geeigneter und richtig konfigurierter Virenscanner und Whitelisting von Software

## 2.3. Musterkonzepte für Referenzarchitekturen für die Wasser- und Abwasserwirtschaft

Angesichts all dieser Anforderungen ist es nur zu verständlich, dass Projektteams sich möglicherweise überfordert fühlen, wenn sie vor der Aufgabe stehen, bei der Umsetzung eines technischen Projekts adäquate tiefgestaffelte Sicherheitskonzepte für Systeme zu realisieren.

Für jedes der in Abschnitt 2.2 angesprochenen Themen sind zahlreiche technische Lösungen, Werkzeuge und bewährte Verfahren verfügbar – aber Projektteams fehlt die Zeit und Erfahrung, eine geeignete Lösung für jedes Sicherheitsthema auszuwählen. Daher wird oft der Fehler gemacht, manche Themen eingehend zu behandeln, während andere Fallstricke übersehen werden.

Um das Sicherheits-Engineering besser handhabbar zu machen und diesen Fehler zu vermeiden, präsentiert Siemens an dieser Stelle eine Reihe von Musterkonzepten für Automatisierungs- und Leitsysteme. Diese Musterkonzepte bieten Unterstützung in Form von Verweisen auf bestimmte Ressourcen und gewährleisten, dass alle nach IEC 62443-2-4 vorgeschriebenen sicherheitsbezogenen Dokumente in das technische Projekt einfließen. Auf der Grundlage einer Standardlösung mit dem SCADA-System WinCC OA sind die Musterkonzepte dafür vorgesehen, die Anforderungen einer bestimmten, aber dennoch typischen Wasser- und Abwasseranwendung zu erfüllen.

# 3. Musterkonzept – Abwasserbehandlungsanlage

Das Musterkonzept repräsentiert die typische Systemarchitektur für eine Abwasserbehandlungsanlage (ABA) auf Basis von WinCC OA.

Die Musterarchitektur berücksichtigt jedoch auch die Projektierung einer Wasserbehandlungsanlage (WBA).

Die Prozesselemente sind für die verschiedenen Anlagentypen wie folgt unterteilt:

Tabelle 3-1 – Übersicht über die Anlagentypen

| Abwasserbehandlungsanlage | Wasserbehandlungsanlage |
|---|---|
| Mechanische Behandlung | Rohwasserzulauf |
| Biologische Behandlung | Filtrierung, Waschwasser/Reinwasser |
| Schlammbehandlung | Schlammbehandlung, Neutralisierung |

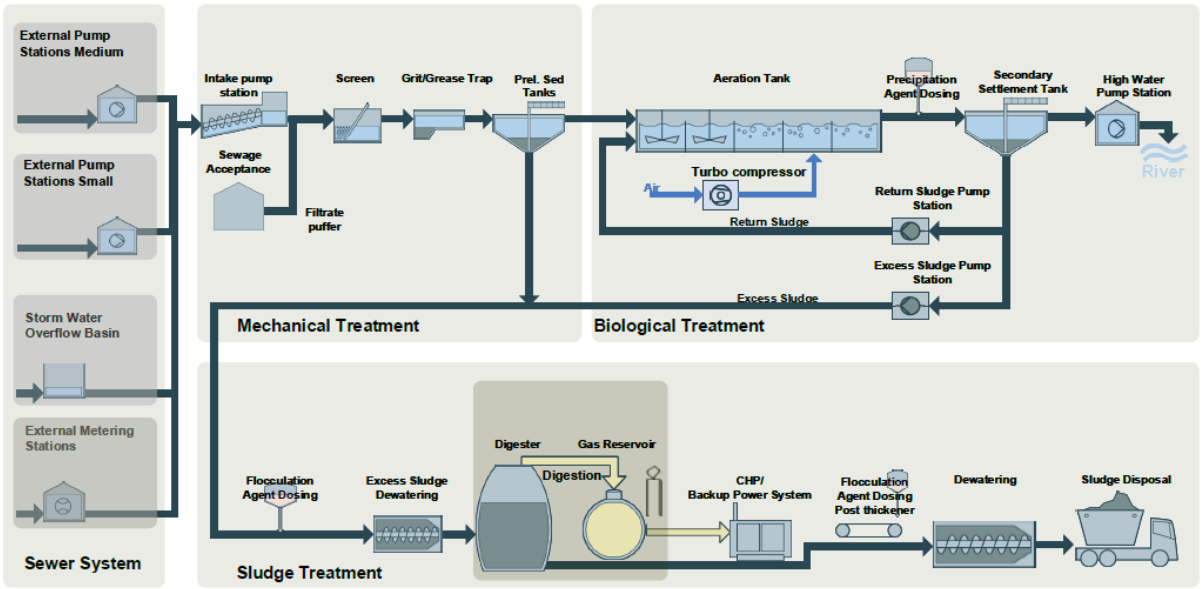
## 3.1. Prozessbeschreibung

Eine Abwasserbehandlungsanlage sammelt das Abwasser von ca. 100.000 Haushalten und bereitet es in verschiedenen Schritten auf, damit das behandelte Wasser wiederverwendet werden kann.

Der Prozess der Abwasserbehandlungsanlage für das Musterkonzept ist in Bild 3-2 dargestellt. Der Prozess umfasst die folgenden Hauptschritte:

- Mechanische Behandlung
- Biologische Behandlung
- Schlammbehandlung
- Kanalisation

Bild 3-1 – Prozessübersicht



### 3.1.1. Mechanische Behandlung

In diesem Verfahrensschritt wird das gesamte Abwasser aus der Kanalisation in die Behandlungsanlage überführt und von Grobbestandteilen und absetzbaren Verunreinigungen wie Sand, kleinen Steinen oder Glassplittern befreit.

Die Zulaufpumpstation dient zum Heben des aus der Kanalisation kommenden Abwassers in die mechanische Behandlungsstufe einer Abwasserbehandlungsanlage. Die Schnecken- oder Kreiselpumpen werden durch den Ablaufstrom der Zulaufpumpstation geregelt. Diese Pumpen stellen sicher, dass die mechanische Behandlung von einem konstanten Zulaufstrom gespeist wird, was eine höhere Prozessqualität ergibt.

Der Rechen entfernt Grobbestandteile aus dem Abwasser. Nachdem das Abwasser die Recheneinheit passiert hat, wird es einer Waschpresse zugeführt. Die Waschpresse verdickt die Grobbestandteile im Abwasser und fördert das Rechengut in einen Container. Das vorgereinigte Abwasser gelangt durch einen Kanal zum Sand- und Fettfang.

Der Sand- und Fettfang dient zum Entfernen grober absetzbarer Verunreinigungen wie Sand, kleinen Steinen oder Glassplittern aus dem Abwasser. Der Sand- und Fettfang besteht aus einem Absetzbecken und einer darüber installierten Räumerbrücke mit Fahrwerk und Räumer. Schwere, mineralische Feststoffe (hauptsächlich Sand) setzen sich am Boden des Beckens ab. Ungelöstes Fett und Öl sammelt sich auf der Wasseroberfläche und wird von einem Fetträumer abgezogen.

Das primäre Absetzbecken dient zum Abscheiden weiterer absetzbarer und aufschwimmender Feststoffe aus dem Abwasser. Das Abwasser fließt sehr langsam durch das primäre Absetzbecken. Feststoffe können sich so am Boden des Beckens absetzen.

### 3.1.2. Biologische Behandlung

Der biologische Abwasserbehandlungsprozess dient zum Entfernen von Verunreinigungen, die nach der mechanischen Behandlung übrigbleiben.

Das Belüftungsbecken ist in zwei Bereiche unterteilt.

- Denitrifikationsbecken
- Durch die anoxischen Bedingungen im Denitrifikationsbecken wird Nitrat in Stickstoff umgewandelt und die N-Last des Abwassers gesenkt.
- Nitrifikationsbecken
- Im Nitrifikationsbecken verringert sich die organische Last des Abwassers durch die Arbeit von Mikroorganismen. Dafür ist gelöster Sauerstoff im Wasser notwendig. Turbokompressoren drücken Luft in das Nitrifikationsbecken.

Das sekundäre Absetzbecken dient zum Reinigen des Wassers vom Schlamm. Schlamm, der schwerer als Wasser ist, bildet ein Sediment am Boden des sekundären Absetzbeckens. Ein kontinuierlich rotierender Räumer bewegt den überschüssigen Schlamm zu einem Sammelbecken. Rücklaufschlammpumpen fördern den Schlamm aus dem Sammelbecken zurück in das Belüftungsbecken. Überschussschlammpumpen führen den überschüssigen Schlamm der Schlammbehandlung zu.

Schlamm, der leichter als Wasser ist, schwimmt auf der Wasseroberfläche und wird von einer am Räumer montierten schwimmenden Schlammabsaugeinrichtung gesammelt und zum Schlammeindicker gepumpt.

Die Hochwasserpumpstation dient bei Bedarf dazu, das gereinigte Wasser in einen Flusslauf zu pumpen.

### 3.1.3. Schlammbehandlung

Dieser Prozess hat die Aufgabe, den bei der Abwasserbehandlung entstehenden Klärschlamm aufzubereiten und zu entsorgen. Schlamm ist großteils Wasser mit Anteilen von Feststoffen, die aus Abwasser entfernt wurden.

Die Schlammeindickung dient dazu, den Faulturm mit Schlamm zu befüllen. Der Schlamm – Primär- oder Überschussschlamm – kann im Schlammeindicker eingedickt werden, bevor er in den Faulturm gelangt.

Der Faulturm ist Teil der Schlammbehandlung einer Abwasserbehandlungsanlage. Die anaerobe Behandlung des Schlamms dient zur Stabilisierung des Schlamms durch Zersetzung organischer Anteile (gelöst oder schwebend). Das entstehende Biogas wird wegen seines Methangehalts zur Energieerzeugung genutzt.

Gasbehälter und Gasfackel sind Teil der Schlammbehandlung einer Abwasserbehandlungsanlage. Der Gasbehälter dient zum Speichern des Biogases aus dem Faulturm und sichert eine stabile Gasversorgung des Blockheizkraftwerks (BHKW) und einer Heizungsanlage.

Zur Entwässerung muss der Schlamm wegen der starken Haftung des Wassers an den Feststoffe konditioniert werden. Eine Flockungsstation dosiert Flockungsmittel in Abhängigkeit von Trübung und Durchflussmenge am Zulauf des Klärbeckens.

### 3.1.4. Kanalisation

Die Kanalisation bildet die Zulaufseite der Abwasserbehandlungsanlage und speist die Anlage mittels Pumpstationen.

Die externe Pumpstation ist mit dem Abwasserkanal verbunden. Das Abwasser fließt vom Abwasserkanal in die mechanische Vorbehandlung, wo der Rechen grobe Bestandteile aus dem Abwasser entfernt. Nach dem Passieren der Recheneinheit fließt das Abwasser in eine Abwassersammelkammer. Die externe Pumpstation speist die Zulaufpumpstation der Abwasserbehandlungsanlage.

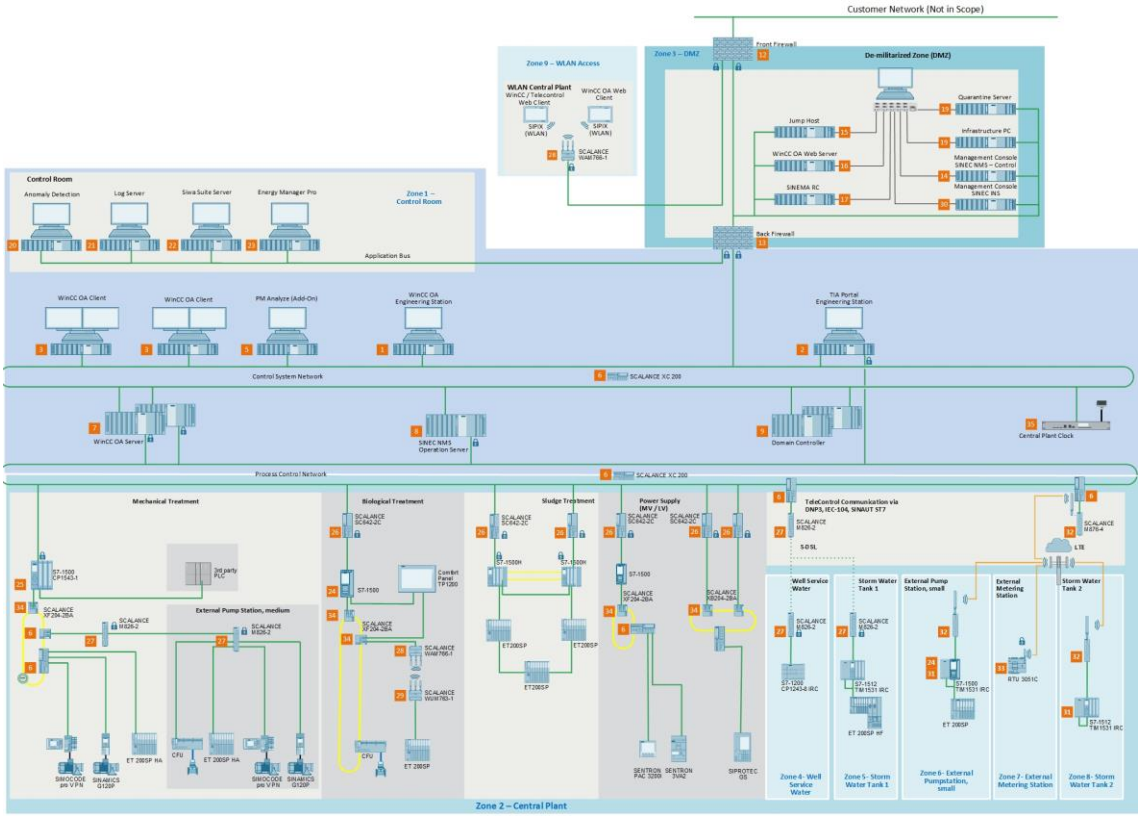
Das Regenwasserbecken ist über ein Zulaufüberlaufwehr mit dem Abwasserkanal verbunden. Bei sehr starken Regenfällen überströmt das Gemisch aus Wasser und Abwasser ein Überlaufwehr im Regenwasserbecken und reduziert die Belastung der nachgeschalteten Kläranlage. Sobald sich nach dem Starkregenereignis der Zulauf aus dem Abwasserkanal normalisiert hat, wird das Abwassergemisch aus dem Regenwasserbecken langsam in den Abwasserkanal zurückgeleitet.

Die externe Zählerstation dient zum Messen der aus Wohn- und Gewerbegebäuden kommenden Wassermenge, die über das öffentliche Abwasserkanalnetz herangeführt wird.

## 3.2. Systemarchitektur

Die WinCC OA-Systemarchitektur für das Musterkonzept der Abwasserbehandlungsanlage ist in Bild 3-2 dargestellt.

Bild 3-2 – WinCC OA-Systemarchitektur




### 3.2.1. Systemkomponenten für das Musterkonzept

Die Norm IEC 62443 klassifiziert die Systemkomponenten in drei Gerätetypen:

- Host / Anwendung:
- Workstation bestehend aus handelsüblicher PC-Hardware mit COTS-Betriebssystem und einer oder mehreren Anwendungen.
- Netzwerkkomponente:
- Gerät, das den Datenfluss zwischen Geräten in einem Netzwerk ermöglicht bzw. begrenzt, aber nicht direkt mit einem Steuerungsprozess interagiert.
- Eingebettetes Gerät:
- Spezielles Gerät, auf dem eingebettete Software läuft, um einen industriellen Prozess direkt zu überwachen, zu steuern oder zu regeln. Beispiele hierfür sind speicherprogrammierbare Steuerungen (SPS) und Feldsensorgeräte.

Die im Musterkonzept für die Wasserindustrie verwendeten Systemkomponenten sind in den folgenden Tabellen aufgeführt.

**Host / Anwendung**

Tabelle 3-2 – Hosts

| Komponente | Funktion |
|---|---|
| 1 – WinCC OA Engineering-Station | PC-Station für das zentralisierte anlagenweite SCADA-Engineering.<br>Online-Änderungen und Erweiterungen des Datenmodells.<br>Einbindung neuer Geräte.<br>Online-Anwendungsänderungen (Betriebsbildschirme, Treibereinstellungen, Geschäftslogik).<br>Verteilung der Änderungen an den SCADA-Server. |
| 2 – TIA Engineering-Station | PC-Station für das zentralisierte anlagenweite Engineering für SPS-Geräte.<br>Projektierung der Hardware.<br>Projektierung der Kommunikationsnetzwerke.<br>Projektierung kontinuierlicher und sequenzieller Prozessreihenfolgen.<br>Bedien- und Beobachtungsstrategien.<br>Übersetzung und Download aller Projektierungsdaten für alle Zielautomatisierungsgeräte. |
| 3 – WinCC OA-Client | Für die Bedienung und Beobachtung. WinCC OA-Clients greifen auf die Daten auf den WinCC OA-Servern zu, visualisieren diese Daten und erlauben Bedienern, den Prozess zu beeinflussen. |
| 5 – PM ANALYZE | Add-on zum Vorbereiten und Erstellen spezieller Berichte in Konformität mit ATV-Vorschriften. |
| 7 – WinCC OA-Server, redundant | Die redundanten Server des Hot-Standby-Systems enthalten alle Daten der verbundenen Automatisierungsgeräte und -systeme. Jeder Server enthält ein Messwertarchiv und ein Alarmarchiv. Sie bauen die Kommunikationsverbindung zu den Automatisierungsgeräten auf. Die WinCC OA-Server übermitteln die Prozessdaten an die WinCC OA-Clients. |
| 8 – SINEC NMS – Operation Server | Netzwerkmanagementsystem zum Überwachen und Verwalten industrieller Netzwerke. Die Komponente „Operation" dient zum Anzeigen ausführlicher Informationen über die überwachten Geräte und stellt die Geräte in Netzwerktopologien dar. |
| 9 – Domain Controller, redundant | Unterstützt den Active Directory Service und liefert Zeitinformationen. |
| 14 – SINEC NMS Control UMC | Netzwerkmanagementsystem zum Überwachen und Verwalten industrieller Netzwerke. Die Komponente „Control" dient zur Überwachung und Administration des gesamten Netzwerks. |
| 16 – WinCC OA Web Server | Bietet die Möglichkeit, eine Anlage über das Internet/Intranet mit einem WinCC OA-ULC-UX-Client zu bedienen und zu beobachten. Wenn ein Browser versucht, eine Verbindung zur ULC UX-URL des WinCC OA Web Servers herzustellen, gibt der Web Server die ULC UX-Webseite zurück und startet automatisch einen lokalen WinCC OA UI-Manager. Dieser serverseitige UI-Manager überträgt die angezeigten Informationen der UI in mit HTML 5 interpretierbare Datenblöcke. |
| 17 – SINEMA RC-Server | Bietet sicheren Fernzugriff über das Internet auf unterlagerte Netzwerke für Wartungs-, Bedienungs- und Diagnosezwecke. |
| 15 – Jump Host | Bietet Zugriff auf die Anlage via Terminal oder Remote-Kommunikation. |
| 19 – Infrastruktur-PC | Wird für Aktualisierungen von Windows, Virenschutzanwendungen und den Quarantäne-Server eingesetzt. |
| 20 – Anomalieerkennung | Überwacht den Netzwerkverkehr und die Netzwerkressourcen mit Hinsicht auf abnormes Geräteverhalten und Netzwerkkommunikations-Anomalien.<br>Sendet Alarme im Fall von Problemen bei der Netzwerksicherheit. |

| Komponente | Funktion |
|---|---|
| 21 – Log Server mit SIEM-Tool | Zentraler Server zum Speichern aller protokollierten Informationen der Anlage. |
| 22 – SIWA Suite Server | Besteht aus SIWA Optim, LeakControl, Abwassersteuerung, Infrastruktursimulation. |
| 23 – Energy Manager Pro | Energiedatenmanagementsystem zum Erstellen der Grundlage für ein Energiebetriebsmanagement zum Steigern der Energieeffizienz und zum Senken der Energiekosten. |
| 30 – SINEC INS | SINEC INS (Infrastructure Network Services) ist das Softwaretool für häufig benötigte zentrale Netzwerkdienste, insbesondere im Bereich Operational Technology (OT). SINEC INS ist übersichtlich und benutzerfreundlich und sorgt dafür, dass häufig benötigte Dienste wie RADIUS- und Syslog-Server im Netzwerk effizient genutzt werden können. |

**Netzwerkkomponenten**

Tabelle 3-3 – Netzwerkkomponenten

| Komponente | Funktion |
|---|---|
| 6 – SCALANCE XC Series | Router und Switches zum Verbinden der Hostsysteme und eingebetteten Geräte mit Terminalbus und Prozessregelungsnetzwerk. |
| 12 – Front-Firewall | Schützt das Leitsystem vor Zugriffen aus äußeren Zonen wie einem Unternehmens-LAN und ermöglicht hauptsächlich einen zertifikatbasierten, verschlüsselten und authentifizierten Zugriff auf Stationen in der DMZ. |
| 13 – Back-Firewall | Schützt das Produktionsnetzwerk des Leitsystemnetzwerks vor Zugriffen aus dem DMZ-Netzwerk und ermöglicht hauptsächlich einen zertifikatbasierten, verschlüsselten und authentifizierten Zugriff auf einzelne und vertrauenswürdige ferne Stationen/Netzwerke. |
| 26 – SCALANCE SC642-2C | Netzwerkrouter mit Firewall zum Aufbauen einer sicheren Kommunikation zwischen dem Prozessregelungsnetzwerk und S7-1500. |
| 27 – SCALANCE M826-2 | Router für die SHDSL-Kommunikation über private Kommunikationsinfrastruktur. Für die sichere Kommunikation mit fernen Stationen, z.B. Regenwasserbecken 1.<br>Mögliche Kommunikationsprotokolle sind PROFINET, DNP3, IEC 60870-5-104, SINAUT ST7 über TeleControl. |
| 28 – SCALANCE WAM766-1 | IWLAN-Zugangspunkt für die drahtlose PROFINET-Kommunikation auf der Grundlage von IEEE 802.11ax. |
| 29 – SCALANCE WUM763-1 | IWLAN-Client für die drahtlose PROFINET-Kommunikation auf der Grundlage von IEEE 802.11ax. |
| 31 – TIM 1531 IRC | Kommunikationsmodul für die WAN-Fernkommunikation, mögliche Kommunikationsprotokolle sind DNP3, IEC 60870-5-101/104, SINAUT ST7 über TeleControl. |
| 32 – SCALANCE M876-4 | Router für die Kommunikation mittels GSM/UMTS/LTE über private Kommunikationsinfrastruktur. Für die sichere Kommunikation mit fernen Stationen, z.B. externe Zählerstation oder Regenwasserbecken 2. Mögliche Kommunikationsprotokolle sind DNP3 IEC 0870-5-104, SINAUT ST7 über TeleControl. |
| 34 – SCALANCE XF204-2BA | PROFINET-Netzwerkswitch (gemanagt) mit Redundanzmanager zum Anschließen eines PROFINET-Rings / einer PROFINET-Linie an S7-1500. |

**Eingebettete Geräte**

Tabelle 3-4 – Eingebettete Geräte

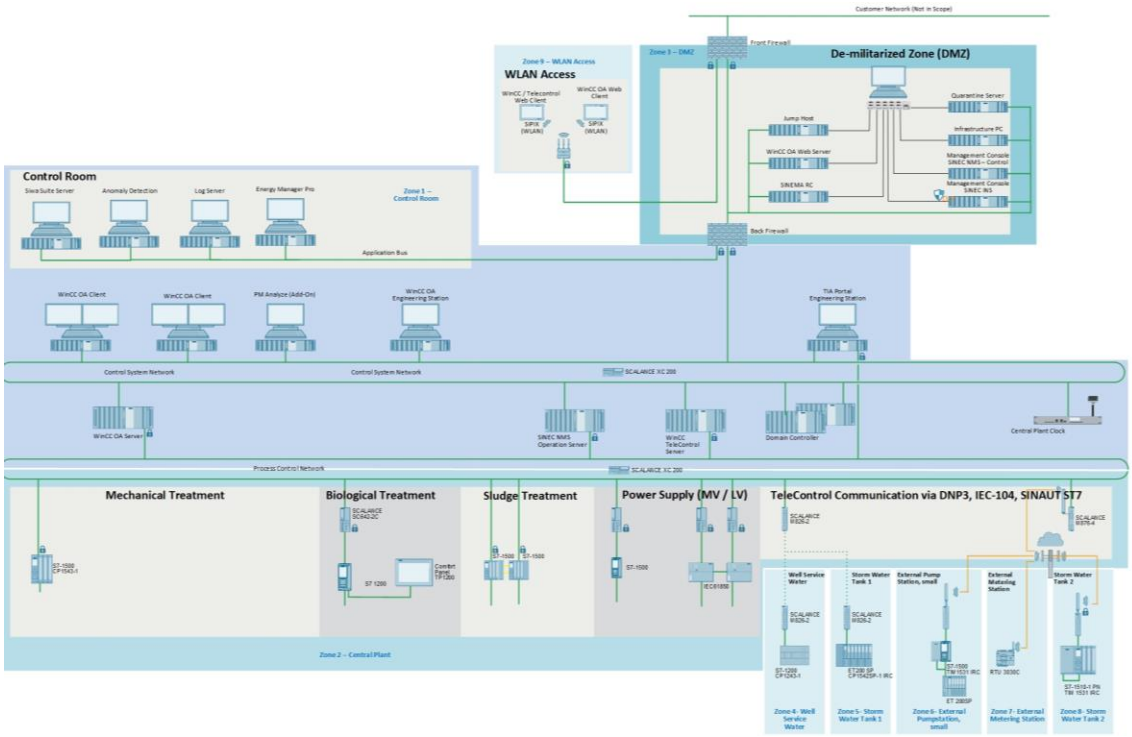
| Komponente | Funktion |
|---|---|
| 24 – S7-1500 (H), Option Redundanz | SPS mit 3 integrierten Schnittstellen für die Kommunikation via PROFINET und/oder Prozessregelungsnetzwerk<br>Optional hohe Verfügbarkeit. |
| 25 – S7-1500 | SPS mit 3 integrierten Schnittstellen für die Kommunikation via PROFINET und/oder Prozessregelungsnetzwerk<br>Optional hohe Verfügbarkeit.<br>CP1543-1 für zusätzliche Sicherheit bei der Kommunikation |
| 27 – S7-1200 | SPS mit zusätzlichem CP1243-8 IRC für Fernwirken und sichere Kommunikation. |
| 33 – RTU3051C | Bedienen und Beobachten kleiner Außenstationen ohne Anschluss an eine Energieversorgungssystem. In TeleControl-Netzwerken dient die RTU zum Verbinden der fernen Stationen mit der Leitwarte über die mobile Kommunikation wie LTE und 5G. |
| 35 – Zeitserver | Relevant für Komponenten mit interner Hardware-Uhr oder Echtzeituhr (RTC), um für das Prozessleitsystem eine Standardzeit vorzugeben. |

## 3.3. Zonen und vorgesehene Betriebsumgebung

Das Musterkonzept einer Abwasserbehandlungsanlage ist in Zonen mit ähnlichen Sicherheitsmerkmalen gegliedert. Eine Übersicht der definierten Zonen ist in Bild 3-3 dargestellt.

Das Bild zeigt auch die physischen Standorte (Serverschränke, Steuerschränke und zentrale Leitwarte) und die Netzwerke (Leitsystemnetzwerk, Anwendungsbus, Perimeternetzwerk (DMZ) und Prozessregelungsnetzwerk) der inneren Zonen.

Bild 3-3 – Übersicht über die Zonen




### 3.3.1. Zentrale Leitwarte

In der zentralen Leitwarte befinden sich die Workstations der Bediener (WinCC OA-Client 1 und 2).

Der Zutritt zur zentralen Leitwarte ist auf autorisiertes Personal beschränkt.

### 3.3.2. Engineering-Raum

Der Engineering-Raum beherbergt die TIA Engineering-Station für die Automatisierungsgeräte sowie die WinCC OA-Engineering-Station.

Der Zutritt zum Engineering-Raum ist auf autorisiertes Personal beschränkt.

### 3.3.3. Serverraum

Der Serverraum beherbergt die Serverschränke, in denen sämtliche Client/Server-Chassis und Firewalls/Switches untergebracht sind. Darüber hinaus beherbergt der Serverraum einen als Einschubgerät ausgeführten KVM-Switch. Dieser fungiert als lokale Konsole für alle Server (DMZ und Leitsystemnetzwerk), die keinen KVM-Bildschirm in der zentralen Leitwarte haben.

Der Zutritt zum Serverraum ist auf autorisiertes Personal beschränkt.

### 3.3.4. Leitsystemnetzwerk

Das Leitsystemnetzwerk umfasst die Server und Clients für das System WinCC OA, wie in der Systemarchitektur Bild 2-3 dargestellt.

Das Leitsystemnetzwerk hat eine Ringtopologie, um eine höhere Verfügbarkeit zu gewährleisten. Dieser Aufbau vermeidet Kommunikationsausfälle, wenn beispielsweise die Leitung beschädigt oder an einer bestimmten Stelle unterbrochen wird.

### 3.3.5. Application Bus

Der Application Bus umfasst die Server für besondere Anwendungen:

- Energy Manager Pro.
- SIWA Suite – Anwendung für die Wasserwirtschaft.

### 3.3.6. Demilitarisierte Zone (DMZ) / Perimeternetzwerk

Die demilitarisierte Zone (DMZ) umfasst die Server, auf die von externen Systemen/Zonen zugegriffen werden muss und umgekehrt:

- SINEC NMS Control UMC.
- Jump Host.
- WinCC OA Web Server.
- SINEMA RC Server.
- Infrastruktur-PC (z.B. Server für Virenscanner, WSUS-Patchserver, Quarantänesystem).
- SINEC INS

Die DMZ existiert nur physisch in den Serverschränken im Serverraum.

### 3.3.7. Prozessregelungsnetzwerk

Das Prozessregelungsnetzwerk verbindet alle Automatisierungsgeräte (z.B. SIMATIC S7-1500-Controller) mit den WinCC OA-Servern, der TIA Engineering-Station und dem SINEC NMS-Server. Die folgenden Hauptstufen des Abwasserreinigungsprozesses werden von eigenen Automatisierungsgeräten gesteuert:

- Mechanische Behandlung.
- Biologische Behandlung.
- Schlammbehandlung.
- Spannungsversorgung (Mittelspannung und Niederspannung).

Es besteht keine Verbindung zwischen Leitsystemnetzwerk bzw. DMZ und Prozessregelungsnetzwerk.

Auch das Prozessregelungsnetzwerk hat eine Ringtopologie. Dieser Aufbau vermeidet Kommunikationsausfälle, wenn beispielsweise die Leitung beschädigt oder an einer bestimmten Stelle unterbrochen wird.

### 3.3.8. Steuerschränke

Steuerschränke enthalten die Automatisierungsgeräte (Controller SIMATIC S7-1500), die sich an verschiedenen physischen Standorten im zentralen Anlagenbereich befinden und mit dem Prozessregelungsnetzwerk verbunden sind.

### 3.3.9. WLAN-Zugang

Die WLAN-Zugangszone ist mit der Front-Firewall verbunden und bietet beschränkten Zugang zu Geräten in der DMZ (normalerweise begrenzt auf HTTPS-Zugang zu Web Server oder über RDP auf einen Terminalserver).

Die WLAN-Zugangspunkte befinden sich auf dem Gelände überall dort, wo es erforderlich ist, und stellen WLAN-Verbindungen für Tablet-PCs oder Mobiltelefone zur Verfügung.

Verbindungen zu den WLAN-Zugangspunkten werden verschlüsselt, weshalb die WLAN-Clients den jeweiligen WLAN-Schlüssel „kennen" müssen, oder sie werden über das Protokoll 802.1x authentifiziert (RADIUS, Beschränkung des Netzwerkzugangs).

### 3.3.10. Externe Pumpstation, (mittel) – Remote-Station

Die Remote-Station dient zum Speisen der Zulaufpumpstation der Abwasserbehandlungsanlage (ABA). Die Kommunikation zwischen dem zentralen Bereich einer Abwasserbehandlungsanlage und Remote-Stationen wird über private Infrastruktur abgewickelt.

Um die Kapselung der Kommunikation zwischen Remote-Station und Prozessregelungsnetzwerk zu gewährleisten, wird der Router SCALANCE XF204-2BA verwendet, einschließlich Adapter VD für variable Distanz.

### 3.3.11. Brunnenwasser/Betriebswasser – Remote-Station

Die Remote-Station liefert Betriebswasser für die Abwasserbehandlungsanlage (ABA). Das Betriebswasser kommt aus Brunnen, die sich normalerweise außerhalb des zentralen Bereichs einer Abwasserbehandlungsanlage befinden. Die Kommunikation zwischen dem zentralen Bereich einer Abwasserbehandlungsanlage und Remote-Stationen wird über private Infrastruktur abgewickelt.

Um die Kapselung der Kommunikation zwischen ferner Station und Prozessregelungsnetzwerk zu gewährleisten, wird der Router SCALANCE M826-2 verwendet.

### 3.3.12. Regenwasserbecken 1 – Remote-Station

Die Remote-Station dient bei Starkregenereignissen zum Verringern der Belastung der nachgeschalteten Abwasserbehandlungsanlage (ABA). Die Kommunikation zwischen dem zentralen Bereich einer Abwasserbehandlungsanlage und Remote-Stationen wird über private Infrastruktur abgewickelt.

Um die Kapselung der Kommunikation zwischen Remote-Station und Prozessregelungsnetzwerk zu gewährleisten, wird der Router SCALANCE M826-2 verwendet.

Die Kommunikation wird über ein Virtual Private Network abgewickelt. Zu diesem Zweck wird eine sichere Verbindung (Tunnel) zwischen zwei geschützten IT-Systemen oder Netzwerken über ein unsicheres Netz eingerichtet. Beide Partner müssen sich beim Öffnen des Tunnels authentifizieren. Während des Betriebs wird die Datenübertragung durch Verschlüsselung gegen Einsichtnahme durch unbefugte Personen und gegen die Einschleusung nicht erkennbarer Änderungen geschützt.

### 3.3.13. Externe Pumpstation (klein) – Remote-Station

Die Remote-Station dient zum Speisen der Zulaufpumpstation der Abwasserbehandlungsanlage (ABA). Die Kommunikation zwischen dem zentralen Bereich einer Abwasserbehandlungsanlage und Remote-Stationen wird über LTE (4G) abgewickelt.

Um die Kapselung der Kommunikation zwischen Remote-Station und Prozessregelungsnetzwerk zu gewährleisten, wird der Router SCALANCE M876-4 verwendet.

### 3.3.14. Externe Zählerstation – Remote-Station

Die Remote-Station dient zum Messen der aus Wohn- und Gewerbegebäuden kommenden Wassermenge, die über das öffentliche Abwasserkanalnetz herangeführt wird. Die Kommunikation zwischen dem zentralen Bereich einer Abwasserbehandlungsanlage und Remote-Stationen wird über öffentliche Netzwerke abgewickelt.

Um die Kapselung der Kommunikation zwischen Remote-Station und Prozessregelungsnetzwerk zu gewährleisten, wird der Switch SCALANCE M876-4 verwendet.

### 3.3.15. Regenwasserbecken 2 – Remote-Station

Die Remote-Station dient bei Starkregenereignissen zum Verringern der Belastung der nachgeschalteten Abwasserbehandlungsanlage. Die Kommunikation zwischen dem zentralen Bereich einer Abwasserbehandlungsanlage und Remote-Stationen wird über öffentliche Netzwerke abgewickelt. Um die Kapselung der Kommunikation zwischen Remote-Station und Prozessregelungsnetzwerk zu gewährleisten, wird der Switch SCALANCE M876-4 verwendet.

### 3.3.16. Externe Zonen

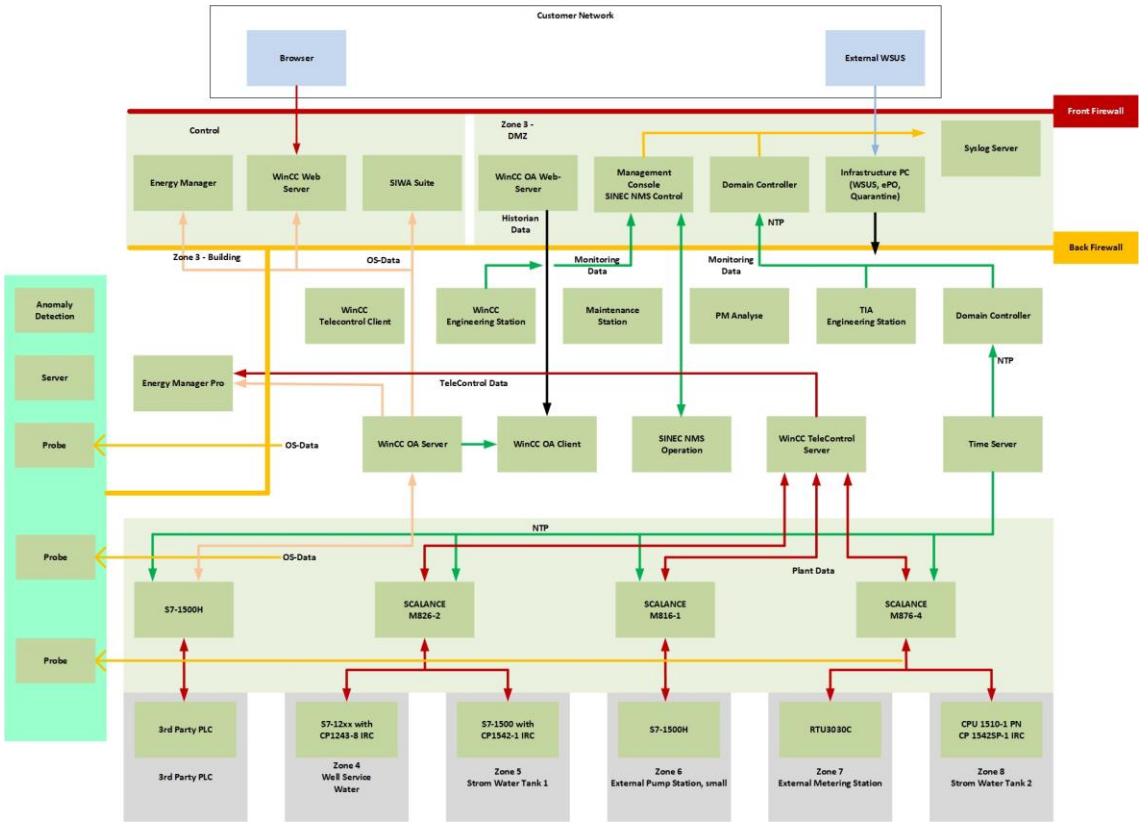
Das Musterkonzept der Abwasserbehandlungsanlage verfügt über zwei externe Zonen: Unternehmensnetzwerk (WAN) undInternet/UT

Diese Zonen stellen konventionell Aktualisierungsdienste für die in der DMZ laufenden Anwendungen bereit. Die dafür notwendigen Netzwerkverbindungen für diese Dienste werden konventionsgemäß von der DMZ als Initiator (Quelle) zum jeweiligen Dienstanbieter (Ziel) im Unternehmensnetzwerk hergestellt. Einige wenige Dienste wie Web oder Remote Desktop Clients werden vom Unternehmensnetzwerk als Initiator zur DMZ hergestellt (Aktualisierungen für Windows, Virenerkennungsmuster).

## 3.4. Datenaustausch zwischen Zonen

Eine allgemeine Übersicht über den Datenverkehr und die Verbindungen zwischen den Servern und Anwendungen in den jeweiligen Zonen ist im folgenden Bild dargestellt.

Bild 3-4 – Übersicht über den Datenaustausch



# 4. Schutzziele

Die Schutzziele, was Vertraulichkeit, Integrität und Verfügbarkeit anbelangt, können von Anlage zu Anlage unterschiedlich sein. Aufgrund dieser Unterschiede muss für jede Anlage und für jedes Automatisierungs- und Leitsystemprojekt eine individuelle Bedrohungs- und Risikoanalyse durchgeführt werden. Diese sollte als Delta-Analyse zusätzlich zu der hier beschriebenen Bedrohungs- und Risikoanalyse erfolgen.

Für das generische Musterkonzept einer Abwasserbehandlungsanlage wurden die folgenden Daten und Funktionalitäten als sensibel hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit identifiziert, siehe hierzu folgende Tabelle:

Tabelle 4-1 – Schutzziele

| Schutzziele | Beschreibung der Schutzziele | Zugehörige Hauptkomponenten / Assets |
|---|---|---|
| Vertraulichkeit | • Benutzerpasswörter<br>• Prozessdaten<br>• Informationen über Kunden-Assets<br>• Interne Prozessdaten werden öffentlich, z.B. Messdaten zur Wirksamkeit der Reinigungsprozesse<br>• Projekt-Engineering-Daten in Skripten und Panels | • Domain Controller<br>• WinCC OA-Server, S7-1500-Controller |
| Integrität | • Historian-Daten<br>• Messdaten<br>• Integrität des Wasserbehandlungsprozesses (z.B. Verwendung der richtigen Chemikaliendosierung)<br>• Projektkonfiguration und Engineering-Daten<br>• Integrität des Gasprozesses (Methan) | • PM Analyze<br>• WINCC OA-Server, WinCC OA-Engineering-Stationen<br>• WinCC OA Engineering, S7-1500-Controller<br>• SINEC NMS<br>• S7-1500-Controller, WinCC OA-Engineering-Station |
| Verfügbarkeit | • Verfügbarkeit der Abwasserbehandlungsanlage<br>• Verfügbarkeit von Regenwasserbecken / Kanalnetz / Zulaufpumpstation (Absperrschieber)<br>• Flotation, Faulturm (Bakterien) | • S7-1500-Controller<br>• S7-1500-H-Controller<br>• S7-1200-Controller<br>• WinCC OA-Server / -Client |

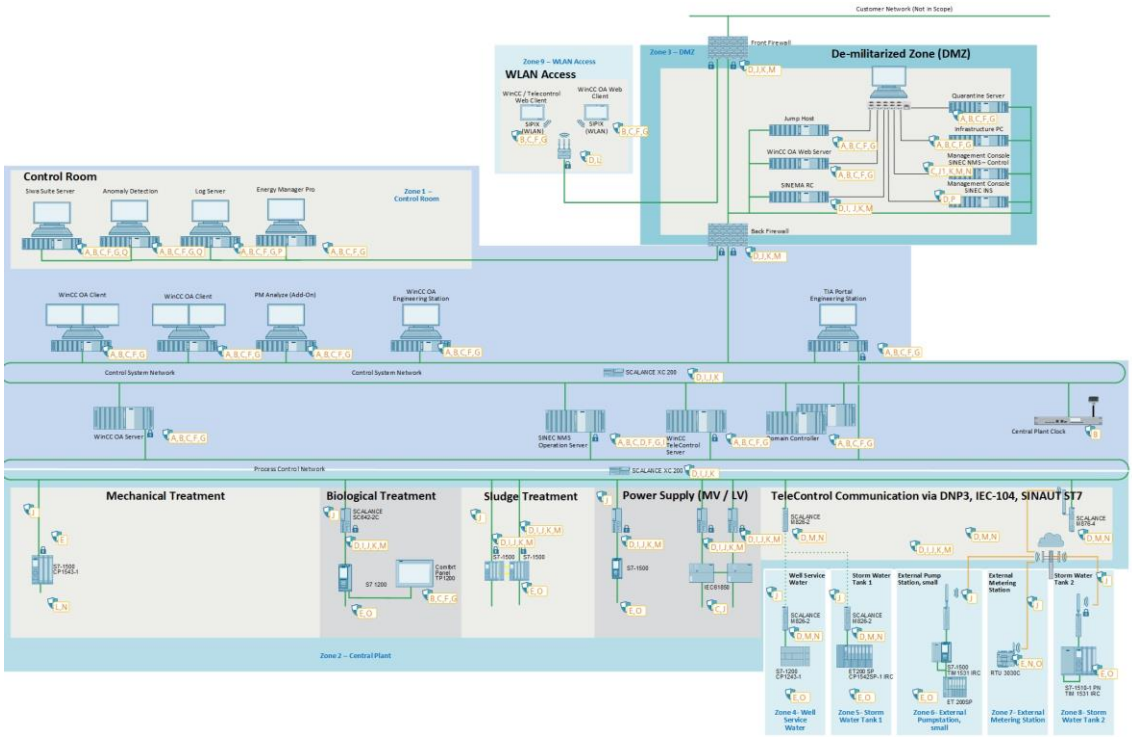
Für die genannten Schutzziele wird die Auswirkung auf die Anlage im Fall von Verletzungen der Vertraulichkeit, Integrität und Verfügbarkeit bewertet, und die Priorität der resultierenden Maßnahmen wird durch eine Bedrohungs- und Risikoanalyse ermittelt.

Die folgende Grafik zeigt die Schutzziele der einzelnen Komponenten in der Zonenübersicht.

Bild 4-1 – Legende der Schutzziele

| | |
|---|---|
| A | Operating system hardening, e.g. via dedicated operating system build, security policies, ... |
| B | Operating system and IACS patch management |
| C | Antivirus pattern management, endpoint security, application whitelisting |
| D | Firmware patch management for network and security devices |
| E | AS Firmware Update |
| F | Identity and access management for Windows user roles and accounts, aligned IACS roles and accounts, password policies |
| G | Operating system backup and restore (backup server project specific) |
| H | IACS project / data backup and restore (backup server project specific) |
| I | Central network and network security and device management and backup (backup server project specific) |
| J | Security zones and cells, zone and cell protection via network segmentation, firewalls |
| K | Restriction of IP addresses, restrictions of services / ports, packet inspection |
| L | WLAN encryption, layer 2 tunnel, WLAN iPCF |
| M | Encrypted communication between security zones / cells |
| N | Encrypted IPSec VPN for remote communication |
| O | Field Interface Security |
| P | Monitoring and Logging |
| Q | Industrial Anomaly Detection |

Bild 4-2 – Schutzziele für Zonen




Für dieses Musterkonzept wurde eine generische Bedrohungs- und Risikoanalyse durchgeführt. Diese kann Hinweise auf mögliche Bedrohungen und Risiken geben, die Bedrohungs- und Risikoanalyse muss jedoch für jede Anlage individuell durchgeführt werden.

## 4.1. Physischer Zugang

**Perimetersicherheit**

***Zugang zur Anlage zur Sabotage von Arbeitsvorgängen/Prozessen*** → Umzäunung und Barrieren, Überwachungskameras und Beleuchtung, Sicherheitspersonal.

***Physische Störung/Manipulation ferner Stationen*** → Umzäunung, Überwachungskameras und Beleuchtung.

***Manipulation kritischer Infrastrukturen, z.B. Notstromversorgungssysteme*** → Manipulationssichere Siegel zur Erkennung unbefugter Zugangsversuche.

**Gesicherte Teile und Gebäude**

***Zugang zum zentralen Standort/zu den Gebäuden für Angreifer*** → Zutrittskontrolle, 2-Faktor-Authentifizierung für den Zugang.

***Physischer Zugriff zum Diebstahl von Daten*** → Überwachung aller Assets, unterschiedliche Zugriffsebenen (für Mitarbeiter) auf die verschiedenen Bereiche der Anlage, Sicherung/Verriegelung von Serverräumen und Schaltschränken.

***Physischer Zugriff zum Diebstahl/zur Zerstörung von Hardware*** → Sicherung/Verriegelung aller Hardwarekomponenten.

***Schadprogramme / Sabotage durch Fremdpersonal*** → Vertragsmanagement, Hintergrundüberprüfungen von Fremdpersonal, das Zugang zur Anlage benötigt.

**Ungesicherte / freiliegende Teile und Gebäude / ferne Stationen (Ventile, Behälter, Pumpen, Zählerstationen...)**

***Angreifer können sich Zugang zu diesen weniger gesicherten Netzwerken verschaffen*** → System- und Kommunikationsüberwachung in SCADA.

***Angreifer können diese Stationen zerstören / deaktivieren*** → Redundante externe Systeme (Brunnen, Pumpen etc.)

***Angreifer können Daten in diesen Stationen verändern*** → Als ungesicherte Teile behandeln, zulässige Kommunikation wird minimiert.

**Netzwerk- und Windows-PCs**

***Prozessregelungsnetzwerk / Leitsystemnetzwerk ist gesichert, aber der Zugriff wäre kritisch*** → Überwachung von Netzwerkkomponenten, 802.1x, Industrial Anomaly Detection.

***Möglicherweise ungepatchte Sicherheitslücken in Windows*** → Updates und/oder Application Whitelisting.

## 4.2. Stromversorgungssystem

***Stromversorgung aus dem öffentlichen Netz*** → System überwachen, Backup-System bereitstellen.

***Interne USV*** → Backup-System muss überwacht und instandgehalten werden.

## 4.3. Firewall

**Mit Kontakt zum Internet, höchste Sichtbarkeit selbst für Scriptkiddies** → Sichere Projektierung.

***Kritischer Netzwerkteil*** → Dauerhafte zentrale Überwachung von Firewall-Protokolldaten / Anomalieerkennung

## 4.4. Interne und organisatorische Maßnahmen

***Zugang zu Infrastruktur-PCs, interne Manipulation möglich*** → Mitarbeiterschulung, organisatorische Verfahren.

***Zugang zu Betriebs-PCs, interne Manipulation möglich*** → Mitarbeiterschulung, organisatorische Verfahren.

***Ungesicherte USB-Ports*** → Systemhärtung, Deaktivierung von USB-Ports.

***Software-Updates können die ordnungsgemäße Funktionalität des Betriebssystems beeinträchtigen*** → Application Whitelisting (kann eine Option anstelle von Updates sein).

# 5. Sicherheitsmaßnahmen

Für das Musterkonzept der Abwasserbehandlungsanlage werden Sicherheitsmaßnahmen ausgewählt, um Sicherheitsanforderungen zu erfüllen und alle hohen Risiken, die im Zuge der konzeptspezifischen Bedrohungs- und Risikoanalyse identifiziert wurden, zu mindern. Die ausgewählten Sicherheitsmaßnahmen werden nach technischen Bereichen gegliedert, entsprechend ihrem jeweiligen Beitrag zur Gesamtsicherheit der Sicherheitsauslegung des Musterkonzepts und zur Abdeckung aller wichtigen Aspekte der anwendbaren Spezifikationen nach die IEC 62443.

Die in den folgenden Abschnitten beschriebenen Sicherheitsmaßnahmen gelten nur für das Musterkonzept einer Abwasserbehandlungsanlage und die definierten Schutzziele. Für andere Lösungen können die Sicherheitsmaßnahmen unterschiedlich sein, je nach Schutzzielen und hohen Risiken, die im Zuge der Bedrohungs- und Risikoanalyse identifiziert wurden.

## 5.1. Sichere Netzwerkauslegung

Ein Element zum Schutz der Automatisierungs- und Leitsysteme und der Netzwerke ist Netzwerksicherheit. Die Netzwerke von Automatisierungs- und Leitsystemen müssen vor unbefugtem Zugriff geschützt werden und die Schnittstellen zu anderen Netzwerken, z.B. zum Büronetzwerk oder für die Fernwartung über das Internet, müssen gesteuert, überwacht und auf die notwendige Kommunikation beschränkt werden, indem geeignete Technologien wie Firewalls zum Einsatz kommen.

### 5.1.1. Netzwerksegmentierung

| | |
|---|---|
| **IEC 62443-3-3** | **SR 5.1 Netzwerksegmentierung**<br>Gemäß SR 5.1 RE 1 – Physische Netzwerksegmentierung<br>SR 5.1 RE 2 Unabhängigkeit von nicht-automatisierungstechnischen Netzwerken |

Als Teil der Implementierung einer Defense-in-Depth-Abwehr wird das Automatisierungssystem in Sicherheitszonen segmentiert, wie in Abschnitt 0 dargestellt. Die Zonen sind so aufgeteilt, dass Systemkomponenten mit ähnlichen Kommunikations- und Schutzbedürfnissen in einer Zone zusammengefasst sind. Die Grenze zwischen Zonen wird als Vertrauensgrenze bezeichnet, und die Kommunikation zwischen diesen Zonen muss überwacht und gesteuert werden, siehe Abschnitt 5.1.2.

Für das Musterkonzept wird die Segmentierung zwischen zentraler Anlagenzone und ferner Zone forciert. Das Netzwerk ist in ein Leitsystemnetzwerk und ein Prozessregelungsnetzwerk unterteilt, an die jeweils zwei PCs, einschließlich Firewalls, angeschlossen sind. Diese Server-PCs können Daten an übergeordnete Systeme verteilen.

Die zentrale Anlagenzone, einschließlich des Prozessregelungsnetzwerks, überspannt den gesamten Anlagenbereich, allerdings im Vergleich zur Gebäudezone mit einem niedrigeren physischen Schutzgrad. Sie verbindet die untergeordneten Teilsystemzonen (Zone 4 bis Zone 8 in Bild 3-3) mit dem System WinCC OA in der zentralen Anlagenzone, wobei die Kommunikation zwischen diesen Zonen über verschlüsselte virtuelle Privatnetzwerke stattfindet.

Teilstationen an fernen Standorten außerhalb des physischen Perimeters der Hauptanlage müssen über einen angemessenen physischen Schutz verfügen, da in diesen Teilstationen kein Personal anwesend ist. Das Netzwerk dieser Teilstationen selbst stellt eigene Zonen dar, die über verschlüsselte virtuelle Privatnetzwerke mit dem zentralen TeleControl-Server verbunden sind. Dadurch soll sichergestellt werden, dass ein angemessener Schutzgrad für die Kommunikation über das Prozessregelungsnetzwerk sichergestellt ist.

Sämtliche Kommunikation zwischen externen Zonen und der Wasserbehandlungsanlage, z.B. über das Büronetzwerk eines Betreibers oder per Fernzugriff, muss die DMZ passieren. Die DMZ wird ebenfalls als separate Zone implementiert, die mit der Gebäudezone verbunden ist.

Die als Teil dieses Musterkonzepts implementierte Netzwerksegmentierung entspricht den Empfehlungen in:

- \25\ - WinCC OA Security Guideline (Chapter 6.1: Security Cells and Network Architecture)
- \2\ – Rundum-Schutz mit Industrial Security – Netzwerksicherheit

### 5.1.2. Schutz der Zonengrenzen

| | |
|---|---|
| **IEC 62443-3-3** | **Gemäß SR 5.2 – Schutz der Zonengrenzen**<br>**SR 5.2 RE 1 Deny by default, allow by exception**<br>SR 5.2 RE 2 Inselmodus |

Sämtliche Kommunikation zwischen den Sicherheitszonen muss überwacht und gesteuert werden. Um die erforderlichen Kommunikationsregeln durchzusetzen und eine sichere Kommunikation zwischen den verschiedenen Zonen zu gewährleisten, werden Firewalls mit VPN-Funktionalität (IPsec) als Sicherheitsmaßnahme eingesetzt. Sämtlicher unbekannter Netzwerkverkehr, der aufgrund einer Firewall-Regel nicht zulässig ist, wird von diesen Netzwerkgeräten blockiert, da die Firewall-Richtlinie das Prinzip 'Grundsätzlich ablehnen, Ausnahmen zulassen' verfolgt.

Zum Schutz der Außengrenze des Anlagennetzwerks bieten DMZ-Hosts zusätzliche Kontrollmechanismen auf Anwendungsebene, da die gesamte Kommunikation aus externen Zonen in der DMZ abgefangen wird. Dadurch wird sichergestellt, dass ein direkter Zugang zu internen Komponenten der, z.B. direkter Engineering-Zugang, nicht möglich ist. Stattdessen werden Proxies oder Hosts in der DMZ verwendet. Das schließt beispielsweise Web-Zugriff auf die HMI, Kommunikation über OPC-UA mit zentraler Steuerung oder die kontrollierte Übertragung von Sicherheitsaktualisierungen zur Prüfung und anschließenden Installation in der Anlage ein.

Die Kommunikation über das Prozessregelungsnetzwerk zwischen den WinCC OA-Servern und den fernen Stationen wird durch SCALANCE S Firewall Appliances geschützt. Diese wenden zudem strenge Firewall-Regeln an, um die Angriffsfläche des Prozessregelungsnetzwerks bei der Kommunikation mit verbundenen fernen Standorten zu reduzieren.

Neben den netzwerkbasierten Firewalls müssen auch die PC-basierten Host-Firewalls genutzt werden, um eine zusätzliche Schutzschicht zu bieten. Die Projektierung der Host-Firewall muss bei der Installation von WinCC OA erfolgen.

Empfohlene Projektierungen (Regelsätze) für Front-Firewall und Back-Firewall sowie für die SCALANCE-Sicherheitsnetzwerkgeräte, über die ferne Stationen für das Musterkonzept einer Wasserbehandlungsanlage angebunden werden, werden in den Abschnitten 6.2, 6.3 und 6.4 beschrieben.

Die obigen Maßnahmen zum Schutz der Zonengrenzen des Musterkonzepts werden weiter ergänzt durch adaptierbare Maßnahmen zur Sicherheitsprotokollierung und Überwachung, die in Abschnitt 5.6 ausführlich beschrieben werden.

### 5.1.3. Netzwerkzugriffsschutz

| | |
|---|---|
| **IEC 62443-3-3** | **SR 2.2 Nutzungskontrolle von Funkverbindungen**<br>SR 2.2 RE 1 Nicht genehmigte drahtlose Geräte erkennen und anzeigen |

Zwar schützen Firewalls die Netzwerkzonen an den Außengrenzen, doch auch lokaler Zugriff auf das Netzwerk kann für Angriffe ausgenutzt werden. In diesem Kontext müssen einige zusätzliche Aspekte berücksichtigt werden:

- Beschränkung des Zugriffs mit mobilen Geräten wie Laptops von Servicetechnikern.
- WLAN-Zugriffsschutz

Benutzer, Softwareprozesse oder Geräte, die über drahtlose Kommunikation zugreifen, müssen identifiziert und authentifiziert werden. Eine allgemein akzeptierte Sicherheitsmaßnahme ist die Verwendung moderner Sicherheitsprofile mit starker Authentifizierung und Verschlüsselung nach dem Standard 802.11 für die Drahtloskommunikation. Diese Maßnahme dient dazu, den Zugriff zu authentifizieren und zu autorisieren und Nutzungsbeschränkungen für Drahtlosverbindungen durchzusetzen und zu überwachen.

Gängige Maßnahmen zum Schutz gegen unbefugten Zugriff auf das Netzwerk über portable und mobile Geräte (z.B. Laptops, Tablets und Smartphones) sind das Härten der eingesetzten Netzwerkgeräte und das Schließen/Deaktivieren ungenutzter Ethernet-Anschlüsse. Als Vorkehrung für portable Geräte empfehlen wir, den Zugriff auf das WLAN nur mit ordnungsgemäßer Benutzerauthentifizierung zu gestatten.

Die Härtungsmaßnahmen und die Konfiguration der Drahtlosgeräte für das Musterkonzept werden in Abschnitt 6.3 beschrieben.

### 5.1.4. Administration der Netzwerkgeräte

Eine sichere Administration und Konfiguration der Netzwerkgeräte ist von höchster Wichtigkeit wegen der zentralen Rolle dieser Geräte für die Verfügbarkeit der internen und externen Kommunikation einer Anlage sowie ihrer potentiellen Funktion zur Realisierung und Durchsetzung einer Netzwerksegmentierung.

Alle administrativen Zugriffe auf Geräte (z.B. Router, Switches, Firewalls, WLAN-Zugangspunkte), die im Rahmen des Musterkonzepts eingesetzt werden, geschehen anhand von Kommunikationsprotokollen, die durch neueste kryptographische Verfahren geschützt sind (entweder webbasiert oder über HTTPS oder SSH), mit beidseitiger Authentifizierung und starker Verschlüsselung aller ausgetauschten Daten. Ungesicherte Altmethoden wie HTTP oder Telnet – wenn überhaupt unterstützt – sind standardmäßig deaktiviert.

Die Verwaltung des menschlichen Benutzerzugriffs auf solche Geräte erzwingt eine rollenbasierte Zugriffssteuerung, wobei die Zugriffsrechte der Benutzer auf ein Minimum eingeschränkt werden. Administrativer Zugriff wird auf autorisiertes Personal beschränkt.

Darüber hinaus sind Benutzerverwaltung und Zugriffssteuerung für administrativen Zugriff in eine zentralisierte Kontenverwaltung auf der Grundlage von Active Directory integriert. Hierbei erlaubt das Netzwerkmanagementsystem SINEC NMS eine zentrale Administration und Aktualisierung der Firmware aller verwalteten SCALANCE-Netzwerkgeräte, siehe Abschnitt 0.

### 5.1.5. Schutzmaßnahmen gegen Dienstblockade

| | |
|---|---|
| **IEC 62443-3-3** | SR 7.1 Schutz gegen DoS-Ereignisse |

Zum Schutz der Lösungen für das Musterkonzept vor Angriffen in Form einer Dienstblockade (Denial of Service, DoS) müssen zwei Hauptaspekte betrachtet werden.

Einerseits kann DoS auf die Gesamtverfügbarkeit des Anlagennetzwerks oder einzelner Geräte abzielen, zum Beispiel durch Überflutung mit überflüssiger Netzwerkkommunikation. Hier erfordert die Automatisierungslösung die Fähigkeit, den Betrieb während eines DoS-Ereignisses in einem Notfallmodus fortzusetzen.

Andererseits müssen Komponenten, die sichere Zonen schützen oder in geschützten Zonen stationiert sind und kritische Rollen in der Prozessregelung übernehmen, eine nachgewiesene Robustheit gegenüber missgebildeten Netzwerkpaketen und Angriffen auf Netzwerkebene aufweisen und solche Pakete entweder ignorieren oder in einen definierten Zustand wechseln.

Hauptmaßnahmen zum Schutz gegen DoS-Angriffe im Musterkonzept:

- Palo Alto Firewalls (Frontend und Backend) zum allgemeinen Schutz gegen gewöhnliche DoS-Angriffe auf Netzwerkebene. Härtungsmaßnahmen und Konfiguration der Palo Alto Firewalls werden in Abschnitt 6.2.1 beschrieben.
- Als Teil des Gesamtkonzepts für Industrial Security in den Automatisierungssystemen von Siemens umfasst der Entwicklungsprozess aller Automatisierungsgeräte und -software Sicherheitsüberlegungen und regelmäßige Penetrationstests.
- \25\ - WinCC OA Security Guideline (Chapter 6.2.2.5: Usage of WinCC OA mxProxy and restriction of open ports)
- \25\ - WinCC OA Security Guideline Chapter 6.2.2.21: Keep secure settings in WinCC OA config file)

## 5.2. Identitäts- und Zugriffsmanagement

Benutzeridentifizierung und -authentifizierung wird unterstützt und muss an allen Schnittstellen, die menschlichen Benutzerzugriff bieten, erzwungen werden. Zu den menschlichen Benutzerschnittstellen zählen:

- Bedienerkonten für Anwendungen mit Benutzerschnittstellen (z.B. HMI-Client, Web-Schnittstellen).
- Betriebssystemkonten.
- Engineering-Konten (z.B. WinCC OA Engineering-Station, TIA Engineering-Station).
- Konten für administrativen Zugriff auf Netzwerkgeräte.
- Benutzerkonten für Automatisierungsgeräte (Online-Anbindung an SIMATIC S7-1500-Controller, Zugriff auf den Web Server, Zugriff auf den OPC UA Server etc.).

Die Benutzerverwaltungs- und Authentifizierungslösungen, die für das Musterkonzept der Abwasserbehandlungsanlage verwendet werden, werden in Abschnitt 7 beschrieben.

## 5.2.1. Authentifizierungsmechanismen für Benutzer und Komponenten

| | |
|---|---|
| **IEC 62443-3-3** | SR 1.1 Identifizierung und Authentifizierung von menschlichen Benutzern |
| | SR 1.1 RE1 Eindeutige Identifizierung und Authentifizierung |
| | SR 1.1 RE2 Multifaktor-Authentifizierung über nicht vertrauenswürdige Netzwerke |
| | SR 1.1 RE3 Kontenverwaltung |
| | SR 1.2 Identifizierung und Authentifizierung von Softwareprozessen und Geräten |
| | SR 1.2 RE1 Eindeutige Identifizierung und Authentifizierung |
| | SR 1.8 PKI-Zertifikate (Public-Key-Infrastruktur) |
| | SR 1.9 Stärke der Authentifizierung durch öffentliche Schlüssel |
| | SR 1.9 RE1 Hardwaresicherheit für die Authentifizierung durch öffentliche Schlüssel |
| | SR 1.10 Rückmeldung vom Authentifikator |
| | SR 1.11 Erfolglose Anmeldeversuche |
| | SR 1.12 Nutzungshinweis |

**Betriebssysteme**

Für den Betriebssystemzugriff werden personalisierte Windows-Benutzerkonten und Gruppen verwendet. Diese können von einem Active Directory (Windows Domain), das alle an Leitsystemnetzwerk, Anwendungsbus und DMZ-Netzwerke angeschlossenen windowsbasierten Rechner abdeckt, zentral verwaltet werden. Siehe Abschnitt 7.1.

Ausnahmen für personalisierte (eindeutige) Konten sind abhängig von Projektierung und Betriebsverfahren. Hierunter fallen typischerweise Konten für Rechner, die dauerhaft betriebsfähig sein müssen und von mehreren Personen, wie Bedienern der Leitwarte, genutzt werden. In diesen Szenarien ist es wichtig, dass lokale Notfallmaßnahmen und kritische Leitsystemfunktionen nicht durch Identifikations- oder Authentifizierungsprozesse behindert werden.

**Anwendungsfälle**

Für den Zugriff auf Anwendungsebene (z.B. auf WinCC OA-Clients) wird die Benutzerauthentifizierung und die Kontoverwaltung von einem Active Directory Server gehandhabt. Alle persönlichen Benutzerkonten an Komponenten werden Domaingruppen zugewiesen. TIA Portal unterstützt UMC (User Management Component), wodurch Engineering-Konten in den Gesamtdienst von Active Directory integriert werden können.

**Netzwerkgeräte**

Sicherer Zugriff auf Netzwerkgeräte wird in Abschnitt 5.1.4 beschrieben und kann mit den in Active Directory verwalteten Gruppen und Benutzern über den UMC-Server in SINEC NMS integriert werden. Der auf SINEC INS gehostete RADIUS-Server stellt den administrativen Zugriff auf die SCALANCE-Geräte zur Verfügung.

Um zu verhindern, dass Administratoren bei einem Ausfall des Authentifizierungsservers ausgesperrt werden, können auf Netzwerkgeräten lokale Benutzerkonten als Backup-Authentifizierungsmechanismus angelegt werden. Diese lokalen Konten können mit Multifaktor-Authentifizierung für die unten aufgeführten SCALANCE-Geräte konfiguriert werden.

Tabelle 5-1 – Zwei-Faktor-Authentifizierung für SCALANCE-Geräte

| Gerät | Mindest-Firmware-Version |
|---|---|
| SCALANCE SC622-2C | V3.1 |
| SCALANCE SC632-2C | V3.1 |
| SCALANCE SC636-2C | V3.1 |
| SCALANCE SC642-2C | V3.1 |
| SCALANCE SC646-2C | V3.1 |
| SCALANCE M800 | V8.0 |
| SCALANCE S615 | V8.0 |

**Automatisierungsgeräte**

Der Zugriff auf SIMATIC-Controller erfolgt benutzerbasiert. So wird sichergestellt, dass Benutzer, die eine Verbindung herstellen möchten, eindeutig identifiziert und authentifiziert werden.

Ausnahmen, die eine gruppenbasierte Authentifizierung erfordern, können über den konventionellen Zugriff des Controllers realisiert werden. Dieser beruht auf Passwörtern, die verschiedenen Zugriffsebenen zugewiesen sind.

Weitere Informationen zur Zugriffskontrolle auf SIMATIC-SPSen sind in Abschnitt 6.10 zu finden.

- \25\ – WinCC OA Security Guideline (Chapter 6.2.2.9: Activate Kerberos encryption for WinCC OA systems)
- \25\ – WinCC OA Security Guideline (Chapter 6.4.1: Usage of TLS/SSL for plant communication)
- \25\ – WinCC OA Security Guideline (Chapter 6.4.1.5: Enforce usage of strong cipher suite)
- \25\ – WinCC OA Security Guideline (Chapter 6.4.3: User Administration)
- \25\ – WinCC OA Security Guideline (Chapter 6.4.3.2.1: Usage of Operating system (Windows or Linux) based user management)
- \25\ – WinCC OA Security Guideline (Chapter 6.4.3.3: Single Sign On)
- \25\ – WinCC OA Security Guideline (Chapter 6.4.3.5.2: Server-side Authentication for Managers with session binding)
- \25\ – WinCC OA Security Guideline (Chapter 6.4.8: Configure System Use Notification)
- \44\ – Aktivierung der Zwei-Faktor-Authentifizierung für SCALANCE-Geräte

## 5.2.2. Verwaltung von Kennungen und Berechtigungen

**IEC 62443-3-3**

**SR 1.3 Kontenverwaltung**
**SR 1.3 RE 1 Einheitliche Kontenverwaltung**
**SR 1.4 Kennungsverwaltung**
**SR 1.5 Verwaltung der Authentifikatoren**
**SR 1.6 Verwaltung drahtloser Zugriffsverfahren**
SR 1.6 RE1 Eindeutige Identifizierung und Authentifizierung

**Active Directory**

Die Zentralisierung der Kontenverwaltung reduziert den Administrationsaufwand. Das Microsoft Active Directory wird im gesamten Musterkonzept für die Windows-basierten Host-Systeme im Automatisierungsnetzwerk eingesetzt. Das Musterkonzept unterstützt die Verwaltung von Kennungen (z.B. Benutzername, Hostname) und Passwörter für die Konten der Windows Domain über die Windows AD Domain Controller. Dies schließt Mechanismen für Wiederstellung und Rücksetzung von Passwörtern ein.

Durch zentralisierte Verwaltung und Integration in die Domain Controller erübrigt sich eine lokale Verwaltung an Maschinen.

**User Management Component (UMC)**

UMC wird im Musterkonzept eingesetzt, um die Benutzerverwaltung für die Software-, Netzwerk- und Automatisierungsgeräte von Siemens zu zentralisieren, und kann mit dem Active Directory von Microsoft verbunden werden.

SINEC NMS unterstützt UMC und kann in Kombination mit SINEC INS für die zentrale Benutzerverwaltung von SCALANCE-Netzwerkgeräten eingesetzt werden. Weitere Informationen zu SINEC NMS sind in Abschnitt 0 zu finden.

Bei Automatisierungsgeräten kann die Benutzerverwaltung global über UMC (für S7-1500-Controller mit FW 4.0 und höher) oder lokal über die Benutzerverwaltung und Zugriffssteuerung von TIA abgewickelt werden.

**Benutzerverwaltung und Zugriffssteuerung (UMAC)**

Die Benutzerverwaltung und Zugriffssteuerung des TIA Portals bietet eine zentrale Lösung für die Verwaltung aller benutzerbezogenen Aufgaben innerhalb eines Projekts. Es können Richtlinien festgelegt werden, um starke Passwörter durch eine Mindestlänge und verschiedene Zeichentypen zu forcieren.

Die Verwaltung weiterer Sicherheitsberechtigungen, z.B. zum Einrichten einer sicheren Kommunikation, wird ausführlich in den jeweiligen Produktsicherheitshandbüchern für WinCC OA beschrieben. Sie wird unterstützt durch eine Reihe von Tools und Managementkonsolen.

- \25\ – WinCC OA Security Guideline (Chapter 6.2.2.9: Activate Kerberos encryption for WinCC OA systems)
- \25\ – WinCC OA Security Guideline (Chapter 6.2.1.6: Delete or disable unneeded default users on OS Level)
- \25\ – WinCC OA Security Guideline (Chapter 6.2.2.16: Limit usage of the root user)
- \25\ – WinCC OA Security Guideline (Chapter 6.4.3.3: Single Sign On)

## 5.2.3. Kontenverwaltung und Projektierung von Zugriffsrechten und Privilegien

Die Handhabung der Kontenverwaltung (Benutzer und Gruppen) findet über das Active Directory statt. Zugänge mit den wenigsten Berechtigungen sollten eingerichtet werden, um Benutzern nur das Mindestmaß an Zugriff oder Berechtigungen zu gewähren, das sie benötigen, um ihre jeweiligen Aufgaben auszuführen und somit das Risiko einer unbefugten und unbeabsichtigten Nutzung von Diensten oder Systemen zu reduzieren. Nicht verwendete Standard-Systemkonten, die für die Erstinstallation von Anwendungen, Systemen, Geräten usw. verwendet wurden, sollten entfernt werden.

UMC wird für die zentrale Benutzerauthentifizierung eingesetzt, kann aber keine Autorisierung von Benutzern vornehmen. Daher müssen die Zugriffsrechte für ein TIA Portal-Projekt (Engineering-Rechte) und für Automatisierungsgeräte (Laufzeitrechte) im TIA Portal-Projekt selbst konfiguriert werden.

## 5.2.4. Steuerung des Zugriffs über nicht vertrauenswürdige Netzwerke (Fernzugriff)

Da die Lösung im Musterkonzept durch Firewalls und eine DMZ geschützt wird, besteht keine Zugriffsmöglichkeit für Benutzer aus externen Netzwerken, die standardmäßig als nicht vertrauenswürdig eingestuft sind. Zugriff ist nur möglich über Rechner in der DMZ, die speziell projektiert und geschützt sind, um den Zugriff auf Anwendungsebene zu erlauben. Remote-Benutzer benötigen daher Benutzerkonten mit besonderen Berechtigungen; alle derartigen Konten werden ebenfalls durch Active Directory kontrolliert.

Wenn SINEMA Remote Connect in der DMZ installiert ist, kann ein Fernzugriff realisiert werden. In Kombination mit einer Jump Host-Lösung wird ein hochsicherer Fernzugriff auf die Engineering-Station ermöglicht. Im Anwendungsfall Fernzugriff meldet sich der Benutzer beim SINEMA RC Server an und baut eine sichere VPN-Verbindung zum Passieren der unsicheren Netzwerke wie dem Internet auf. Diese Verbindung kann dann dazu genutzt werden, eine RDP-Verbindung zur Jump Host-Station aufzubauen.

Darüber hinaus errichtet der Benutzer eine Verbindung von der Jump Host-Station durch die Back-Firewall zur Engineering-Station, die auf Schadprogramme und unbefugte Dateiübertragungen überwacht werden muss. Schließlich resultiert die Kombination von SINEMA RC in der Jump Host-Lösung mit der Back-Firewall in einer hohen Sicherheit und einer zeitgemäßen Fernzugriffslösung.

# 5.3. Reduzierung der Angriffsfläche

Die Angriffsfläche des Automatisierungs- und Leitsystems wird von seinen Schnittstellen gebildet.

## 5.3.1. Minimierung des Funktionsumfangs

Da die Angriffsfläche eines Systems von seinen Schnittstellen gebildet wird, tragen zwei wichtige Sicherheitsmaßnahmen zur Reduzierung der Angriffsfläche („Härtung“) bei:

- Deaktivierung aller unnötigen Schnittstellen.
- Schutz dieser Schnittstellen, die entweder notwendig sind oder nicht deaktiviert werden können, durch sichere Projektierung.

Typische Maßnahmen zum Schutz solcher Schnittstellen, die auch im Musterkonzept umgesetzt werden, sind gerichtet auf:

- Physische Kommunikationsschnittstellen (USB-Anschlüsse, Ethernet-Anschlüsse, Diagnoseschnittstellen, Drahtloskommunikation)
- Funktionalität auf Systemebene insbesondere bei Schnittstellen zu externen Komponenten (unnötige Funktionen, Softwareanwendungen, Ports, Protokolle und/oder Dienste)

Alle oben aufgeführten Elemente werden auf unterschiedlichen Ebenen angewendet:

- Anwendungen
- Betriebssystem (OS)
- Schnittstellen auf unteren Ebenen im BIOS

Empfohlene Härtungsmaßnahmen für das Musterkonzept, mit dem Ziel, die Angriffsfläche der oben beschriebenen Bereiche zu reduzieren, sind in Kapitel 6.6 aufgeführt.

Das schließt auch physische Schutzmaßnahmen wie Schlösser oder zutrittsbeschränkte Räume ein, diese werden als Teil der vorgesehenen Betriebsumgebung der Zonen in Kapitel 0 beschrieben.

Außerdem muss die Entfernung aller vorübergehend aktivierten Funktionen nach der Inbetriebnahme sichergestellt sein, z.B. für Fehlerbehebungs- und Testschnittstellen, einschließlich der Konten, die lediglich bei der Inbetriebnahme benötigt werden, um die Angriffsfläche während des Anlagenbetriebs zu minimieren.

Weitere Informationen zur Minimierung des Funktionsumfangs für das System WinCC OA sind zu finden in:

- \25\ – WinCC OA Security Guideline (Chapter 6.2: Hardening)

# 5.4. Sichere Kanäle und Verschlüsselung

## 5.4.1. Sichere Kanäle

Verschlüsselte Kanäle sind eine Kernmaßnahme zum Schutz von Daten während der Übertragung durch nicht vertrauenswürdige Zonen. Für Verkehr in eine vertrauenswürdigen wird die Notwendigkeit der Nutzung sicherer Kanäle individuell analysiert, wobei Bedrohungen und Kosten gegeneinander abgewogen werden.

Es dürfen nur bewährte und nicht abstreitbare Verschlüsselungs- und Hashing-Algorithmen verwendet werden. Richtlinien und Verfahren für die Schlüsselverwaltung müssen regelmäßige Schlüsseländerungen, die Vernichtung von Schlüsseln, die Verteilung von Schlüsseln und die Sicherung von Verschlüsselungsschlüsseln unter Einhaltung festgelegter Standards vorsehen.

## 5.4.2. Sensible Daten

Die als sensibel einzustufenden Daten werden anhand der Schutzziele in Abschnitt 4 identifiziert. Für solche Daten werden die Zugangsbeschränkungen sowie die verschlüsselte Speicherung in den jeweiligen Produkt- oder Komponentenhandbüchern beschrieben.

Als Ergebnis werden im Kontext des Musterkonzepts die folgenden Standardsicherheitsmaßnahmen empfohlen:

- Sichere Kommunikation für sämtlichen Verkehr zu und von der Anlage, d.h. zwischen den Servergeräten in der DMZ und externen Kommunikationsendpunkten. Eigene, durch IPsec-VPN geschützte Kanäle zwischen Hauptanlage und allen fernen Stationen, um Unabhängigkeit von den Sicherheitsfähigkeiten der eingesetzten Kommunikationsinfrastruktur zu erreichen (z.B. WWAN oder WLAN-Funk).
- Verschlüsselung der vertraulichen Daten der SPS (z.B. private Schlüssel) durch Passwortschutz.

- Sichere Kommunikation innerhalb von vertrauenswürdigen Zonen für die Übertragung sensibler Daten (z.B. OPC UA, HTTPS, Secure OUC etc.). Die Anforderungen an die Echtzeitkommunikation müssen berücksichtigt werden.

## 5.5. Schutz der Systemintegrität

Die Integrität des Systems muss gegen unbefugte Änderungen an Software und Daten geschützt werden, und solche Änderungen müssen erkannt, aufgezeichnet und gemeldet werden.

Das schließt insbesondere den Schutz gegen Schadprogramme ein, mit Fokus auf den verschiedenen Schnittstellen, über die – fahrlässig oder vorsätzlich – Schadprogramme auf USB-Sticks oder anderen mobilen Geräten eingeschleust werden könnten, oder durch Benutzer, die infizierte Websites besuchen oder infizierte E-Mail-Anhänge öffnen.

Je nach Schadprogrammen sind zahlreiche Auswirkungen möglich, wie Verbrauch von Rechenressourcen oder Blockierung von Komponenten bis hin zur Übernahme der Kontrolle über einen Client oder Server durch einen Angreifer. Ein gezielter Einsatz von Schadprogrammen kann auch das Systemverhalten manipulieren.

Die für das Musterkonzept empfohlenen Schutzmaßnahmen gegen Schadprogramme werden in Abschnitt 8 beschrieben.

### 5.5.1. Software- und Informationsintegrität

Neben technischem Support zur Absicherung von Arbeitsabläufen für die Aktualisierung von Software und Projektierung und zusätzlichen Maßnahmen wie digital signierten Softwareaktualisierungen lässt sich der Schutz des Systems gegen Schadprogramme implementieren durch den Einsatz von:

- Virenscannersoftware:
- Virenscannersoftware erkennt, blockiert und entfernt Schadprogramme (wenn notwendig und projektiert).
- Für die eigentliche Betriebsumgebung des Musterkonzepts auf Basis von WinCC OA gelten spezifische Projektierungsempfehlungen, siehe Abschnitt 8. Diese sind wichtig, um sicherzustellen, dass der Einsatz von Virenscannersoftware auf den Rechnern einer Automatisierungssystems nicht den Prozessmodus einer Anlage stört. Beispiele:

  - Die Projektierung wird an Verfügbarkeitsanforderungen ausgerichtet und generiert Alarme, deaktiviert aber nicht proaktiv Teile der Systemfunktionalität, was möglicherweise zum Verlust der Kontrolle über das Produktionssystem führt (z.B. bei einem OS-Server).
  - Die Projektierung wird angepasst, um potentielle Auswirkungen auf das Betriebsverhalten kritischer Softwareanwendungen während der Laufzeit zu minimieren.

- Whitelisting-Technologien:
- Whitelisting und Application Control sind Techniken, die nur die Ausführung vertrauenswürdiger Anwendungen zulassen oder Dateioperationen auf bestimmte Anwendungen beschränken. Whitelisting dient entweder als Ergänzung oder als Alternative zu Virenscanner-Lösungen.

  - Whitelisting, listenbasiert: Softwareprozesse und Dienste, die Teil einer verwalteten Whitelist sind und als vertrauenswürdig eingestuft sind, dürfen gestartet werden und in Betrieb sein. Alle anderen Elemente (wie eingeschleuste Schadprogramme, nicht freigegebene Tools) werden blockiert.
  - Whitelisting, regelbasiert (Application Control): Es werden Regeln definiert, um zu entscheiden, ob eine Anwendung gestartet werden kann, oder um die zulässigen Dateioperationen einzuschränken.

Die Stationen und Server für das Musterkonzept sind mit Virenscannersoftware ausgestattet. Diese hat die Fähigkeit, die Virenerkennungsmuster in der DMZ auf dem neuesten Stand zu halten. Diese Aufgabe übernimmt ein Infrastrukturserver für den Austausch von Virenmusterdateien. Die Stationen und Server für das Musterkonzept arbeiten mit Whitelisting. Abschnitt 8 beschreibt diese Schutzmaßnahmen im Detail. Es ist wichtig, darauf hinzuweisen, das typische Schadprogramme die Schwachstellen installierter Softwarekomponenten und Dienste ausnutzen, und sowohl Virenscanner als Whitelisting-Lösungen müssen durch Aufspielen aktueller Sicherheitspatches ergänzt werden. Die Patchmanagementverfahren für das Musterkonzept werden in Abschnitt 9 beschrieben.

- \25\ - WinCC OA Security Guideline (Chapter 6.6: Virus Scanner)

### 5.5.2. Nachweis der Sicherheitsfunktionalität

Dieser ist wichtig, um die korrekte Funktionsweise der implementierten Sicherheitsmaßnahmen sicherzustellen. Der Nachweis der vorgesehenen Funktion von Sicherheitsmaßnahmen wird beim Fabrikabnahmetest (FAT) oder Standortabnahmetest (SAT) durch entsprechende Sicherheitstests erbracht und sollte danach auf regelmäßiger Grundlage wiederholt werden (z.B. im Rahmen der planmäßigen Wartung).

- \25\ - WinCC OA Security Guideline (Chapter 6.8: Security Tests)

### 5.5.3. Eingangs- und Ausgangsvalidierung und Fehlerbereinigung

WinCC OA gewährleistet die Berücksichtigung von Aspekten wie Eingangsvalidierung und Ausgangsüberwachung in einem durchgängig sicheren Entwicklungsprozess. Der sichere Entwicklungsprozess ist nach dem Rahmenwerk der Norm IEC 62443 für Sicherheit in industriellen Leitsystemen zertifiziert (Teil 4-1, sichere Entwicklung).

### 5.5.4. Support für die Sicherung und Wiederherstellung von Leitsystemen

Das Ziel der Sicherung und Wiederherstellung besteht darin, dass der Bediener oder Asseteigner einen bekannten Zustand wiederherstellen kann, nachdem es zu einer Störung oder einem Ausfall gekommen ist. Weitere Einzelheiten sind in Abschnitt 10 zu finden.

### 5.5.5. Zeitverteilung und Synchronisation

Im Musterkonzept ist die Anlagenzentraluhr mit dem Leitsystemnetzwerk und mit dem Prozessregelungsnetzwerk verbunden. Der Domain Controller des Leitsystemnetzwerks verwendet das Zeittelegramm von der Anlagenzentraluhr und übermittelt die Zeit an alle Domainmitglieder (z.B. OS-Clients und Server, MES-Systeme, OPC-Server). Die mit dem Prozessregelungsnetzwerk verbundenen Controller S7-1500 erhalten das Zeitsignal direkt von der Anlagenzentraluhr.

Empfohlene Maßnahmen und weitere Einzelheiten über Zeitverteilung und Synchronisation sind in Abschnitt 6.8 zu finden.

# 5.6. Sicherheitsprotokollierung und Überwachung

| | |
|---|---|
| **IEC 62443-3-3** | **Gemäß SR 1.13 – Zugriff über nicht vertrauenswürdige Netzwerke**<br>**SR 1.13 RE1 Genehmigung ausdrücklicher Zugriffsanfragen** |

Die in den vorstehenden Abschnitten beschriebenen Sicherheitsmerkmale und Fähigkeiten werden ergänzt durch die Sicherheitsprotokollierung und Überwachung sicherheitsbezogener Aktionen und Ereignisse über alle erforderlichen Systemkomponenten hinweg. Zusätzlich zu der auf den geregelten Prozess fokussierten Protokollierung und Überwachung, die von den Fähigkeiten des regulären Automatisierungs- und Leitsystems vollständig abgedeckt wird, sind Informationen aus Sicherheitsprotokollen und zu überwachten Ereignissen wichtig, um eine IT-Forensik im Fall von Cybersicherheitsvorfällen durchzuführen.

Neben der Sicherheitsprotokollierung und Überwachung können weitere Fähigkeiten zur Erkennung industrieller Anomalien implementiert werden. Siehe Abschnitt 0.

## 5.6.1. Überwachung des Zugriffs aus nicht vertrauenswürdigen Zonen

Wie in Abschnitt 5.1 beschrieben, wird das Musterkonzept der Abwasserbehandlungsanlage durch eine DMZ geschützt, was die vollständige Kontrolle sämtlicher Netzwerkkommunikation und Fernzugriffe aus externen, möglicherweise nicht vertrauenswürdigen Netzwerken erlaubt. Die Sicherheitsprotokollierung und Überwachung erstrecken sich auf beide Firewalls der DMZ sowie auf die PC-basierten Systeme innerhalb der DMZ. Damit werden alle Zugriffe auf Benutzer- oder Systemebene und alle Kommunikationssitzungen auf Netzwerkebene (TCP/IP) abgedeckt.

Das Musterkonzept umfasst verschiedene ferne Stationen wie Brunnen, Behälter oder externe Pumpen und Zählerstationen. Kommunikationsleitungen zwischen zentraler Anlage und fernen Stationen werden mit SCALANCE-Netzwerkgeräten für die sicheren Verbindungen überwacht.

- \25\ – WinCC OA Security Guideline (Chapter 6.1.8.4: Protected Service Access)

## 5.6.2. Protokollierung sicherheitsbezogener Ereignisse

Für die geschützten Zonen des Musterkonzepts einer Wasserbehandlungslage, einschließlich Gebäude und zentrale Anlagenzonen, wird eine Sicherheitsprotokollierung durchgeführt. Dabei werden sowohl PC-basierte WinCC OA-Systeme als auch SCALANCE-Netzwerkgeräte und SIMATIC-SPSen abgedeckt. Die PC-basierten Systeme führen Sicherheitsprotokolle für Ereignisse sowohl auf Anwendungsebene als auch auf Betriebssystemebene. Sicherheitsprotokolle können über standardisierte Kommunikationsprotokolle (Syslog, SNMP) zu zentralen Servern exportiert werden. Diese Server erfassen zentral die Sicherheitsprotokollinformationen von den Systemkomponenten und bieten Schnittstellen, die in übergeordnete SIEM-Lösungen (Security Information Event Management) des Asseteigners integriert werden können. Weitere Informationen über optionale SIEM-Funktionalitäten sind in Abschnitt 0 zu finden.

Für die Überwachung der Palo Alto Firewalls (Frontend und Backend) wird Panorama Management Software eingesetzt. Generell wird der gesamte Zugriff auf Sicherheitsprotokolle geschützt und auf autorisierte Benutzer der Automatisierungslösung beschränkt, hierzu dienen die in Abschnitt 5.2 beschriebenen Systemfähigkeiten. Damit wird der gesamte Zugriff auf Sicherheitsprotokolldaten ebenfalls von den Fähigkeiten zur Sicherheitsüberwachung und Protokollierung abgedeckt.

Auf den Automatisierungsgeräten werden Syslog-Clients konfiguriert, um eine bessere Verfolgung und Überwachung kritischer SPS-Änderungen und -Vorgänge zu ermöglichen. Bei sicherheitsrelevanten Ereignissen, wie z.B. Benutzeranmeldungen, Konfigurationsänderungen oder Betriebszustandsänderungen, werden Meldungen in einem separaten Meldungsspeicher der SPS generiert. Die konfigurierbare Weiterleitung an externe Syslog-Server / SIEM-Systeme ermöglicht die Integration in bestehende Sicherheitsüberwachungssysteme.

- \25\ – WinCC OA Security Guideline (Chapter 6.7: Logging, audit, maintenance and asset management)
- \51\ – Sicherheitsvorfälle in WinCC OA

### 5.6.3. Audit Trail

Um die Anforderungen im Hinblick auf das Änderungsmanagement zu erfüllen, werden alle Änderungen entweder über das WinCC OA oder TIA ES (betrifft Automatisierungsausrüstung) oder über SINEC NMS (betrifft Netzwerkkomponenten) zentral durchgeführt. Auf diese Weise können jederzeit Auditberichte generiert werden, um nachzuweisen, welcher menschliche Benutzer welche Änderungen vorgenommen hat.

SINEC INS kann als Syslog-Server verwendet werden, um Änderungen und Sicherheitsvorfälle von Automatisierungs- und Netzwerkkomponenten zu überwachen. Direkter Zugriff auf SPSen oder SCALANCE-Geräte sollte nur bei der erstmaligen Inbetriebnahme genutzt werden, nicht später während der Betriebs- und Instandhaltungsphase.

- \25\ – WinCC OA Security Guideline (Chapter 6.7: Logging, audit, maintenance and asset management)
- \49\ - SIMATIC NET: Netzwerkmanagement SINEC INS

# 6. Härtung und Projektierung der Systemkomponenten

Für die im Musterkonzept der Abwasserbehandlungsanlage verwendeten Komponenten sind verschiedene Härtungsmaßnahmen in Betracht zu ziehen, je nach Ergebnis der Bedrohungs- und Risikoanalyse und den definierten Schutzzielen, siehe Abschnitt 4.

Die empfohlenen Härtungsmaßnahmen und Projektierungen, die in den folgenden Abschnitten beschrieben werden, sind nur für das Musterkonzept einer Abwasserbehandlungsanlage gültig.

Bei jeder Abweichung vom Musterkonzept muss eine Bedrohungs- und Risikoanalyse durchgeführt werden, und die Härtungsmaßnahmen und Projektierungen müssen entsprechend angepasst werden.

## 6.1. Annahmen

| | |
|---|---|
| **IEC 62443-3-3** | **SR 1.7 Stärke der Authentifizierung durch Passwörter**<br>**SR 1.7 RE1 Erzeugung und Lebensdauerbeschränkungen von Passwörtern für menschliche Benutzer**<br>**SR 1.7 RE2 Lebensdauerbeschränkungen von Passwörtern für alle Benutzer** |

Neben den Härtungsmaßnahmen für das Automatisierungs- und Leitsystem empfiehlt das Konzept „Defense-in-Depth“ physische und organisatorische Sicherheitsmaßnahmen, die in der Verantwortung des Anlagenbetreiber liegen.

In einer Bewertung der möglichen Sicherheitsrisiken für das Musterkonzept einer Abwasserbehandlungsanlage werden die folgenden physischen Sicherheitsmaßnahmen angenommen:

- Unbefugter Zugang zu zentraler Anlage und Gebäuden wird durch physische Maßnahmen verhindert. Nur autorisiertes Personal hat Zugang.
- Unbefugter Zugang zu den fernen Stationen wird durch physische Maßnahmen verhindert. Der Zugang zu den fernen Stationen wird überwacht, z.B. mit Hilfe von Türschaltern. Nur autorisiertes Personal hat Zugang.
- Alle Schränke haben eine Schließanlage mit Halbzylindern.
- Alle Schränke, sowohl im Hauptteil der Abwasserbehandlungsanlage als auch in den fernen Stationen, sind in abschließbaren Schalt- oder Serverräumen installiert. Der Zugang zu Schalt- und Serverräumen ist auf autorisiertes Personal (Instandhaltung) beschränkt.
- Das Leitsystemnetzwerk ist in einem Gebäude mit hochgradigem physischen Schutz installiert, wie in Bild 3-3 dargestellt.
- Das Prozessregelungsnetzwerk läuft im zentralen Teil der Abwasserbehandlungsanlage mit physischer Zugriffssteuerung, wie in Bild 3-3 „Allgemeine Härtungsmaßnahmen“ dargestellt.

Für alle im Musterkonzept der Abwasserbehandlungsanlage verwendeten Komponenten sind die folgenden allgemeinen Härtungsmaßnahmen in Betracht zu ziehen, um eine sichere Projektierung während des Anlagenbetriebs zu gewährleisten.

- Es sind die neuesten freigegebenen Firmwareversionen zu installieren. Firmwareversionen für alle Siemens-Komponenten sind über den Siemens Industry Online Support verfügbar \4\.
- Für alle Komponenten sind die neuesten freigegebenen Patches zu installieren. Die Patches für Siemens-Komponenten sind über den Siemens Industry Online Support verfügbar \4\. Weitere Informationen zum Patchmanagement sind in Abschnitt 9 zu finden.
- Für die Virenscanner der Workstations und Server sind immer die neuesten Virenerkennungsmuster zu installieren. Weitere Informationen sind zu finden in:
- \25\ WinCC OA Security Guideline – WinCC OA Security Guideline (Chapter 6.6: Virus Scanner)
- Standardbenutzer und Passwort müssen vor der Erstinstallation an allen Geräten geändert werden. Für verschiedene Benutzer und Systeme darf nicht das gleiche Passwort verwendet werden. Der Zugriff muss geschützt und für unbefugte Personen unmöglich sein.
- Weitere Informationen sind in Abschnitt 7 zu finden.

- Für SCALANCE-Komponenten sind die Härtungsmaßnahmen in \5\ beschrieben – eine Checkliste für die Einrichtung von SCALANCE-Geräten ist in Betracht zu ziehen und zentral von SINEC NMS abzuarbeiten.

## 6.2. Firewalls für sichere Kommunikation zwischen den Zonen

Die Kommunikation zwischen den Sicherheitszonen muss überwacht und gesteuert werden, wie in Abschnitt 5.1.2 beschrieben.

Die Grenze des Anlagennetzwerks wird durch eine Front-Firewall und eine Back-Firewall geschützt. Diese Firewalls bilden die demilitarisierte Zone (DMZ) für das Musterkonzept. Härtungsmaßnahmen und Projektierung der Firewalls werden in Abschnitt 6.2.1 beschrieben. Weitere Informationen siehe:

- \25\ WinCC OA Security Guideline (Chapter 6.1: Security Cells and Network Architecture)

Die Kommunikation zwischen den Sicherheitszonen innerhalb des Automatisierungs- und Leitsystems wird durch SCALANCE-Netzwerksicherheitsgeräte geschützt. Härtungsmaßnahmen und Projektierung dieser Geräte werden in Abschnitt 6.2.2 beschrieben.

### 6.2.1. Palo Alto 440 NGFW

Front-Firewall:

- Schützt sowohl das DMZ-Netzwerk als auch die internen Netzwerke vor nicht vertrauenswürdigen Netzwerken (Schnittstelle zur Unternehmens-Firewall oder Schnittstelle zum Internet).
- Server in der DMZ können geschützt mit öffentlichen Servergeräten kommunizieren. Sowohl ausgehende als auch eingehende Daten werden mittels DPI durchsucht.

Back-Firewall:

- Daten, die zum und vom Prozessregelungsnetzwerk übertragen werden müssen, werden anhand eines Mehrfaktorverfahrens durchsucht und kontrolliert. Dadurch wird der Verkehr bis Schicht 7 auf diejenigen Anwendungen und Dienste beschränkt, die für den Betrieb erforderlich sind.

Die empfohlenen Härtungsmaßnahmen und Projektierungen für Front-Firewall und Back-Firewall sind in Tabelle 6-2 aufgeführt.

Bild 6-1 – DMZ mit Front- und Back-Firewall

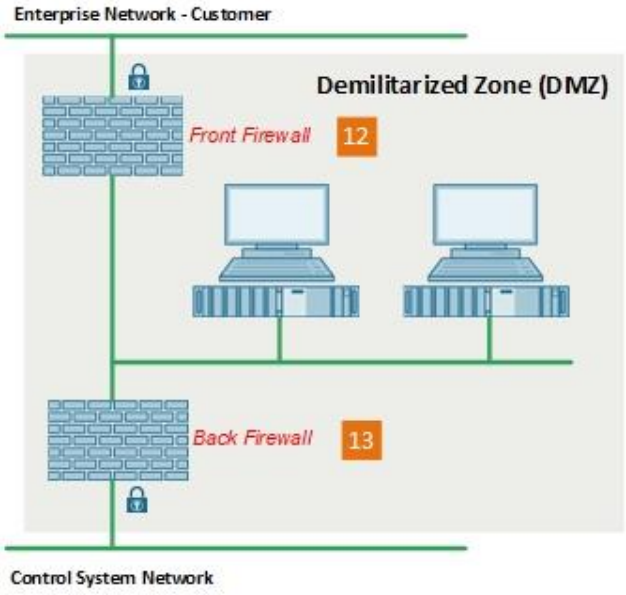



Tabelle 6-1 – Front- und Back-Firewall

| Funktion | SCI | Lieferant | Typ | MLFB |
|---|---|---|---|---|
| Front-Firewall | 12 | Palo Alto | 440 NGFW | 9LA1110-6SY12-1AB1 |
| Back-Firewall | 13 | Palo Alto | 440 NGFW | 9LA1110-6SY12-1AB2 |

Für die nachstehend aufgeführten Firewalls sind mindestens die folgenden allgemeinen Härtungsmaßnahmen in Betracht zu ziehen:

Tabelle 6-2 – Härtungsmaßnahmen für die Firewalls

| Nr. | Sicherheitsthema | Härtungsmaßnahme | Dokumente |
|---|---|---|---|
| 1 | Beschränkung von IP-Adressen | Beschränkung des Zugriffs auf diejenigen IP-Adressen, die notwendig sind | \39\ |
| 2 | Beschränkung von Diensten | Kein Zugriff über das unsichere Protokoll HTTP oder Telnet, erforderlich ist SSH und/oder HTTPS | \39\ |
| | | Einstellung der Verschlüsselung auf mindestens Version TLSv1.2 | \39\ |
| 3 | Änderung von Admin-Berechtigungen / Benutzerverwaltung | Änderung des Standardbenutzernamens | \39\ |
| | | Änderung des Standardpassworts | \39\ |
| | | Projektierung eines Kontos für jede Person, die Zugriff benötigt, und nur Erteilung derjenigen Rechte, die benötigt werden | \39\ |
| | | Einsatz von Mehrfaktorauthentifizierung (RADIUS oder SAML) | \39\ |
| | | Projektierung strenger Passwortregeln | \39\ |
| 4 | Dedizierte Managementschnittstelle | Einsatz der dedizierten Managementschnittstelle in einem separaten Management-LAN oder Management-VLAN | \39\ |
| 5 | Sicherheitsrichtlinie mit Regeln und Profilen | Durchsuchung des gesamten Verkehrs zur Managementschnittstelle auf Bedrohungen | \39\ |
| | | Erstellung eines Sicherheitsprofils, Aktivierung einer erweiterten Paketerfassung | \39\ |
| | | Inbound Inspection und SSL Forward Proxy projektieren | \39\ |
| 6 | Protokollierung | Einrichtung einer Protokollierung für Projektierungsänderungen | \39\ |
| | | Einrichtung einer Protokollierung für unbefugte Anmeldeversuche | \39\ |
| 7 | SNMP | Einsatz von SNMP v3 | \39\ |
| | | Einen nicht leicht zu erratenden SNMP-String einrichten | \39\ |
| | | SNMP nur an internen Schnittstellen aktivieren | \39\ |
| 8 | Zertifikate | Das Standardzertifikat durch ein vom Enterprise-CA der Organisation signiertes Zertifikat ersetzen | \39\ |
| 9 | Aktualisierungen | PAN-OS und alle Softwarepakete auf dem neuesten Stand halten | \39\ |

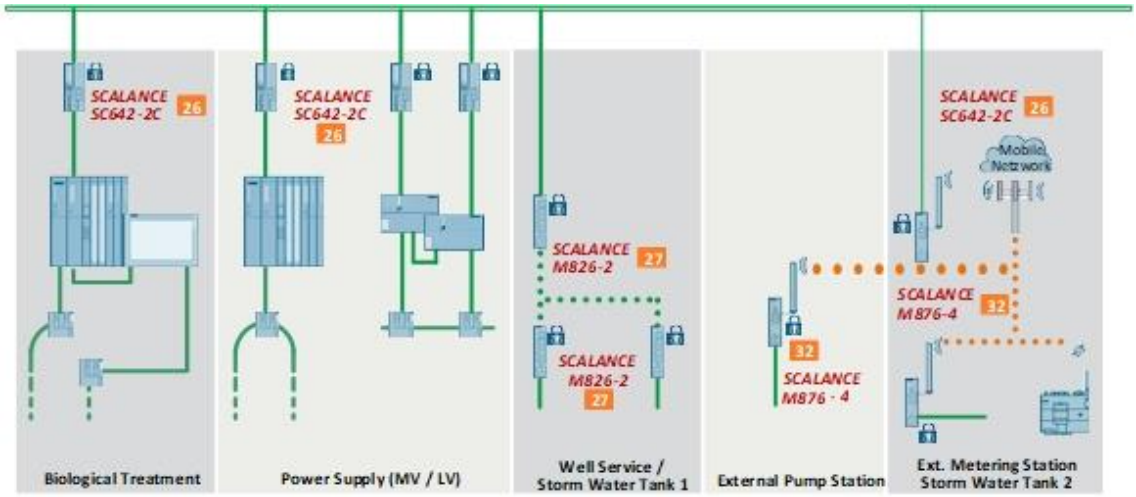
Weitere Informationen über die Projektierung der Palo Alto Next Generation Firewall sind zu finden in:

- \6\ – PAN-OS Administrator's Guide
- \7\ – Palo Alto Website zu PAN-OS
- \39\ – Palo Alto – Best Practices for Securing Administrative Access

### 6.2.2. SCALANCE-Netzwerksicherheitsgeräte

Im Musterkonzept wird die sichere Kommunikation im Prozessregelungsnetzwerk und zu den fernen Stationen durch den Einsatz von SCALANCE-Netzwerksicherheitsgeräten implementiert, wie in Bild 6-2 dargestellt. Die folgende Tabelle enthält verschiedene Beispiele für die Verschaltung.

Bild 6-2 – SCALANCE-Netzwerksicherheitsgeräte



Im Musterkonzept werden die folgenden SCALANCE-Netzwerksicherheitsgeräte eingesetzt:

Tabelle 6-3 – SCALANCE-Netzwerksicherheitsgeräte

| Funktion | SCI | Lieferant | Typ | MLFB |
|---|---|---|---|---|
| Sichere Kommunikation zwischen Prozessregelungsnetzwerk und<br>• S7-1500-Controller<br>• Station Gateway | 26 | Siemens | SCALANCE SC642-2C | 6GK5642-2GS00-2AC2 |
| Sichere Kommunikation zwischen Prozessregelungsnetzwerk und<br>• Ferne Station *„Brunnenwasser/Betriebswasser“*<br>• Ferne Station *„Regenwasserbecken 1“* | 27 | Siemens | SCALANCE M826-2 | 6GK5826-2AB00-2AB2 |
| Sichere Kommunikation zwischen Prozessregelungsnetzwerk und ferner Station *„Externe Pumpstation, klein“* | 32 | Siemens | SCALANCE M876-4 | 6GK5876-4AA10-2BA2 |
| Sichere Kommunikation zwischen Prozessregelungsnetzwerk und fernen Stationen *„Externe Zählerstation“* und *„Regenwasserbecken 2“* | 32 | Siemens | SCALANCE M876-4 | 6GK5876-4AA10-2BA2 |
| Sichere Kommunikation zwischen Prozessregelungsnetzwerk und<br>S7-1500 an Fremd-SPS in der mechanischen Behandlung<br>S7-1500 an internen MRP-Ring | 25 | Siemens | SIMATIC Net CP 1543-1 | 6GK7543-1AX00-0XE0 |

Für die in Tabelle 6-2 aufgeführten SCALANCE-Geräte sind mindestens die folgenden allgemeinen Härtungsmaßnahmen in Betracht zu ziehen:

Tabelle 6-4 – Härtungsmaßnahmen für SCALANCE-Netzwerksicherheitsgeräte

| Nr. | Sicherheitsthema | Härtungsmaßnahme | Dokumente |
|---|---|---|---|
| 1 | Sicheres Netzwerk | Priorität für Quality of Service (QOS) ist auf „DSCP“ eingestellt | \5\ – Abschnitt 3.10 |
| | | Spanning Tree deaktivieren, wenn nicht erforderlich | \5\ – Abschnitt 3.11.2 |
| | | Passives Mithören deaktivieren | \5\ – Abschnitt 3.11.3 |
| 2 | Identitäts- und Zugriffsmanagement | Zentrale Authentifizierung über RADIUS/UMC/AD verwenden.<br>Passwortregeln (Komplexität und Änderungshäufigkeit) festlegen und Änderungen zentral und regelmäßig über SINEC NMS verbreiten. | \5\ – Abschnitt 3.4<br>\43\ – Abschnitt 7 |
| 3 | Reduzierung der Angriffsfläche | Deaktivierung unverschlüsselter und nicht erforderlicher Protokolle.<br>Details zeigt Tabelle 6-3 | \5\ – Abschnitt 3.3 |
| | | Vollständige Deaktivierung der PROFINET-Schnittstelle | \5\ – Abschnitt 3.7 |
| | | Beschränkung des DCP-Zugriffs auf „Nur lesen“ | \5\ – Abschnitt 3.9.1 |
| | | Deaktivierung ungenutzter Ports | \2\ – Abschnitt 5.71<br>\5\ – Abschnitt 3.14.1 |
| | | Deaktivierung aller nicht erforderlichen Dienste wie DHCP oder DNS | |
| 4 | Sichere Kanäle und Verschlüsselung | Keine Maßnahmen erforderlich (siehe Tabelle 6-6 | |
| 5 | Systemintegrität | Einsatz von NTP zur Uhrzeitsynchronisation<br>Falls verfügbar, ist die sichere NTP-Variante zu verwenden | \5\ – Abschnitt 3.2 |
| 6 | Protokollierung und Überwachung | Syslog-Client aktivieren. Siehe Abschnitt 0. | |

Die folgende Tabelle zeigt die Einstellungen für die Protokolle:

Tabelle 6-5 – Protokolle

| Nr. | Protokoll | Einstellungen |
|---|---|---|
| 1 | Telnet-Server | Deaktiviert |
| 2 | SSH-Server | Deaktivieren und SINEC NMS zur Projektierung aller Netzwerkgeräte verwenden |
| 3 | HTTP-Dienste | Nur HTTPS |
| 4 | DCP-Server | Nur Lesezugriff |
| 5 | SNMP<br>• SNMP v1/v2, nur Lesezugriff<br>• SNMP v1 Traps<br>• SINEMA-Konfigurationsschnittstelle | Einsatz von SNMP v3<br>• Deaktiviert<br>• Deaktiviert<br>• Deaktiviert |

Die sichere Kommunikation zwischen den Zonen wird durch IPsec-VPN und die interne Firewall gewährleistet. Tabelle 6-6 und Tabelle 6-7 zeigen daher die Einstellungen.

Tabelle 6-6 – IPsec-VPN-Konfiguration

| Nr. | Thema | Einstellungen |
|---|---|---|
| 1 | Ferne Gegenstelle | Remote-Modus: Standard<br>Remote-Typ: Manuell |
| 2 | Verbindung | KEYing-Protokoll: IKEv2 |
| 3 | Authentifizierung | Einsatz von CA-Zertifikaten<br>Nicht PSK verwenden |
| 4 | Phase 1 | Voreingestellte Ciphers verwenden<br>Mindestens zu verwenden<br>• Verschlüsselung: AES128 GCM 16<br>• Authentifizierung: SHA256<br>• Schlüsselableitung: DH-Gruppe 14<br>Aggressive Mode nicht verwenden |
| 5 | Phase 2 | Voreingestellte Ciphers und automatische Firewallregeln verwenden<br>Mindestens zu verwenden<br>• Verschlüsselung: AES128 GCM 16<br>• Authentifizierung: SHA256<br>• Schlüsselableitung: DH-Gruppe 14 |

Tabelle 6-7 – Firewall-Einstellungen

| Nr. | Thema | Einstellungen |
|---|---|---|
| 1 | IPv4 vordefiniert | Alle nicht erforderlichen Dienste für gesamtes VLAN deaktivieren |

Die folgende Tabelle enthält zusätzliche Einstellungen für die verwendeten Typen der SCALANCE-Netzwerksicherheitsgeräte.

Tabelle 6-8 – Zusätzliche Einstellungen

| Nr. | Typ | Einstellungen |
|---|---|---|
| 1 | SCALANCE SC642-2C | MRP deaktivieren |
| 2 | SCALANCE M826-2 | Eigenes VLAN für SHDSL und Transfer-Subnetz errichten.<br>Die Firewall muss aktiviert sein, um den Zugriff zu beschränken |
| | | IPsec-Kommunikation zwischen zwei M826-2 nutzen, um die Subnetze über SHDSL-Verbindung (Transfer-Subnetz) zu verbinden |
| 3 | SCALANCE M876-4 | Mobile Drahtloskonfiguration<br>• Authentifizierungsmethode: Auto |

| Nr. | Typ | Einstellungen |
|---|---|---|
| | | • Daten-Roaming: Deaktivieren |
| | | SMS: SMS-Dienste deaktivieren, wenn nicht benötigt |
| | | Kein Dienst darf über usb0 (mobile Drahtlosschnittstelle) zugänglich sein. Siehe Firewall-Konfiguration in Tabelle 6-7. |

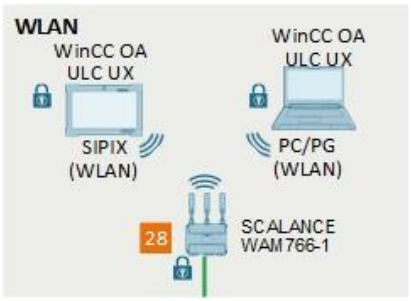
Weitere Informationen zur Projektierung der SCALANCE-Netzwerksicherheitsgeräte sind zu finden in:

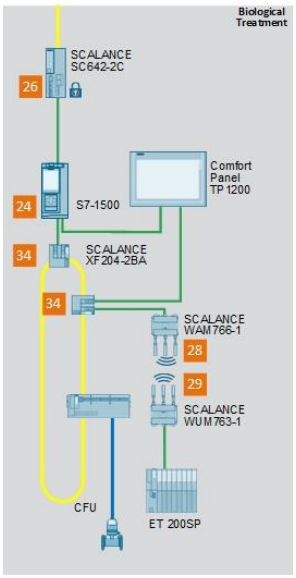
- \5\ – Checkliste für die Einrichtung von SCALANCE-Geräten
- \8\ – SCALANCE SC-600 – Web Based Management (WBM)
- \9\ – SCALANCE SC-600 – Betriebsanleitung
- \10\ – SCALANCE M800 – Web Based Management (WBM)
- \11\ – SCALANCE M874, M876 – Betriebsanleitung
- \12\ – SCALANCE M826 – Betriebsanleitung
- \13\ – SCALANCE M874, M876 – Betriebsanleitung
- \43\ – Benutzerverwaltung für SCALANCE-Geräte mit RADIUS-Protokoll

# 6.3. Netzwerkkomponenten für die Drahtloskommunikation

Drahtloskommunikation mittels IWLAN wird im Musterkonzept eingesetzt, um Feldperipheriegeräte wie die Compact Field Unit (CFU) über PROFINET mit dem Automation Controller S7-1500 zu verbinden. Außerdem werden Tablets für die mobile Projektierung und Bedienung über IWLAN mit dem Automatisierungs- und Leitsystem verbunden, siehe Bild 6-3.

Bild 6-3 – Drahtloskommunikation




Im Musterkonzept werden die folgenden SCALANCE-Drahtlosgeräte eingesetzt:

Tabelle 6-9 – SCALANCE-Drahtlosgeräte

| Funktion | SCI | Lieferant | Typ | MLFB |
|---|---|---|---|---|
| IWLAN-Zugangspunkt für die PROFINET-Drahtloskommunikation mit Feldperipheriegeräten. Wird auch für die Kommunikation mit mobilen Laptops und Tablets in der zentralen Anlage verwendet (auch CLP in Betracht ziehen und nationale Zulassungen beachten). | 28 | Siemens | SCALANCE WAM766-1 | 6GK5766-1GE00-7DA0 |
| IWLAN-Client für die PROFINET-Drahtloskommunikation mit Feldperipheriegeräten (auch CLP in Betracht ziehen und nationale Zulassungen beachten). | 29 | Siemens | SCALANCE WUM763-1 | 6GK5763-1AL00-3DA0 |

Die Härtungsmaßnahmen für die SCALANCE-Drahtlosgeräte sind aufgeführt in

- Tabelle 6-4 – Härtungsmaßnahmen für SCALANCE-Netzwerksicherheitsgeräte.
- Tabelle 6-5 – Protokolle.

Neben diesen allgemeinen Härtungsmaßnahmen und der Projektierung sind die folgenden Härtungsmaßnahmen in Betracht zu ziehen:

Tabelle 6-10 – Zusätzliche Härtungsmaßnahmen SCALANCE W

| Nr. | Sicherheitsthema | Härtungsmaßnahme | Dokumente |
|---|---|---|---|
| 1 | WLAN-Verschlüsselung | Aktivieren der AES-Verschlüsselung für iPCF | \5\ – Abschnitt 3.12.1 |
| 2 | Tunnel WLAN Schicht 2 | Mac-Modus auf 'Layer-2-Tunnel' einstellen. Nur möglich, wenn ausschließlich SCALANCE-Geräte verwendet werden. | \5\ – Abschnitt 3.12.2 |
| 3 | WLAN iPCF | iPCF verwenden, wenn zeitkritische Daten, z.B. PROFINET, auf der Funkverbindung übertragen werden. | \5\ – Abschnitt 3.12.3 |

Weitere Informationen zur Projektierung der SCALANCE-Drahtlosgeräte sind zu finden in

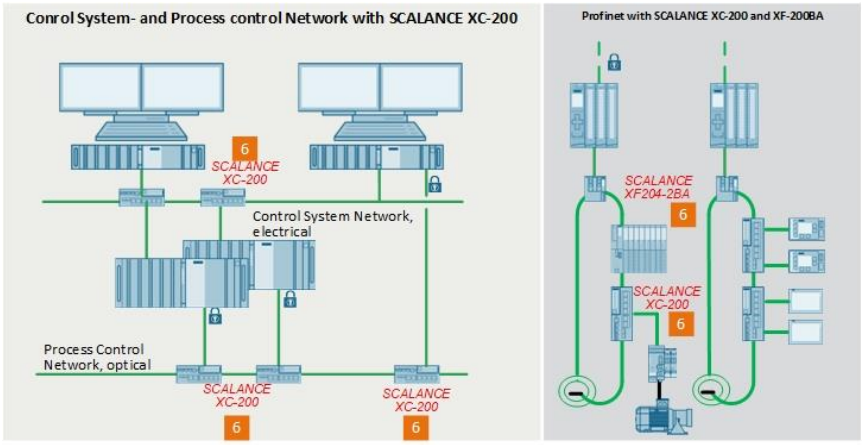
- \5\ – Checkliste für die Einrichtung von SCALANCE-Geräten
- \14\ – SCALANCE WAM766 – Betriebsanleitung
- \15\ – SCALANCE WUM763 – Betriebsanleitung

# 6.4. Netzwerkkomponenten SCALANCE XC und XF

Die Verbindung der Workstations und Server mit den jeweiligen Netzwerken (z.B. DMZ-Subnetz oder Leitsystemnetzwerk) und die Verbindung der PROFINET-Geräte mit PROFINET-Netzwerken wird im Musterkonzept unter Verwendung der folgenden SCALANCE-Geräte implementiert.

- SCALANCE XC-200.
- SCALANCE XF-200BA.

Bild 6-4 – SCALANCE XC-200 und XF-200BA




Die Härtungsmaßnahmen für die Geräte SCALANCE XC-200 und XF-200BA sind aufgeführt in

- Tabelle 6-4 – Härtungsmaßnahmen für SCALANCE-Netzwerksicherheitsgeräte.
- Tabelle 6-5 – Protokolle.

Neben diesen allgemeinen Härtungsmaßnahmen und der Projektierung sind die folgenden Härtungsmaßnahmen in Betracht zu ziehen:

Tabelle 6-11 – Zusätzliche Härtungsmaßnahmen SCALANCE XC-200 und XF-204 BA

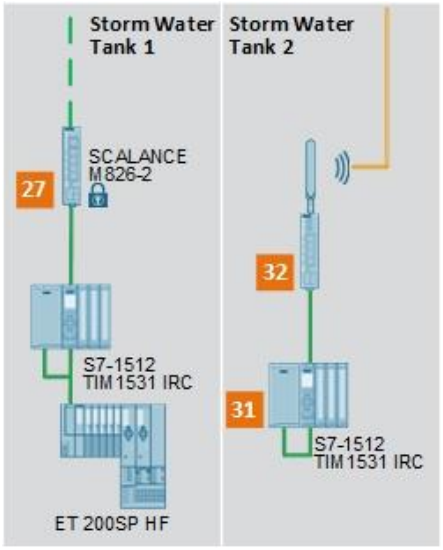
| Nr. | Sicherheitsthema | Härtungsmaßnahme | Dokumente |
|---|---|---|---|
| 1 | Ringredundanz | Ringredundanz deaktivieren, wenn das Gerät nicht in einem Ring betrieben wird | \5\ – Abschnitt 3.11.1 |
| 2 | PROFINET | Wenn das SCALANCE-Gerät in einem PROFINET-Netzwerk verwendet wird, muss die Schnittstellenfunktionalität für PROFINET aktiviert werden. | \5\ – Abschnitt 3.7 |

Weitere Informationen zur Projektierung der Geräte SCALANCE XC-200 und XF-204 sind zu finden in

- \5\ – Checkliste für die Einrichtung von SCALANCE-Geräten
- \16\ – SCALANCE XC-200 / XF-200BA – Web Based Management (WBM)
- \17\ – SCALANCE XC-200 – Betriebsanleitung
- \18\ – SCALANCE XF-200BA – Betriebsanleitung

## 6.5. TeleControl TIM 1531 IRC

Bild 6-5 - TeleControl TIM 1531 IRC




Die Kommunikationsbaugruppe TIM 1531 IRC dient zum Verbinden ferner Stationen mit dem TeleControl-Endpunkt (in den WinCC OA-Server integriert) über öffentliche oder private Infrastrukturen. Das Gerät umfasst einen Telegrammpuffer für die kontinuierliche Aufzeichnung von Daten einschließlich Zeitstempel, wenn der Kommunikationsweg gestört ist oder ein Kommunikationspartner ausfällt.

Die folgenden Härtungsmaßnahmen werden empfohlen:

Tabelle 6-12 – Härtungsmaßnahmen TIM 1531 IRC

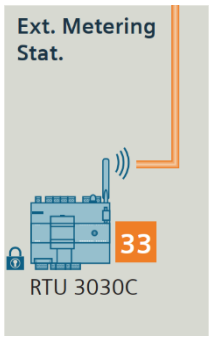
| Nr. | Sicherheitsthema | Härtungsmaßnahme | Dokumente |
|---|---|---|---|
| 1 | MSC-Protokoll | Einsatz von MSCsec | \19\ – Abschnitt 1.4 |
| 2 | Zeitsynchronisation | Einsatz von NTP. Falls verfügbar, ist die sichere NTP-Variante zu verwenden | \19\ – Abschnitt 1.4 |
| 3 | SNMP | Einsatz von SNMPv3 | \19\ – Abschnitt 1.4 |
| 4 | Web-Server-Zugang | Nur Einsatz von HTTPS | \19\ – Abschnitt 1.4 |

Weitere Informationen zur Konfiguration der Kommunikationsbaugruppe TIM 1531 IRC sind zu finden in:

- \19\ – TIM 1531 IRC – Handbuch

## 6.6. TeleControl RTU3051C

Bild 6-6 – TeleControl RTU3051C




Die kompakte Fernwirkeinheit SIMATIC RTU3051C dient zum Überwachen und Steuern von Außenstationen, die geographisch verteilt sind und keinen Anschluss an ein Spannungsversorgungsnetz besitzen. Die RTU kann Prozessdaten speichern und über mobiles WLAN an eine Masterstation übertragen.

Um eine sichere Kommunikation zwischen der RTU3051C in der fernen Station und dem TeleControl-Endpunkt zu gewährleisten, erfolgt eine verschlüsselte Kommunikation mit dem SINEMA RC Server.

Die folgenden Härtungsmaßnahmen werden empfohlen:

Tabelle 6-13 – Härtungsmaßnahmen RTU3051C

| Nr. | Sicherheitsthema | Härtungsmaßnahme | Dokumente |
|---|---|---|---|
| 1 | VPN | Einsatz von OpenVPN, RTU als OpenVPN Client projektieren | \20\ – Abschnitte 3.7 und 6.15.2 |
| 2 | HTTPS für WAN | HTTPS für WAN aktivieren, SMS-Eingang sperren | \20\ – Abschnitt 6.13 |
| 3 | Web-Server-Zugang | Nur Einsatz von HTTPS | \20\ – Abschnitt 6.15.3 |

Weitere Informationen zur Projektierung der Fernwirkeinheit RTU3051C sind zu finden in:

- \20\ – RTU3051C – Betriebsanleitung

## 6.7. Industrial Ethernet CP 1543-1

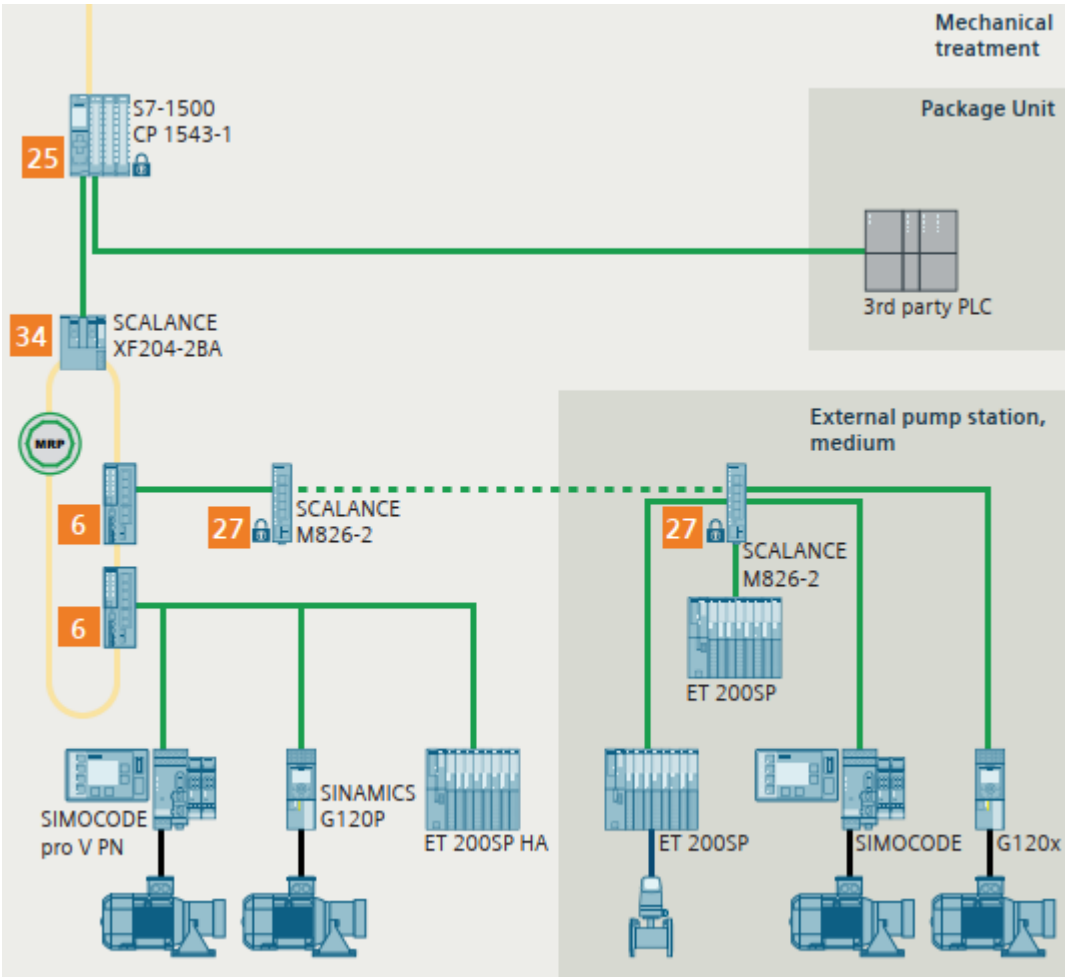
Bild 6-7 – Sichere Kommunikation über CP 1543-1


Die sichere Kommunikation innerhalb der Automatisierungsgeräte S7-1500 und der externen Systeme wie der Pumpstation wird im Musterkonzept über Industrial Ethernet CP 1543-1 abgewickelt.

Tabelle 6-14 – CP 1543-1

| Nr. | Gerät | MLFB |
|---|---|---|
| 1 | SIMATIC NET CP 1543-1 | 6GK7543-1AX00-0XE0 |

Bild 6-8 – Einsatz von CP 1543-1




Die Konfiguration der Firewall-Funktionalitäten und des VPN-Tunnels (via IPSec) zu externen Stationen erfolgt direkt im TIA Engineering Tool.

Industrial Ethernet CP 1543-1 bietet die folgenden Sicherheitsfunktionen:

Tabelle 6-15 – Sicherheitsfunktionen CP 1543-1

| **Nr.** | Schutzfunktion | Beschreibung |
|---|---|---|
| 1 | Firewall | • IP-Firewall mit Stateful Packet Inspection (Schichten 3 und 4) – Zustandsorientierte Paketüberprüfung<br>• Firewall auch für Ethernet Non-IP Frames nach IEEE 802.3 (Schicht 2)<br>• Bandbreitenbegrenzung<br>• Globale Firewall-Regeln |
| 2 | Durch IPsec-Tunnel geschützte Kommunikation | Der CP 1543-1 kann bei der Projektierung mit anderen Sicherheitsmodulen kombiniert werden. Zwischen allen Sicherheitsmodulen einer VPN-Gruppe werden IPsec-Tunnel eingerichtet. Alle internen Knoten dieser Sicherheitsmodule können durch diese Tunnel sicher miteinander kommunizieren. |
| 3 | Protokollierung | Um eine Überwachung zu ermöglichen, können Ereignisse in Protokolldaten gespeichert werden. Diese Dateien können mit dem Projektierungswerkzeug ausgelesen oder automatisch an einen Syslog-Server gesendet werden. |
| 4 | HTTPS | Zur verschlüsselten Übertragung von Webseiten, zum Beispiel in der Prozessregelung |
| 5 | FTPS | Zur verschlüsselten Übertragung von Dateien |
| 6 | NTP (geschützt) | Zur sicheren Synchronisation und Übertragung der Uhrzeit |
| 7 | SNMPv3 | Zur sicheren Übertragung von Netzwerkanalyseinformationen mit Abhörschutz |

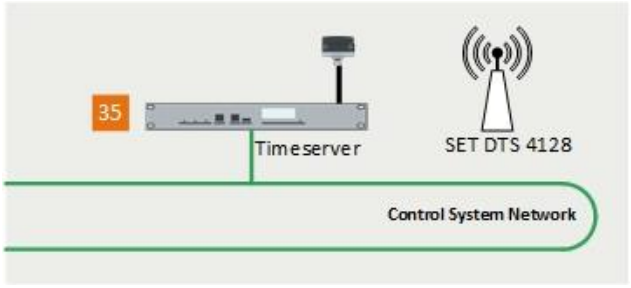
| Nr. | Schutzfunktion | Beschreibung |
|---|---|---|
| 8 | Schutz für Geräte und Netzwerksegmente | Firewall und VPN-Schutzfunktion können auf den Betrieb einzelner Geräte, mehrerer Geräte oder ganzer Netzwerksegmente angewendet werden |

Ausführliche Beschreibungen der Verwendung und Projektierung des CP 1543-1 sind zu finden in:

- \22\ – Industrial Ethernet CP 1543-1 Advanced – Handbuch
- Einsatz von CP 1543-1
- \21\ – Industrial Ethernet Security, Grundlagen und Anwendung, Abschnitt 1.8
- Projektierung der Firewall im Standardmodus
- \21\ – Industrial Ethernet Security, Grundlagen und Anwendung, Abschnitt 4.1.1
- Projektierung der Firewall im erweiterten Modus
- \21\ – Industrial Ethernet Security, Grundlagen und Anwendung, Abschnitt 4.3
- \23\ – Kommunikation mit SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro

## 6.8. Anlagenzentraluhr

Bild 6-9 – Zeitsynchronisation via Zeitserver




Die Anlagenzentraluhr verwaltet an zentraler Stelle die Zeit für die gesamte Anlage und synchronisiert alle anderen Anlagenkomponenten über deren Schnittstellen. Die Anlagenzentraluhr ist mit dem Leitsystemnetzwerk verbunden.

Der Domain Controller empfängt das Zeitsignal von der Anlagenzentraluhr und überträgt die Zeit an den Server, der an das Leitsystemnetzwerk und DMZ-Subnetz angeschlossen ist. Der OS-Server überträgt das Zeitsignal an die angeschlossenen OS-Clients.

Die Automatisierungsgeräte S7-1500 empfangen das Zeitsignal direkt von der Anlagenzentraluhr.

Die empfohlenen Schutzmaßnahmen sind

- Einsatz von NTP (Secure).
- Einsatz von SNMPv3.

Weitere Informationen zur Projektierung der Uhrzeitsynchronisation für das System WinCC OA sind zu finden in:

- \25\ WinCC OA Security Guideline (Chapter 6.1.2: Highly Secure Large System)

## 6.9. Workstations und Server

Im Musterkonzept einer Abwasserbehandlungsanlage werden für alle Workstations und Server die Siemens Industrial Workstations (IPC) für WinCC OA verwendet. Auf diesen IPCs laufen das notwendige Betriebssystem und die SIMATIC WinCC OA Software.

Die in den folgenden Abschnitten beschriebenen Härtungsmaßnahmen beziehen sich auf Siemens Industrial Workstations (IPC) für WinCC OA.

- \41\ – Empfohlene Sicherheitseinstellungen für IPCs in der Industrieumgebung
- \25\ – WinCC OA Security Guideline (Chapter 6.2.2: Hardening WinCC OA)

### 6.9.1. Allgemeine Härtungsmaßnahmen für Workstations und Server

Für die Workstations und Server sind die folgenden Härtungsmaßnahmen in Betracht zu ziehen:

Tabelle 6-16 – Allgemeine Härtungsmaßnahmen für Workstations und Server

| Nr. | Sicherheitsthema | Härtungsmaßnahme | Dokumente |
|---|---|---|---|
| 1 | Sicheres Netzwerk | Einsatz der Firewall | \25\ – Abschnitt 6.2.2.5 |
| 2 | Identitäts- und Zugriffsmanagement | BIOS-Einstellungen | \25\ – Abschnitt 6.2.1.3 |
| | | Benutzerverwaltung mit Active Directory und SIMATIC Logon | Ausführliche Beschreibung siehe Abschnitt 7 |
| 3 | Reduzierung der Angriffsfläche | Unnötige Windows-Komponenten entfernen | \25\ – Abschnitt 6.2.1.1 |
| | | Windows-Dienste deaktivieren | \25\ – Abschnitt 6.2.1 |
| | | Serverfunktionalität Automation License Manager (ALM) deaktivieren, wenn die Anlage in Betrieb ist | \25\ – Abschnitt 6.2.1.1 |
| | | SMB-Signierung aktivieren | \25\ – Abschnitt 6.2.1.9 |
| | | Blockierung von USB-Speichermedien<br>• Sperren oder mit anderen mechanischen Mitteln deaktivieren<br>• Beschränkung des Zugriffs mit Windows-Gruppenrichtlinie | \25\ – Abschnitt 6.2.1.5 |
| 4 | Sichere Kanäle und Verschlüsselung | Verschlüsselte Kommunikation aktivieren | \25\ – Abschnitt 5.6 |
| 5 | Systemintegrität | Einsatz von Whitelisting | Ausführliche Beschreibung siehe Abschnitt 8<br>\25\ – Abschnitt 6.2.1.11 |
| | | Installation von Virenscannersoftware | Ausführliche Beschreibung siehe Abschnitt 8<br>\25\ – Abschnitt 6.6 |
| | | Digitale Signaturen für Anwendung | \25\ – Abschnitt 6.2.2.18 |
| | | Patching des Betriebssystems | Ausführliche Beschreibung siehe Abschnitt 9<br>\25\ – Abschnitt 6.5.2.1.2 |
| | | Sicherung von Engineering-Daten und Systemdaten | Ausführliche Beschreibung siehe Abschnitt 10<br>\25\ – Abschnitt 6.9 |
| 6 | Protokollierung und Überwachung | Einsatz von Benutzerverwaltung | \25\ – Abschnitt 6.4.3 |

Einige der oben aufgeführten Härtungsmaßnahmen können in den Gruppenrichtlinienobjekten (GPOs) von Windows eingestellt werden. Im Musterkonzept werden die GPOs zentral am Domain Controller eingestellt, siehe Abschnitt 7.

### 6.9.2. Zusätzliche Härtungsmaßnahmen

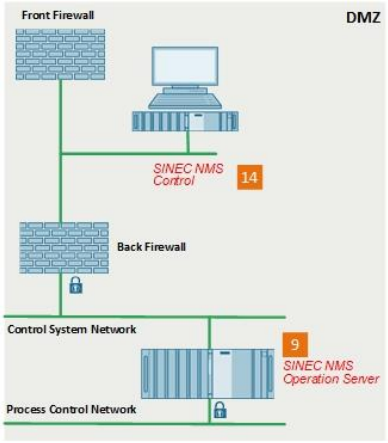
Für einige der WinCC OA Workstations und Server werden zusätzliche Härtungsmaßnahmen empfohlen.

- \25\ – WinCC OA Security Guideline Hardening (Chapter 6.2.2: Hardening WinCC OA)
- \25\ – WinCC OA Security Guideline Hardening (Chapter 6.3: Administration and Configuration of OS)

### 6.9.3. Härtungsmaßnahmen für SINEC NMS

SINEC NMS ist eine Software für die Überwachung und Administration von Netzwerken und deren Geräten und besteht aus der Komponente „Control" und mindestens einer Komponente „Operation". Im Musterkonzept sind die Komponenten von SINEC NMS wie im folgenden Bild projektiert:

Bild 6-10 – Übersicht über SINEC NMS




- Die Komponente „Control" dient zur Überwachung und Administration des gesamten Netzwerks
- Die Komponente „Operation" dient zum Anzeigen ausführlicher Informationen über die überwachten Geräte und stellt die Geräte in Netzwerktopologien dar.

Die Benutzerverwaltung von SINEC NMS wird mit User Management Component (UMC) implementiert. Für WinCC OA ist der UMC-Server von SINEC NMS zu installieren. Der lokale Benutzer kann auf dem Domain Controller in Active Directory integriert werden.

Neben den in Abschnitt 6.9.1 erwähnten Härtungsmaßnahmen empfiehlt es sich, die zusammen mit SINEC NMS gelieferte Protokollkomponente SNMPv3 zu installieren.

Whitelisting wird nicht empfohlen, weil dadurch die Funktionalität von SINEC NMS beeinflusst werden kann.

Weitere Informationen über SINEC NMS sind zu finden in

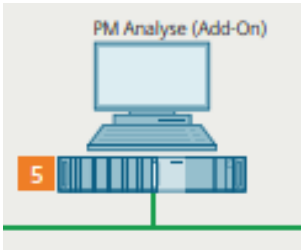
- \28\ – Netzwerkmanagement SINEC NMS

### 6.9.4. Härtungsmaßnahmen für PM ANALYZE

PM ANALYZE wird im Musterkonzept eingesetzt, um spezielle Berichte gemäß ATV-Vorschriften zu erstellen, und besteht aus den folgenden Modulen:

- PM Server: Installiert auf dem PM ANALYZE Server.
- PM Agent: Auf dem OS-Server installierter HTTPS-Server.
- PM ANALYZE Client.

Bild 6-11 – Übersicht über PM Analyze




Neben den in Tabelle 6-14 aufgeführten Härtungsmaßnahmen ist die folgende Maßnahme in Betracht zu ziehen:

- Whitelisting des OS-Servers.
- Der Einsatz von Whitelisting auf dem PM ANALYZE Server wird nicht empfohlen.

\29\ – Übersicht über die Premium Add-ons für SIMATIC WinCC

### 6.9.5. Härtungsmaßnahmen für SIMATIC Energy Manager Pro

SIMATIC Energy Manager ist das Energiemanagementsystem für die Industrie und nach ISO 50001 zertifiziert.
Mit SIMATIC Energy Manager werden Energieströme und Verbrauchswerte in Prozessen detailgenau visualisiert. Die Werte werden den relevanten Verbrauchern oder Kostenstellen zugeordnet und es wird ermittelt, weshalb es zu Änderungen gekommen ist. Das System hilft, die Energieeffizienz zu steigern und somit die Energiekosten zu senken.

Die Erfassungskomponente von Energy Manager Pro kommuniziert über OPU UA (HA) mit der WinCC OA Web Server-Station in der DMZ.

Neben den in Tabelle 6-14 aufgeführten Härtungsmaßnahmen ist die folgende Maßnahme in Betracht zu ziehen:

- SIMATIC Energy Manager Pro nutzt den Microsoft Information Service (IIS). Empfohlene Einstellung:
- \33\ – SIMATIC Energy Manager PRO V7.5 - Installation, Kapitel 3.1

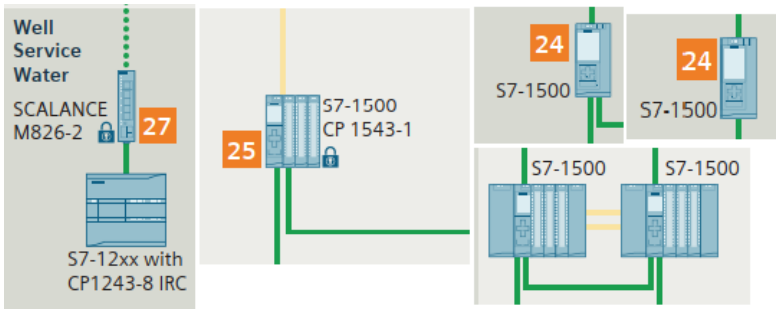
Weitere Informationen über SIMATIC Energy Manager Pro sind zu finden in:

- \31\ SIMATIC Energy Manager PRO V7.5 – Operation
- \32\ SIMATIC Energy Manager PRO V7.5 – Acquisition
- \33\ SIMATIC Energy Manager V7.5 – Installation
- \34\ SIMATIC Energy Manager PRO V7.2 – Systemhandbuch

## 6.10. Automatisierungsgeräte SIMATIC S7-1500 / S7-1200

Im Musterkonzept werden die Automatisierungsgeräte SIMATIC S7-1500 und S7-1200 für die Steuerung des Hauptteils der Abwasserbehandlungsanlage eingesetzt.

Bild 6-12 – S7-1500 / S7-1200




Im Musterkonzept kommen die folgenden Projektierungen der Automatisierungsgeräte S7-1500 and S7-1200 zum Einsatz:

Tabelle 6-17 – Übersicht über S7-1500 und S7-1200

| SCI | Funktion | Lieferant | Typ | MLFB |
|---|---|---|---|---|
| 24 | S7-1500 (H), Option Redundanz | Siemens | SPS mit 3 integrierten Schnittstellen für die Kommunikation via PROFINET und/oder Prozessregelungsnetzwerk. Optional hohe Verfügbarkeit. | 6ES7515-2AM01-0AB0<br>6GK7543-1AX00-0XE0 |
| 25 | Automatisierungsgerät | Siemens | SPS mit 3 integrierten Schnittstellen für die Kommunikation via PROFINET und/oder Prozessregelungsnetzwerk. CP1543-1 für zusätzliche Sicherheit bei der Kommunikation. | 6ES7515-2AM01-0AB0<br>6GK7543-1AX00-0XE0 |

| SCI | Funktion | Lieferant | Typ | MLFB |
|---|---|---|---|---|
| 27 | Automatisierungsgerät | Siemens | SPS mit zusätzlichem CP1243-8 IRC für Fernwirken und sichere Kommunikation. | 6ES7215-1AF40-0XB0 |

Eine sichere Kommunikation zwischen Automatisierungsgeräten und Prozessregelungsnetzwerk wird auf zwei verschiedene Weisen implementiert:

- CP 1543-1:
- Härtungsmaßnahmen und Projektierung siehe Tabelle 6-6.
- SCALANCE SC 624-2C:
- Härtungsmaßnahmen und Projektierung siehe Abschnitt 6.2.2.

**Härten von SIMATIC-SPSen**

**Siemens-SPSen verfügen über die folgenden Sicherheitsmerkmale, die zu ihrem Schutz angewendet werden können:**

- Zugriffskontrolle:
- Die Controller S7-1500 und S7-1200 verfügen über einen Zugriffskontrollmechanismus, um den Benutzerzugriff auf bestimmte SPS-Funktionalitäten einzuschränken.

Tabelle 6-18 – Zugriffsrechte

| Zugriffsrecht | Berechtigungen |
|---|---|
| HMI-Zugriff | Nur HMI-Zugriffe und der Zugriff auf Diagnosedaten sind möglich. |
| | Tags können über ein HMI-Gerät gelesen und geschrieben werden. |
| Lesezugriff | Ein Lesezugriff auf die Hardwarekonfiguration und die Bausteine ist ohne Eingabe eines Passworts möglich. |
| | Hardwarekonfigurationen und Bausteine können auf das Programmiergerät hochgeladen werden. |
| | HMI-Zugriff und Zugriff auf Diagnosedaten sind möglich. |
| | Der Betriebszustand (RUN/STOP) kann geändert und die Uhrzeit eingestellt werden. |
| Vollzugriff | Die Hardwarekonfiguration und die Bausteine können von allen Benutzern gelesen und geändert werden. |
| | Voller Zugriff auf alle Funktionen, wie das Herunterladen von Bausteinen und Hardwarekonfigurationen in die SPS, das Ausführen von Testfunktionen, des Ändern des Betriebszustands (RUN/STOP) und die Durchführung von Firmware-Updates. |

- Sichere PG/PC- und HMI-Kommunikation:
- Das Transport Layer Security-Protokoll (TLS) wird für die sichere PG/PC- und HMI-Kommunikation mit standardisierten Sicherheitsmechanismen verwendet.
- Schutz der vertraulichen Konfigurationsdaten der SPS:
- Passwortbasierter Schutz zur Verschlüsselung vertraulicher Projektierungsdaten des Controllers (z.B. private Schlüssel zum Signieren und Entschlüsseln von Nachrichten).

**Security-by-Default**

Um Sicherheitsrisiken und potenzielle Cyberangriffe zu minimieren, sind alle Sicherheitseinstellungen standardmäßig aktiviert. Dies gewährleistet den Schutz gegen unbefugten Zugriff und garantiert die Integrität und Vertraulichkeit der Kommunikationsdaten, wodurch ein Abfangen oder eine Manipulation verhindert wird.

\23\ Kommunikation mit SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro
https://support.industry.siemens.com/cs/ww/en/view/59192925

- \23\ – Kommunikation mit SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro
    - \24\ – S7-1500 Handbuchsammlung
    - \26\ – Sicherheit mit SIMATIC-S7-Controllern
    - \27\ – SIMATIC STEP 7 Basic/Professional V16 und SIMATIC WinCC V16
    - \45\ – Konfiguration der Sicherheitsfunktionen in TIA Portal V17
    - \46\ – Benutzerverwaltung & Zugriffssteuerung mit TIA Portal V19
    - \47\ – Zertifikate mit TIA Portal verwenden

# 7. Benutzerverwaltung

Die Benutzerverwaltung im Musterkonzept der Abwasserbehandlungsanlage wird zentral abgewickelt. Hierzu ist auf dem Domain Controller der Active Directory Domain Service installiert. Wegen der zentralisierten Benutzerverwaltung muss das Prinzip AGLP (Account, Global, Domain local, Permission) beachtet werden. Nach diesem Prinzip werden die Domainbenutzerkonten zunächst den domainglobalen Gruppen in Active Directory zugewiesen. Anschließend werden diese Gruppen lokalen Rechnergruppen zugewiesen, die wiederum die Berechtigungen für die Objekte erhalten. Dies schließt Mechanismen für Wiederstellung und Rücksetzung von Passwörtern ein.

Die Logon-Benutzerauthentifizierung für WinCC OA basiert auf Windows-Domaingruppen.

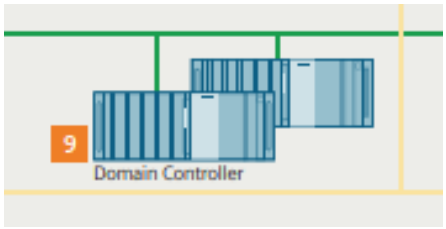
## 7.1. Domain Controller

Der Domain Controller im Musterkonzept ist redundant ausgelegt und in Zone 1, d.h. im Gebäude, installiert, siehe Bild 3-3. Der Domain Controller kann auch in der demilitarisierten Zone (DMZ) installiert werden. Damit kann die Administration des Active Directory Domain Service von einer zentralen IT-Abteilung durchgeführt werden.

Wenn der Domain Controller in der DMZ installiert wird, ist es empfehlenswert, mindestens einen Domain Controller in der Sicherheitszone zu installieren, um den Betrieb des Automatisierungs- und Leitsystems auch bei einem Ausfall der Verbindung zur DMZ sicherzustellen.

Wenn mehrere Subnetze/Sicherheitszonen vorhanden sind, ist abhängig von den Anforderungen in jeder Sicherheitszone mindestens ein Domain Controller vorzusehen. Siehe Bild 7-1.

Bild 7-1 – Domain Controller im Automatisierungssystem




- \25\ – WinCC OA Security Guideline (Chapter 6.4.3.2.1: Usage of Operating system (Windows or Linux) based user management)

## 7.2. User Management Component

Mit der User Management Component (UMC) lässt sich ein zentrales System zur Verwaltung von Benutzern und Benutzergruppen über verschiedene Siemens-Software und -Geräte hinweg einrichten. Benutzer und Benutzergruppen können aus dem Microsoft Active Directory übernommen werden.

### 7.2.1. UMC-Ring-Server

Der UMC-Ring-Server stellt die zentrale Konfigurationsplattform für die Benutzerverwaltung dar. In diesem Server sind Benutzer mit den entsprechenden Gruppenzuweisungen für die UMC-Domain definiert. Um Benutzer und Gruppen aus dem Active Directory zu übertragen, muss der UMC-Ring-Server-PC zur AD-Domain hinzugefügt werden.

Der UMC-Ring-Server kann in einer redundanten Konfiguration realisiert werden, um die Verfügbarkeit zu erhöhen.

- \48\ – Zentrale Benutzerverwaltung mit der User Management Component (UMC)

## 7.3. Authentifizierung und Autorisierung der Benutzer für WinCC OA

Die Benutzerauthentifizierung und -autorisierung werden im Musterkonzept durch Windows-Domaingruppen übernommen, die mit Active Directory verwaltet werden. Alle persönlichen Benutzerkonten an Komponenten werden Domaingruppen zugewiesen.

Für den Betriebssystemzugriff werden personalisierte Windows-Konten und Gruppen genutzt. Diese werden vom Domain Controller zentral verwaltet, wobei alle PC-basierten Rechner im Leitsystemnetzwerk, Anwendungsbus und in DMZ-

Netzwerken abgedeckt werden. Da persönliche Benutzerkonten von der Domain verwaltet werden, entsprechen alle Benutzerpasswörter den Komplexitätsanforderungen.
WinCC OA ermöglicht die Benutzerverwaltung über Windows-Domaingruppen, die mit dem Active Directory verwaltet werden. Das bedeutet, dass die Benutzergruppen für einen Benutzer aus der Windows-Verwaltung übernommen werden.

Die Gruppenrechte für die übernommenen Gruppen müssen in WinCC OA definiert werden. Die Benutzerverwaltung kann wie die WinCC OA-Administration verwendet werden, mit der Ausnahme, dass keine Benutzer oder Gruppen hinzugefügt oder gelöscht werden können.

Wenn sich ein Benutzer anmeldet, prüft das System, ob der Benutzer im System bekannt ist.

Weitere Informationen über die Authentifizierung und Autorisierung der Benutzer sind zu finden in:

- \25\ – WinCC OA Security Guideline (Chapter 6.4.3.2: Usage of WinCC OA external authentication method)

### 7.3.1. Vorteile der Verwendung von Active Directory für die Benutzerauthentifizierung

Ein Active Directory-System ermöglicht die Verwendung von obligatorischen Anforderungen an die Passwortstärke, die über den Gruppenrichtlinien-Editor konfiguriert werden können. Mit forcierten Einstellungen lässt sich ein gutes und sicheres Passwort für Benutzer gewährleisten und das Projekt so vor schwachen Passwörtern schützen.

Neben einem starken Passwort ermöglicht ein Active Directory-basierter Mechanismus zur Benutzerauthentifizierung die Synchronisierung von Benutzern und Gruppen innerhalb einer Domain. Dies vereinfacht das Initiieren von Anmeldungen bei einem WinCC OA-Client, der in der gleichen Domain gehostet wird.

# 8. Schutz gegen Schadprogramme und Application Control

Die Integrität des Systems muss gegen unbefugte Änderungen von Software und Daten geschützt werden, und unbefugte Änderungen müssen erkannt, aufgezeichnet und gemeldet werden.

Im Musterkonzept wird der Schutz gegen Schadprogramme und unbefugte Änderungen implementiert durch den Einsatz von

- Antivirensoftware:
- Die Workstations und Server des Musterkonzepts arbeiten mit der neuesten Version der Antivirensoftware McAfee Endpoint Security. McAfee Endpoint Security (EPS) aktiviert zusätzliche Funktionen, die über den herkömmlichen Virenscanner hinausgehen.
- Um sicherzustellen, dass die Virensignaturdateien aller Workstations und Server auf dem neuesten Stand sind, ist auf dem Infrastruktur-PC in der DMZ ein Virenscannerserver installiert. Dieser Server empfängt seine Virensignaturen vom Aktualisierungsserver des jeweiligen Virenscannerherstellers im Internet oder von einem vorgeschalteten Virenscannerserver und verwaltete seine Virenscannerclients.
- Whitelisting-Techniken:
- Die Workstations und Server des Musterkonzepts arbeiten mit der neuesten Version von Trellix Application and Change Control.
- McAfee Application Control kann dafür genutzt werden, den Start unzulässiger oder unbekannter Anwendungen auf Workstations und Servergeräten zu blockieren. Nach der Installation und Aktivierung von McAfee Application Control sind alle ausführbaren Anwendungen und Dateien gegen Modifikation geschützt.

McAfee Endpoint Security und McAfee Application Control sind nicht auf allen Workstations und Servergeräten im Musterkonzept installiert.

Sowohl Trellix Endpoint Security als auch Trellix Application and Change Control können mit dem Trellix Policy Orchestrator (ePO) zentral projektiert und verwaltet werden. Diese Software wird auf dem Infrastruktur-PC in der DMZ installiert.

Weitere Informationen zu Einsatz und Projektierung von Antivirensoftware und Whitelisting sind zu finden in

- \25\ – WinCC OA Security Guideline (Chapter 6.2.1.11: Whitelisting/Application Control)
- \30\ – Kompatibilität mit Trellix Application Control
- \38\ – Einsatz von Whitelisting mit Trellix Application Control für PCS 7 und WinCC

# 9. Patchmanagement

## 9.1. Patchmanagement für WinCC OA-Komponenten

IEC 62443 empfiehlt zum Schutz gegen Cyberattacken das Konzept „Defense-in-Depth“. Ein wichtiger Baustein des Konzepts „Defense-in-Depth“ ist der Schutz der Systemintegrität, siehe Abschnitt 5.5.

Eine Maßnahme zum Schutz der Systemintegrität ist das Patchmanagement als Teil des umfassenden Sicherheitskonzepts.

Patchmanagement ist die systematische Vorgehensweise zur Installation von Patches auf dem Automatisierungs- und Leitsystem. Patches werden unterschieden in

- Patches für das Betriebssystem Microsoft Windows.
- Dabei handelt es sich um Aktualisierungen, Servicepacks, Featurepacks und ähnliche Installationen aller Art, unabhängig davon, ob diese mit Sicherheit zu tun haben oder nicht.
- Sicherheitsaktualisierungen für das Betriebssystem Microsoft Windows
- Patches für Firmware und Software zur Beseitigung von Schwachstellen, vorgesehen für Software und Produkte von Siemens und Fremdkomponenten.

Bei Software und Produkten von Siemens werden Sicherheitsschwachstellen von der verantwortlichen Siemens-Produkteinheit bearbeitet. Das gilt auch für Schwachstellen von Fremdkomponenten in Siemens-Produkten, auch hier wird die jeweilige Siemens-Produkteinheit tätig.

Bei Sicherheitsschwachstellen von Fremdkomponenten, die sich nicht im Eigentum von Siemens befinden, trägt der Anlagenbetreiber die Verantwortung dafür, dass diese Komponenten während des Betriebs stets auf dem neuesten Stand sind, was Patches anbelangt.

Der auf dem Infrastruktur-PC installierte Windows Server Update Service (WSUS) des Musterkonzepts verwaltet die Windows-Patches für das Automatisierungs- und Leitsystem. Der WSUS kann die Windows-Patches entweder vom Microsoft Update-Server oder vom Server im Unternehmensnetzwerk des Kunden erhalten. Der WSUS verteilt die Patches an alle windowsbasierten PCs des Automatisierungs- und Leitsystems.

Microsoft hat jedoch angekündigt, WSUS im Jahr 2025 einzustellen. Wenn ein Produkt eingestellt wird, bedeutet dies, dass es nicht mehr aktiv weiterentwickelt wird und in zukünftigen Updates entfernt werden könnte. Derzeit plant Microsoft nicht, WSUS aus den Windows Server-Versionen, einschließlich Windows Server 2025, zu entfernen. Das Tool wird weiterhin gewartet, aber es werden keine neuen Funktionen hinzugefügt.

Für alle Produkte von Siemens, Fremdkomponenten eingeschlossen, veröffentlicht Siemens monatlich Ratschläge. Die Ratschläge werden hier veröffentlicht:

- https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications

Weitere Informationen über Patchmanagement und WSUS sind zu finden in

- \25\ – WinCC OA Security Guideline (Chapter 6.5: Patch management and security updates)

## 9.2. Patchmanagement für Automatisierungs- und Netzwerkkomponenten

Neue Firmware von Automatisierungsgeräten wird über den Infrastruktur-PC verwaltet. Im Fall von SCALANCE-Netzwerkkomponenten werden Firmwareaktualisierungen zentral über SINEC NMS verbreitet.

# 10. Sicherung und Wiederherstellung

Die Wiederherstellung und Zurückversetzung eines Automatisierungs- und Leitsystems in einen bekannten Zustand nach einer Störung oder einem Ausfall ist ein wichtiges Thema im Konzept „Defense-in-Depth“ und wird in der Norm IEC 62443 empfohlen.

In einer Strategie zur Sicherung und Wiederherstellung werden alle für die Wiederherstellung notwendigen Daten und ihr Speicherort im System identifiziert. Die Häufigkeit der Speicherung von Sicherheitskopien, die Art der Sicherung (komplett, differentiell oder inkremental) und der Speicherort der Sicherungskopien werden in dieser Strategie beschrieben.

Bei der Datensicherung werden die folgenden Kategorien unterschieden:

- Systemsicherung:
- Eine Systemsicherung stellt ein vollständiges Abbild des Systems dar, z.B. eine Momentaufnahme oder einen „Schnappschuss“ des aktuellen Systems. Dabei werden die folgenden Daten einbezogen:
  - Hardwarespezifische Dateien (Treiber).
  - Dateien und Einstellungen des Windows-Betriebssystems.
  - Installierte Programme und deren Konfiguration
  - Hostgeräte (hardwarespezifische Dateien (Treiber), Dateien und Einstellungen des Betriebssystems Windows, installierte Programme und deren Konfiguration).
  - Für Systemsicherungen wird Symantec System Recovery empfohlen.
- Projektsicherung:
- Eine Projektsicherung erstreckt sich hauptsächlich auf die Sicherung des WinCC OA-Projekts.
- Komponentenspezifische Daten:
- Komponentenspezifische Daten wie Datenbanken oder die individuelle Projektierung eingebetteter Geräte oder Netzwerkgeräte müssen gesichert werden. Für die Sicherung komponentenspezifischer Daten wird SINEC NMS verwendet.

Eine Wiederherstellung von Systemen ist kritischer als die Anfertigung von Sicherheitskopien. Dieser Prozess muss getestet und reproduziert werden, um im Notfall eine schnelle Verfügbarkeit der Anlagensysteme zu gewährleisten und Stillstandszeiten zu minimieren.

Weitere Informationen über Sicherung und Wiederherstellung sind zu finden in

- \25\ – WinCC OA Security Guideline (Chapter 6.9: Implement Backup and Restore concept)

# 11. Optionale Sicherheitsmaßnahmen

Die in Abschnitt 6 beschriebene Projektierung und Härtung gewährleistet zusammen mit den in Abschnitt 5 beschriebenen Sicherheitsmaßnahmen eine hochgradige Sicherheit und umfassenden Schutz auf Basis des Konzepts „Defense-in-Depth“.

Durch Umsetzung weiterer Sicherheitsmaßnahmen lässt sich das Security Level für ein Automatisierungs- und Leitsystem nochmals erhöhen. Die folgenden Abschnitte beschreiben einige dieser Maßnahmen, die Siemens anbietet.

Weitere Informationen über die optionalen Sicherheitsmaßnahmen bietet

- \40\ – Siemens Industrial Security Service

## 11.1. Threat Prevention Subscription für Front-Firewall und Back-Firewall

Die in Abschnitt 6.2.1 beschriebenen Palo Alto Next Generation Firewalls können um die Option Threat Prevention Subscription (TPS) erweitert werden. Wir empfehlen den Einsatz der TPS-Option, wenn Fernzugriff installiert ist.

Threat Prevention Subscription (TPS) umfasst ein Intrusion-Prevention-System (IPS) und ein Intrusion-Detection-System (IDS) zur Abwehr von Eindringversuchen. TPS ergänzt einen integrierten Schutz gegen netzwerkseitige Bedrohungen wie Datenabgriffe, Schadprogramme, Command-and-Control-Datenverkehr und eine Vielzahl von Hackerwerkzeugen durch IPS-Funktionalität und eine datenstrombasierte Blockierung von Millionen bekannter Schadprogramme. Diese TPS-Option muss für jede Automation Firewall Next Generation zusätzlich bestellt werden.

Industrial Vulnerability Manager

In Automatisierungs- und Leitsysteme eingebettete Hardware- und Softwarekomponenten zeigen regelmäßig Sicherheitsschwächen, denen entgegengewirkt werden muss, um die Gefahr von Cyberattacken auf Anlagen und Fabriken zu verringern. Im Rahmen eines globalen Konzepts für das Patchmanagement ist es notwendig, die einzelnen Hardware- und Softwarekomponenten laufend zu überwachen, um ihre Schwächen zu identifizieren.

Der Industrial Vulnerability Manager hat die folgenden Merkmale:

- Hosting der in Ihr ICS eingebetteten Komponenten, die auf Sicherheitsschwächen überwacht werden sollen.
- Freie Zuweisung der Komponenten zu der aufgestellten Überwachungsliste.
- Integration mit:
  - SIMATIC Management Console
  - SINEC NMS
  - TIA Portal
  - Proneta
  - SiESTA
- Dashboards mit Tabellen und Diagrammen zum Hervorheben relevanter Informationen im Zusammenhang mit den veröffentlichten Sicherheitsbulletins.
- Automatische Herausgabe von Sicherheitsbulletins, sobald ein Komponentenlieferant eine neue Sicherheitsschwäche mit Auswirkung auf eine registrierte Komponente bekanntgibt.
- Die automatisch generierten Sicherheitsbulletins enthalten die folgenden Informationen:
  - Beschreibung der Schwachstelle.
  - Punktzahl gemäß Common Vulnerability Scoring System (CVSS) und Prioritätsstatus
  - Liste der betroffenen Komponenten.
  - Empfehlungen, Problemumgehungen und Patchstatus.
  - Vendor Advisory Link – Ratschläge für Lieferanten.
- Kennzeichnung der veröffentlichten Sicherheitsbulletins mit dem Bearbeitungsstatus („Offen“, „In Arbeit“, „Erledigt“).
- Die Anwendung ist über eine geschützte Web-Schnittstelle zugänglich.

Industrial Anomaly Detection

Die Siemens Industrial Anomaly Detection (IAD) ist eine wichtige Ergänzung des umfassenden Konzepts „Defense in Depth“. Sie stellt mit Informationen darüber, wie die Komponenten untereinander kommunizieren, die volle Transparenz der Kommunikation in einem Automatisierungs- und Leitsystem her. Somit können Abweichungen leicht erkannt und vom Anlagenbetreiber untersucht werden.

Die Siemens Industrial Anomaly Detection (IAD) lässt sich nahtlos in ein Automatisierungs- und Leitsystem integrieren und bietet die folgenden Funktionalitäten:

- Implementierung einer Verbindung zum IAD-Sensor über einen SPAN-Port (Switched Port Analyzer – Portspiegelung)
- Ein Sensor kann mit den Daten mehrerer SPAN-Ports arbeiten
- Zentrale Konsole dient auch zum Überwachen der Sensoren
- Visualisierung und Analyse über die zentrale Konsole
- Sensor und Zentrale sind auf einem Siemens IPC installiert
- Ereignisse können von der zentralen Konsole unkompliziert weitergeleitet werden, z.B. an ein SIEM-System

Mit SINEC Security Monitor hat Siemens ein Produkt auf den Markt gebracht, mit dem der Netzwerkverkehr gespiegelt und analysiert werden kann, sodass eine passive, kontinuierliche Identifizierung aller Assets im Netzwerk möglich ist. Zusätzlich können bei Bedarf gezielte aktive Scans mit geringer Beeinträchtigung gestartet werden. Die erkannten Assets werden mit einer umfangreichen Datenbank bekannter Schwachstellen abgeglichen, um Geräte zu identifizieren, die von Schwachstellen betroffen sind. Darüber hinaus ist die Software in der Lage zu lernen, wie die normale Kommunikation im Netzwerk aussieht, und kann mithilfe von KI-basierter Analyse Anomalien erkennen.

Security Information Event Management (SIEM)

Schnell zunehmende Cyberbedrohungen und neu entstehende Sicherheitsrisiken erfordern eine präventive und branchenspezifische Abwehrstrategie.

Ein wirksamer Schutz beginnt mit einem Überblick über alle Aktivitäten in Systemen, Netzwerken, Datenbanken und Anwendungen. Zum Schutz industrieller Automatisierungssysteme gegen Cyberbedrohungen kann ein Security Information and Event Management System (SIEM) eingesetzt werden. Damit können sicherheitsrelevante Vorfälle schneller erkannt, Anlagenbetreiber früher informiert und Gegenmaßnahmen rascher eingeleitet werden.

Ein SIEM-System erfasst kontinuierlich Netzwerkinformationen und Informationen von Sicherheitsgeräten, verknüpft, analysiert und visualisiert diese und leitet anschließend geeignete Sicherheitsmaßnahmen ab.

SIMATIC Security Service Packages

Viele der SIMATIC-Produkte bieten Konfigurationen zur Erhöhung des Security Levels. Diese Konfigurationen sind jedoch in der Praxis nur selten anzutreffen – oft aufgrund mangelnden Sicherheits-Know-hows.

Unsere Industrial Security-Experten unterstützen Sie mit maßgeschneiderten Paketen für SIMATIC-Automatisierungssysteme dabei, das volle Potenzial des Security Levels Ihrer Assets auszuschöpfen.

Ihre Vorteile:

- Transparenz über die Einhaltung von Sicherheitsstandards
- Implementierung und Projektierung von Sicherheitsfunktionen nach dem neuesten Stand der Technik
- Aufrechterhaltung des Security Levels über den gesamten Lebenszyklus

Security Services können bei Ihrem Siemens-Ansprechpartner vor Ort bestellt werden, siehe:

- \44\ – Industrial Security Services – Sicherheitsoptimierung – SIMATIC Security Service Packages

# 12. Links und Literatur

Tabelle 12-1 – Liste der Links

| Nr. | Dokument |
|---|---|
| \1\ | Rundum-Schutz mit Industrial Security – Systemintegrität<br>https://support.industry.siemens.com/cs/de/en/view/92605897 |
| \2\ | Rundum-Schutz mit Industrial Security – Netzwerksicherheit<br>https://support.industry.siemens.com/cs/de/en/view/92651441 |
| \3\ | Rundum-Schutz mit Industrial Security – Anlagensicherheit<br>https://support.industry.siemens.com/cs/de/en/view/50203404 |
| \4\ | Siemens Industry Online Support<br>https://support.industry.siemens.com/cs/ww/de/ |
| \5\ | Checkliste für die Einrichtung von SCALANCE-Geräten<br>https://support.industry.siemens.com/cs/ww/de/view/109745536 |
| \6\ | PAN-OS® Administrator's Guide<br>https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/getting-started |
| \7\ | Palo Alto Website zu PAN-OS<br>https://docs.paloaltonetworks.com/pan-os.html |
| \8\ | SCALANCE SC-600 – Web Based Management (WBM)<br>https://support.industry.siemens.com/cs/ww/de/view/109754815 |
| \9\ | SCALANCE SC-600 – Betriebsanleitung<br>https://support.industry.siemens.com/cs/ww/de/view/109754812 |
| \10\ | SCALANCE M800 Web – Based Management (WBM)<br>https://support.industry.siemens.com/cs/ww/de/view/109751635 |
| \11\ | SCALANCE M874, M876 – Betriebsanleitung<br>https://support.industry.siemens.com/cs/document/109972231 |
| \12\ | SCALANCE M826 – Betriebsanleitung<br>https://support.industry.siemens.com/cs/ww/de/view/99450800 |
| \13\ | SCALANCE M874, M876 – Betriebsanleitung<br>https://support.industry.siemens.com/cs/ww/de/view/74518712 |
| \14\ | SCALANCE WAM766 – Betriebsanleitung<br>https://support.industry.siemens.com/cs/document/109973939 |
| \15\ | SCALANCE WUM763 – Betriebsanleitung<br>https://support.industry.siemens.com/cs/document/109973938 |
| \16\ | SCALANCE XC-200 / XF-200BA – Web Based Management (WBM)<br>https://support.industry.siemens.com/cs/ww/de/view/109750283 |
| \17\ | SCALANCE XC-200 – Betriebsanleitung<br>https://support.industry.siemens.com/cs/ww/de/view/109743149 |
| \18\ | SCALANCE XF-200BA – Betriebsanleitung<br>https://support.industry.siemens.com/cs/ww/de/view/109750282 |
| \19\ | TIM 1531 IRC – Handbuch<br>https://support.industry.siemens.com/cs/de/en/view/109748454 |
| \20\ | RTU3051C – Betriebsanleitung<br>https://support.industry.siemens.com/cs/ww/de/view/109750942 |
| \21\ | Industrial Ethernet Security – Grundlagen und Anwendung – Projektierungshandbuch<br>https://support.industry.siemens.com/cs/ww/en/view/109738463 |
| \22\ | SIMATIC NET: S7-1500 – Industrial Ethernet CP 1543-1 https://support.industry.siemens.com/cs/document/109973328 |

| | |
|---|---|
| \23\ | Kommunikation mit SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro<br>https://support.industry.siemens.com/cs/ww/en/view/59192925 |
| \24\ | S7-1500 Handbuchsammlung<br>https://support.industry.siemens.com/cs/de/en/view/86140384 |
| \25\ | WinCC OA Security Guideline (neueste Fassung, Registrierung erforderlich)<br>https://www.winccoa.com/downloads/category/safety-security.html |
| \26\ | Sicherheit mit SIMATIC-S7-Controllern<br>https://support.industry.siemens.com/cs/de/en/view/77431846 |
| \27\ | SIMATIC STEP 7 Basic/Professional V18 und SIMATIC WinCC V18<br>https://support.industry.siemens.com/cs/document/109815056 |
| \28\ | Netzwerkmanagement SINEC NMS<br>https://support.industry.siemens.com/cs/de/en/view/109762749 |
| \29\ | PM Analyze<br>https://www.siemens.com/global/en/products/automation/industry-software/automation-software/scada/pm-add-ons.html |
| \30\ | Kompatibilität mit Trellix Application Control<br>https://support.industry.siemens.com/cs/document/88653385 |
| \31\ | SIMATIC Energy Manager PRO V7.5 – Operation<br>https://support.industry.siemens.com/cs/document/109963217 |
| \32\ | SIMATIC Energy Manager PRO V7.5 – Acquisition<br>https://support.industry.siemens.com/cs/document/109963216 |
| \33\ | SIMATIC Energy Manager V7.5 – Installation https://support.industry.siemens.com/cs/document/109963215 |
| \34\ | SIMATIC Energy Manager PRO V7.2 – Systemhandbuch<br>https://support.industry.siemens.com/cs/ww/en/view/109748841 |
| \35\ | SIMATIC NET: Industrial Remote Communication – Remote-Netzwerk SINEMA Remote Connect – Betriebsanleitung<br>https://support.industry.siemens.com/cs/ww/en/view/109482122 |
| \36\ | Anwendungsbeispiel – Firewall von Industrial-Security-Systemen verstehen und anwenden<br>https://support.industry.siemens.com/cs/ww/en/view/22376747 |
| \37\ | Übersicht: Sicherer Remote-Zugriff mit VPN<br>https://support.industry.siemens.com/cs/ww/en/view/26662448 |
| \38\ | Einsatz von Whitelisting mit Trellix Application Control für PCS 7 und WinCC<br>https://support.industry.siemens.com/cs/ww/de/view/88653385 |
| \39\ | Palo Alto – Best Practices for Securing Administrative Access<br>https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html |
| \40\ | Siemens Industrial Cybersecurity Services<br>https://new.siemens.com/global/en/products/services/industry/digital-industry-services/industrial-security-services.html |
| \41\ | Empfohlene Sicherheitseinstellungen für IPCs im Industrieumfeld<br>https://support.industry.siemens.com/cs/de/en/view/109475014 |
| \42\ | SIMATIC Prozessleitsystem PCS 7 Sicherheitskonzept PCS 7 & WinCC (Basic)<br>https://support.industry.siemens.com/cs/document/109973483 |
| \43\ | Benutzerverwaltung für SCALANCE-Geräte mit RADIUS-Protokoll<br>https://support.industry.siemens.com/cs/ww/en/view/98210507 |
| \44\ | Aktivierung der Zwei-Faktor-Authentifizierung für SCALANCE-Geräte<br>https://support.industry.siemens.com/cs/ww/en/view/109954344 |
| \45\ | Konfiguration der Sicherheitsfunktionen in TIA Portal V17<br>https://support.industry.siemens.com/cs/ww/en/view/109798583 |
| \46\ | Benutzerverwaltung & Zugriffssteuerung mit TIA Portal V19<br>https://support.industry.siemens.com/cs/ww/en/view/109973173 |
| \47\ | Zertifikate mit TIA Portal verwenden<br>https://support.industry.siemens.com/cs/ww/en/view/109769068 |
| \48\ | Zentrales Benutzermanagement mit der "User Management Component (UMC)"<br>https://support.industry.siemens.com/cs/ww/en/view/109780337 |
| \49\ | SIMATIC NET: Netzwerkmanagement SINEC INS<br>https://support.industry.siemens.com/cs/ww/en/view/109781023 |
| \50\ | Meldungen einer SIMATIC S7-1200/S7-1500 CPU per Syslog an SINEC INS senden<br>https://support.industry.siemens.com/cs/ww/en/view/51929235 |
| \51\ | Sicherheitsvorfälle in WinCC OA |

https://www.winccoa.com/documentation/WinCCOA/latest/en_US/security_events/security_events.html

# 13. Anhang – Liste der Sicherheitsmaßnahmen nach IEC 62433-3-3

**Dieses Kapitel beschreibt die Pflichten der verschiedenen Beteiligten gemäß IEC 62433-3-3**
(**SS**: Systemlieferant Siemens, **SI:** Systemintegrator, **EK:** Endkunde)

**WinCC OA-Kapitel** verweist auf die WinCC OA Security Guideline.
https://www.winccoa.com/downloads/category/safety-security.html (Registrierung erforderlich)

| IEC 62443-3-3 Level 1 | | | Kapitel | WinCC OA-Kapitel |
|---|---|---|---|---|
| SR 1.1 | Identifizierung und Authentifizierung von menschlichen Benutzern | SS: Die verschiedenen Systeme (WinCC, Windows-Betriebssystem, S7-1500, SCALANCE, TIA, SINEC NMS) bieten alle die Möglichkeit zur Benutzerverwaltung.<br>SI: Benutzerauthentifizierung muss für alle Systeme aktiviert und vorkonfiguriert sein | 5.2.1 | • User Administration<br>• Activate Kerberos encryption for WinCC OA systems |
| SR 1.3 | Kontenverwaltung | SS: Die verschiedenen Systeme (WinCC, Windows-Betriebssystem, S7-1500, SCALANCE, TIA, SINEC NMS) bieten alle die Möglichkeit zur Benutzer- und Rollenverwaltung. | | • Activate Kerberos encryption for WinCC OA systems |
| SR 1.4 | Kennungsverwaltung | SS: für alle Systeme möglich<br>SI: muss die eindeutige Identität konfigurieren | | • Activate Kerberos encryption for WinCC OA systems |
| SR 1.5 | Verwaltung der Authentifikatoren | SS: für alle Systeme möglich | | • Delete or disable unneeded default users on OS Level<br>• Delete or disable all default users on WinCC OA level<br>• Limit usage of the root user |
| SR 1.7 | Stärke der Authentifizierung durch Passwörter | SS: für alle Systeme möglich<br>SI: muss die Mindestanforderungen an das Passwort konfigurieren | 6.1 | • Single Sign On<br>• Password strength |
| SR 1.10 | Rückmeldung vom Authentifikator | SS: erfüllt für alle Systeme | 5.2.1 | • Usage of Operating system (Windows or Linux) based user management |
| SR 1.11 | Erfolglose Anmeldeversuche | SS: erfüllt für Windows-Betriebssystem; alle anderen Systeme durch AD-Integration<br>SI: muss AD- und Brute-Force-Schutz installieren und konfigurieren<br>EK: muss entscheiden, welches System Brute-Force-Schutz benötigt | 5.2.1 | • Single Sign On |
| SR 1.12 | Nutzungshinweis | wird hauptsächlich für Fernverbindungen benötigt<br>SS: möglich für Windows-Betriebssystem, SCALANCE, WinCC OA<br>SI: muss den eindeutigen Systemnamen für all die verschiedenen Systeme (WinCC Faceplate, Windows Background, SCALANCE) konfigurieren und anzeigen | 5.2.1 | • Configure System use notification |

| | | | | |
|---|---|---|---|---|
| | | | 5.6.1 | k.A. auf WinCC OA-Ebene, Informationen verfügbar auf Systemebene<br>• Security Cells and Network Architecture |
| SR 1.13 | Zugriff über nicht vertrauenswürdige Netzwerke | SS: möglich, z.B. durch VPN auf der Automation Firewall | | |
| SR 2.1 | Durchsetzung der Autorisierung | SS: Funktionalität basiert auf den Netzwerkkomponenten Windows, WinCC OA und SCALANCE. Diese forcieren diese Funktionalität.<br>SI: Bei Verwendung von Fremdkomponenten muss der SI die einwandfreie Funktionalität sicherstellen. | | • Administration of Role-Based user authorizations |
| SR 2.3 | utzungskontrolle von tragbaren und mobilen Geräten | SS: Musterkonzept muss ein Konzept für die Härtung von Datenports (USB, Ethernet,) enthalten.<br>SI: muss das Konzept implementieren<br>EK: muss dem Konzept folgen | | |
| SR 2.4 | Mobiler Code | SS: Musterkonzept muss ein Konzept enthalten, mit dem die Ausführung von mobilem Code verhindert wird (Makros, Java, Skript, ActiveX...). Das Konzept muss auf Desktop UI Clients basieren. Konzept sollte Web-Clients ausschließen => kein mobiler Code erforderlich<br>SI: Implementierung des Härtungskonzepts (Ausführung von mobilem Code muss deaktiviert werden) | | • WinCC OA User Interface Configuration<br>• Whitelisting/Application Control |
| SR 2.5 | Sitzungssperrung | SS: Funktionalität integriert in SCALANCE, WinCC OA und Windows; Musterkonzept muss Ratschläge enthalten<br>SI: muss die Abmeldefunktion muss entsprechend den Anforderungen des Endkunden und den Empfehlungen des Musterkonzepts konfigurieren | | • Automatic User Logout in WinCC OA |
| SR 2.8 | Auditierbare Ereignisse | SS: Funktionalität integriert in SCALANCE, WinCC OA und Windows;<br><br>WinCC OA stellt Protokolle zur Verfügung | | • User Administration<br>• Activate Kerberos encryption for WinCC OA systems |
| SR 2.9 | Speicherkapazität für Aufzeichnungen | SI: muss genügend Speicherkapazität für die Protokollierung und Verarbeitung von Daten für einen bestimmten Zeitraum gemäß den Anforderungen des Endkunden/den gesetzlichen Bestimmungen bereitstellen<br>WinCC OA stellt Protokolle zur Verfügung | | • Configure Fail-Safe mode of WinCC OA (Emergency Mode) |
| SR 2.10 | Reaktion auf ausgefallene Ereignisdatenverarbeitung | WinCC OA stellt Protokolle zur Verfügung | | • Configure Fail-Safe mode of WinCC OA (Emergency Mode) |
| SR 3.1 | Kommunikationsintegrität | SS: Die Kommunikationsintegrität wird durch TCP/IP-Mechanismen geschützt. | | • Usage of TLS/SSL for plant communication<br>• Activate Kerberos encryption for WinCC OA systems |
| SR 3.2 | Schutz vor Schadcode | SS: Empfehlung des Musterkonzepts sollte Whitelisting sein; getestete Virenschutzlösungen sind eine Alternative<br>SI: muss den Schutz gegen Schadprogramme implementieren und | | k.A. auf WinCC OA-Ebene, Informationen verfügbar auf Systemebene<br>• Virus Scanner |

| | | | | |
|---|---|---|---|---|
| | | konfigurieren<br>EK: muss die Muster häufig aktualisieren, wenn eine Virenschutzlösung ausgewählt wird | | |
| SR 3.3 | Verifikation der Sicherheitsfunktionalität | SI: muss eine Checkliste erstellen, um die Implementierung der Sicherheitsmaßnahmen nach der FAT-, SAT- und Instandhaltungsphase zu überprüfen | | • Virus Scanner<br>• Security tests |
| SR 3.4 | Software- und Informationsintegrität | SS: Software sollte durch Whitelisting und WinCC OA-Binärsignaturen geschützt werden. TIA / S7-1500 sollte durch UMC und Schutzlevel sowie Online-/Offline-Prüfung geschützt werden. Der WinCC OA-Schutz muss im Musterkonzept zum Schutz von WinCC OA-Projektdaten durch Windows-Mechanismen beschrieben werden. WinCC OA arbeitet noch an der Erfüllung der Anforderung, sollte in Version 3.17 kommen<br>SI: muss Sicherheitsmaßnahmen implementieren und konfigurieren | | • Digital signatures for binaries and libraries<br>• Whitelisting/Application Control |
| SR 3.5 | Eingabevalidierung | SS: WinCC OA bietet die Funktionalität zur Validierung von Eingaben.<br>SI: muss die Syntax- und Inhaltsvalidierung im Projekt implementieren | | • Penetration tests |
| SR 4.1 | Vertraulichkeit von Informationen | SS: Bereitstellung für Windows, WinCC OA und Geräte durch Benutzerauthentifizierung und Verschlüsselung<br>SI: muss die Verwaltung von Benutzerrechten implementieren und konfigurieren<br>EK: muss einen Prozess zur Speicherung und Übertragung vertraulicher Daten definieren und einrichten | | Usage of TLS/SSL for plant communication<br>• Activate Kerberos encryption for WinCC OA systems<br>• Protection via authorization levels in WinCC OA |
| SR 4.3 | Verwendung von Verschlüsselung | SS: Verschlüsselte Daten (Passwörter) werden nach bewährten Verfahren gespeichert. | | • Usage of encrypted communication protocols<br>• IPsec Bypass Technology<br>• Usage of TLS/SSL for plant communication |
| SR 5.1 | Netzwerksegmentierung | SS: Die Projektierung des Musterkonzepts implementiert eine Segmentierung des Automatisierungsnetzwerks. | 5.1.1 | • Security Cells and Network Architecture |
| SR 5.2 | Schutz der Zonengrenzen | SS: Musterkonzept muss Firewall- und Zonenkonzept beinhalten (DMZ, externe Verbindung und insbesondere interne Netzwerksegmente).<br>SI: muss Firewall und Zonen implementieren und konfigurieren | 5.2.1 | k.A. auf WinCC OA-Ebene, Informationen verfügbar auf Systemebene<br>• Security Cells and Network Architecture |

| | | | |
|---|---|---|---|
| SR 5.3 | Beschränkung der Verwendung der persönlichen Kommunikation | SS: Musterkonzept sollte die Sperrung der persönlichen Kommunikation vom IT-/Büronetzwerk zum Automatisierungsnetzwerk (Empfang von Nachrichten) in das Zonenkonzept aufnehmen.<br>SI: muss die Sperrung implementieren und konfigurieren (in der Firewall-Konfiguration) | k.A. auf WinCC OA-Ebene, Informationen<br>verfügbar auf Systemebene<br>• Security Cells and Network<br>Architecture |
| SR 5.4 | Partitionierung von Anwendungen | SS: Musterkonzept sollte separate Geräte für kritische Funktionen wie Firewall, Quarantänestation, AD-Controller, WinCC OA-Server definieren. Weniger kritische Funktionen wie WSUS können in Instanzen (VMs) aufgeteilt werden.<br>SI: muss die Funktionen auf den Geräten implementieren | |
| SR 6.1 | Zugriffsmöglichkeit auf Ereignisprotokolle | SS: WinCC-Ereignisprotokolle können als Windows-Dateien abgerufen werden. | • Definition of Access Control List<br>(ACL)<br>• Secure Desktop – Kiosk-Mode |
| SR 7.2 | Ressourcenmanagement | SS: Im Musterkonzept müssen Maßnahmen wie Härtung, Ressourcenplanung, Überwachung der Ressourcen (Bandbreite, Speicherplatz, CPU-Last, Speicherlast...) beschrieben werden.<br>SI: muss Maßnahmen für Ressourcenmanagement, Überwachung und Alarmierung implementieren<br>EK: muss auf Alarmmeldungen reagieren | • Keep secure settings in WinCC OA<br>config file<br>• Configure Fail-Safe mode of<br>WinCC OA (Emergency Mode) |
| SR 7.3 | Datensicherung im Automatisierungssystem | SS: Musterkonzept muss ein Datensicherungskonzept für Betriebssystem, Benutzersoftware, Projekte, Protokolldaten, Konfigurationen usw. enthalten.<br>SI / EK: muss ein Datensicherungskonzept einschließlich Sicherungszeitpläne und Zuständigkeiten definieren | • Implement Backup and Restore<br>concept |
| SR 7.4 | Wiederherstellung des Automatisierungssystems | SI: muss eine vollständige Systemsicherung vornehmen und die Wiederherstellung testen, um die Wiederherstellung sicherzustellen | • Restore procedure |
| SR 7.5 | Notstromversorgung | SS: Im Musterkonzept muss die Notwendigkeit einer Notstromversorgung genannt werden.<br>SI / EK: muss die benötigte Notstromversorgung definieren und implementieren | |
| SR 7.6 | Netzwerk- und Sicherheitseinstellungen | SI: muss die Sicherheitsrichtlinie von SS (dieses Dokument) umsetzen | • Division in security cells |
| SR 7.7 | Minimierung des Funktionsumfangs | SS: Musterkonzept beschreibt Maßnahmen wie Härtung und Benutzerverwaltung.<br>SI: muss die geringste Funktionalität gemäß den Richtlinien für Härtung und Benutzerverwaltung implementieren | • Hardening |

| IEC 62443-3-3 Level 2 | | | Kapitel | WinCC OA-Kapitel |
|---|---|---|---|---|
| SR 1.1 RE 1 | Eindeutige Identifizierung und Authentifizierung | SS: Die verschiedenen Systeme (WinCC, Windows-Betriebssystem, S7-1500, SCALANCE, TIA, SINEC NMS) bieten alle die Möglichkeit zur benutzerbasierten Verwaltung auf der Grundlage von Active Directory.<br>SI: AD-, UMC- und Verschaltungskonfiguration (AD -> UMC, AD -> SCALANCE, AD -> OPC_OA, UMC -> TIA) | 5.2.1 | • User Administration<br>• Activate Kerberos encryption for<br>WinCC OA systems |
| SR 1.2 | Identifizierung und Authentifizierung von Softwareprozessen und Geräten | SS: Benutzerauthentifizierung in Windows, RADIUS-Identifikation an Switches<br>SI: muss die Identifizierung implementieren und konfigurieren<br>EK: muss den Austauschprozess dokumentieren; neue MAC-Adresse muss in RADIUS hinzugefügt werden | 5.2.1 | • Server-side Authentication for<br>Managers with session binding<br>• Usage of TLS/SSL for plant<br>communication |
| SR 1.8 | PKI-Zertifikate (Public-Key-Infrastruktur) | SI: Wenn PKI verwendet wird, muss die Implementierung nach bewährten Verfahren erfolgen. | 5.2.1 | • Usage of TLS/SSL for plant<br>communication |
| SR 1.9 | Stärke der Authentifizierung durch öffentliche Schlüssel | SI: Wenn PKI verwendet wird, muss die Implementierung nach bewährten Verfahren erfolgen. | 5.2.1 | • Enforce usage of strong cipher<br>suite |
| SR 2.1 RE 1 | Durchsetzung der Autorisierung für alle Benutzer | | | • Administration of Role-Based user<br>authorizations<br>• Limit usage of the root user |
| SR 2.1 RE 2 | Abbildung der Berechtigung auf Rollen | SS: Funktionalität basiert auf den Netzwerkkomponenten Windows, WinCC OA und SCALANCE. Diese forcieren diese Funktionalität.<br>SI: muss rollenbasierte Berechtigungen konfigurieren<br>EK / SI: muss Benutzer Rollen zuordnen | | • Single Sign On |
| SR 2.6 | Beendigung einer Fernzugriffssitzung | SS: Muss im Musterkonzept beschrieben werden; Beispiele für die technische Implementierung (Schlüsselschalter für SCALANCE M als SINEMA RC Endpunkt. Kann auch über einen Ausgang der SPS ausgelöst werden, um die Abmeldung zu automatisieren.)<br>SI: muss eine Lösung aus dem Musterkonzept implementieren, um eine Fernverbindung nach einer bestimmten Zeit und bei Bedarf zu beenden | | • Automatic User Logout in WinCC<br>OA |
| SR 2.11 | Zeitstempel | SS: Funktionalität basiert auf den Netzwerkkomponenten Windows, WinCC OA und SCALANCE. | | • Usage of TLS/SSL for plant communication<br>• Integrity with MAC |
| SR 3.2 RE 1 | Schutz vor Schadcode an Eingangs- und Ausgangspunkten | SS: Erfüllung mit Quarantänestation im Musterkonzept (lokale und Fernübertragung von Daten) | | |

| | | | | |
|---|---|---|---|---|
| | | SI: muss die Lösung implementieren und konfigurieren | | |
| SR 3.7 | Fehlerbehandlung | SS: stellt Lösungen für die Fehleranalyse bereit<br>SI, EK: kann Informationen weiterleiten; muss minimale Daten nach dem Grundsatz „Kenntnis erforderlich“ bereitstellen | | • Penetration tests<br>• Implement Risk assessment process based on VDI/VDE 2182 |
| SR 3.8 | Sitzungsintegrität | SS: WinCC bietet standardmäßig TLS-Sicherheit.<br>SI: TLS darf nicht deaktiviert werden. | | • Server-side Authentication for Managers with session binding |
| SR 3.9 | Schutz von Auditinformationen | SS: Windows bietet Funktionen zum Schutz des Sicherheitsprotokolls. WinCC OA schützt Protokolle von Benutzerinteraktionen.<br>SI: muss die Benutzerverwaltung gemäß Musterkonzept implementieren und konfigurieren (Windows, WinCC OA, Geräte, Log Server…) | | • Secure Desktop – Kiosk-Mode |
| SR 4.1 RE 1 | Schutz der Vertraulichkeit bei der Speicherung oder Übertragung über nicht vertrauenswürdige Netzwerke | SS: Übertragungen über ein nicht vertrauenswürdiges Netzwerk (Ferndienst) werden im Musterkonzept über VPN gesichert.<br>SI: muss ein VPN implementieren und konfigurieren | | • Usage of TLS/SSL for plant communication<br>• Activate Kerberos encryption for WinCC OA systems<br>• Protection via authorization levels in WinCC OA |
| SR 4.2 | Dauerhaftigkeit von Informationen | SI / EK: muss den Datenbereinigungsprozess definieren, implementieren und konfigurieren | | • System Decommissioning |
| SR 5.2 RE 1 | Deny by default, allow by exception | SS: Musterkonzept sollte ein Beispiel für eine Firewall-Konfiguration für die benötigte WinCC OA- / Automatisierungskommunikation enthalten (Ethernet-Protokoll, Ports und Anwendungen usw., die für NG-Funktionen benötigt werden).<br>SI: muss die Firewall-Einstellungen implementieren und konfigurieren | 5.1.2 | k.A. auf WinCC OA-Ebene, Informationen verfügbar auf Systemebene<br>• Security Cells and Network Architecture |
| SR 6.2 | Kontinuierliche Überwachung | SS: Musterkonzept muss ein System für die kontinuierliche Überwachung (z.B. SIEM oder IAD) enthalten und beschreiben.<br>SI: muss das System für die kontinuierliche Überwachung implementieren und konfigurieren | | Handling of Security Incidents |
| SR 7.1 RE 1 | Kommunikationslasten verwalten | SS: Musterkonzept muss die Fähigkeit der SCALANCE-Geräte und der Firewall zur Verwaltung der Kommunikationslasten beschreiben.<br>SI: muss Geräte implementieren, die in der Lage sind, Kommunikationslasten zu verwalten, und die Ratenbegrenzung konfigurieren | 5.1.5 | • Keep secure settings in WinCC OA config file<br>• Usage of WinCC OA mxProxy and restriction of open ports |
| SR 7.3 RE 1 | Verifikation der Datensicherung | SS: Musterkonzept muss die Verifikation der Datensicherung nennen.<br>SI / EK: muss definieren, wer für die | | • Backup verification |

| | | | | |
|---|---|---|---|---|
| | | Verifikation der Datensicherung verantwortlich ist, und den Prozess implementieren | | |
| SR 7.8 RE 1 | Verzeichnis der Komponenten einer Automatisierungslösung oder IT-Infrastruktur | SS: Im Musterkonzept sollten die Notwendigkeit und die Möglichkeiten des Asset Managements genannt werden.<br>SI / EK: muss Asset Management definieren und implementieren | | • Hardening |

| IEC 62443-3-3 Level 3 | | | Kapitel | WinCC OA-Kapitel |
|---|---|---|---|---|
| SR 1.3 RE 1 | Einheitliche Kontenverwaltung | SS: für alle Systeme möglich<br>SI: muss einheitliche Konten konfigurieren | | • Activate Kerberos encryption for<br>WinCC OA systems |
| SR 1.5 RE 1 | Beglaubigung der Identität von Softwareprozessen durch Hardwaresicherheit | | | • Single Sign On |
| SR 1.7 RE 1 | Erzeugung und Lebensdauerbeschränkungen von Passwörtern für menschliche Benutzer | SS: Windows-Betriebssysteme bieten diese Optionen. Alle anderen Systeme können diese Möglichkeit mithilfe der AD-Authentifizierung bereitstellen.<br>SI: muss die AD-Authentifizierung installieren und konfigurieren | 6.1 | • Single Sign On<br>• Password strength |
| SR 1.9 RE 1 | Hardwaresicherheit für die Authentifizierung durch öffentliche Schlüssel | SI: muss in der PKI-Lösung implementiert werden | | Noch nicht vorhanden |
| SR 1.13 RE 1 | Genehmigung ausdrücklicher Zugriffsanfragen | | 5.6.1 | k.A. auf WinCC OA-Ebene, Informationen<br>verfügbar auf Systemebene<br>• Protected Maintenance Access of<br>Access via untrusted networks |
| SR 2.3 RE 1 | Security-Status tragbarer und mobiler Geräte durchsetzen | SS: Musterkonzept muss Konzept für Quarantänestation enthalten<br>SI: muss das Konzept implementieren<br>EK: muss dem Konzept folgen | | |
| SR 2.4 RE 1 | Prüfung der Integrität mobilen Codes | SS: integriert in das Härtungskonzept; kein mobiler Code im Konzept erforderlich<br>SI: muss das Härtungskonzept implementieren | | • Whitelisting/Application Control<br>• Mobile Code |
| SR 2.7 | Begrenzung der Anzahl gleichzeitiger Sitzungen | SS: Musterkonzept definiert bereits eine sichere Infrastruktur (VNC...).<br>SI: muss DMZ und VNC implementieren und konfigurieren | | Noch nicht vorhanden |
| SR 2.8 RE 1 | Zentral verwaltetes System | SS: Musterkonzept sollte den Log Server enthalten.<br>SI: muss Log Server implementieren und alle Komponenten so konfigurieren, dass Protokolle an den Server gesendet werden | | • User Administration<br>• Activate Kerberos encryption for WinCC OA systems |

| | | | | |
|---|---|---|---|---|
| SR 2.9 RE 1 | Warnung, wenn die Kapazitätsgrenze zur Speicherung von Ereignisdatensätzen erreicht ist | SS: WinCC OA bietet die Option, Alarme für die Festplattennutzung zu konfigurieren.<br>SI: Log Server auswählen, der Alarme senden kann. Muss WinCC OA und Log Server entsprechend konfigurieren, um den EK zu alarmieren. | | • Configure Fail-Safe mode of WinCC OA (Emergency Mode) |
| SR 2.11 RE 1 | Interne Zeitsynchronisation | SS: Musterkonzept muss einen Zeitserver enthalten, alle Geräte (SCALANCE, Windows, WinCC OA) können synchronisiert werden.<br>SI: muss Server und Clients für die Synchronisierung implementieren und konfigurieren | | • Usage of TLS/SSL for plant communication<br>• Integrity with MAC |
| SR 2.12 | Nicht-Abstreitbarkeit | SS: WinCC OA bietet die Option, (konfigurierte) menschliche Benutzerinteraktionen zu protokollieren. | | • User Administration<br>• Server-side Authentication for Managers with session binding<br>• Integrity with MAC |
| SR 3.1 RE 1 | Kryptographische Schutzmaßnahmen zur Bewahrung der Integrität | SS: WinCC OA-Client <-> Server ist immer mit TLS gesichert. WinCC <-> S7-1500 sollte OPC-UA mit Verschlüsselung sein; muss im Musterkonzept definiert werden.<br>SI: muss entsprechend Musterkonzept implementieren | | • Usage of TLS/SSL for plant communication<br>• Activate Kerberos encryption for WinCC OA systems |
| SR 3.2 RE 2 | Zentrale Verwaltung und Meldewesen zum Schutz vor Schadcode | SS: Whitelisting- und Virenschutzlösungen von Siemens ermöglichen eine zentrale Verwaltung.<br>SI: muss die zentrale Verwaltung implementieren und konfigurieren | | k.A. auf WinCC OA-Ebene, Informationen verfügbar auf Systemebene<br>• Virus Scanner |
| SR 3.3 RE 1 | Automatisierte Mechanismen zur Verifikation der Sicherheitsfunktionalität | SI: muss eine automatisierte Lösung entwickeln und implementieren, um die Umsetzung von Sicherheitsmaßnahmen nach der FAT-, SAT- und Instandhaltungsphase zu verifizieren | | Noch nicht vorhanden |
| SR 4.2 RE 1 | Bereinigung gemeinsam genutzter Speicherressourcen | SI / EK: muss den Datenbereinigungsprozess von flüchtigen Speicherressourcen definieren, implementieren und konfigurieren | | Usage of TLS/SSL for plant communication<br>• System Decommissioning |
| SR 5.1 RE 2 | Unabhängigkeit von nicht-automatisierungstechnischen Netzwerken | SS: ja, es ist keine Verbindung zu anderen Netzwerken erforderlich | 5.1.1 | • Security Cells and Network Architecture |
| SR 5.2 RE 2 | Inselmodus | SS: Musterkonzept sollte Beispiele für das Konzept des Inselmodus enthalten, einschließlich Prozess und der technische Implementierung für den Wechsel in den Inselmodus. | 5.1.2 | NZ |
| SR 5.2 RE 3 | Fail close | SS: Musterkonzept muss eine Zonenarchitektur definieren, die die Möglichkeit eines unabhängigen, vollständigen Betriebs jedes Segments bietet. | 5.2.1 | |

| | | | | |
|---|---|---|---|---|
| | | SI: muss das Zonenkonzept gemäß Musterkonzept implementieren | | |
| SR 5.3 RE 1 | Verbot der Verwendung der persönlichen Kommunikation | | | k.A. auf WinCC OA-Ebene, Informationen verfügbar auf Systemebene<br>• Security Cells and Network Architecture |
| SR 6.1 RE 1 | Programmgesteuerter Zugriff auf Ereignisprotokolle | SS: Ereignisprotokolle sind als Windows-Dateien verfügbar. Programmgesteuerter Zugriff über Tools / Skripte von Drittanbietern.<br>SI: muss gegebenenfalls Rücksprache mit EK halten und implementieren | | • Required knowledge<br>• Detection of security incidents |
| SR 7.1 RE 2 | DoS-Auswirkungen auf andere Systeme oder Netzwerke begrenzen | SS: Musterkonzept muss verschiedene Maßnahmen beschreiben, um die Möglichkeit und Auswirkungen von DoS zu begrenzen. Insbesondere die Fähigkeit der SCALANCE-Geräte und der Firewall zur Verwaltung von Kommunikationslasten, Systemhärtung, Benutzerrechteverwaltung.<br>SI: muss die beschriebenen Maßnahmen umsetzen | 5.1.5 | |
| SR 7.3 RE 2 | Automatisierung der Datensicherung | SS: Musterkonzept muss Optionen zur Automatisierung der Datensicherung nennen.<br>SI: muss die Automatisierung der Datensicherung implementieren | | |
| SR 7.6 RE 1 | Maschinenlesbare Meldungen der momentanen Sicherheitseinstellungen | SI / EK: muss eine automatisierte Meldung der aktuellen Sicherheitseinstellungen definieren und implementieren | | • Secure handling of WinCC OA<br>ASCII Manager |
| IEC 62443-3-3 Level 4 | | | Kapitel | WinCC OA-Kapitel |
| SR 1.1 RE 3 | Multifaktor-Authentifizierung für alle Netzwerke | SS: verfügbar für Windows-Betriebssystem<br>SI: Implementierung und Konfiguration | 5.2.1 | |
| SR 1.7 RE 2 | Lebensdauerbeschränkungen von Passwörtern für alle Benutzer | SS: Verfügbar für WinCC OA und andere Systeme und Geräte, die mit AD verbunden sind, mit Ausnahme von lokalen Administratorkonten.<br>SI: muss Passwort, Zertifikatsablauf für alle Konten und Benutzer konfigurieren<br>EK: muss ablaufende Konten verwalten; muss lokale Administratorkonten ändern, bei denen ein automatischer Ablauf nach einem bestimmten Zeitraum nicht möglich ist | 6.1 | • Usage of WinCC OA external<br>Single Sign On<br>• Password strength |
| SR 2.11 RE 2 | Schutz und Integrität der Zeitquelle | SS: Im Musterkonzept sollte eine sichere Zeitquelle (SICLOCK) beschrieben werden. | | • Usage of TLS/SSL for plant<br>communication |

| | | | |
|---|---|---|---|
| | | SI: muss die Sicherheit für die Zeitquelle gemäß Musterkonzept konfigurieren | • Integrity with MAC |
| SR 2.12 RE 1 | Nicht-Abstreitbarkeit | SS: Alle Aktionen (Menschen, WinCC OA-Softwarekomponente...) können in WinCC OA protokolliert werden.<br>SI: muss die Protokollierung konfigurieren und aktivieren | • Usage of encrypted communication protocols<br>• Integrity with MAC |
| SR 3.3 RE 2 | Verifikation der Sicherheitsfunktionalität im laufenden Betrieb | SI: muss eine automatisierte Lösung entwickeln und implementieren, um die Umsetzung von Sicherheitsmaßnahmen im laufenden Betrieb zu verifizieren | Noch nicht vorhanden |
| SR 3.9 RE 1 | Ereignisdatensätze auf nur einmal beschreibbaren Speichermedien | SI / EK: muss das Medienkonzept „Nur Lesen" für Ereignisprotokolle implementieren, konfigurieren und verwenden | |
| SR 4.1 RE 2 | Schutz der Vertraulichkeit über Zonengrenzen hinweg | SS: Übertragungen über Zonengrenzen hinweg werden im Musterkonzept über VPN gesichert.<br>SI: muss ein VPN implementieren und konfigurieren | |

# 14. Anhang

## 14.1. Service und Support

### SiePortal

Die integrierte Plattform für Produktauswahl, Einkauf und Support – und Verbindung von Industry Mall und Online Support. Die neue Startseite, ersetzt die bisherigen Startseiten der Industry Mall sowie des Online Support Portals (SIOS) und fasst diese zusammen.

- Produkte & Services
  Unter Produkte & Services finden Sie alle unsere Angebote, die bisher im Mall Katalog verfügbar waren.
- Support
  Im Bereich Support finden Sie alle Informationen, die für die Lösung technischer Probleme mit unseren Produkten hilfreich sind.
- mySieportal
  mySiePortal ist Ihr persönlicher Bereich, der Funktionen, wie z.B. die Warenkorbverwaltung oder die Bestellübersicht anzeigt. Den vollen Funktionsumfang sehen Sie hier erst nach erfolgtem Login.

Das SiePortal rufen Sie über diese Adresse auf:
sieportal.siemens.com

### Technical Support

Der Technical Support von Siemens Industry unterstützt Sie schnell und kompetent bei allen technischen Anfragen mit einer Vielzahl maßgeschneiderter Angebote – von der Basisunterstützung bis hin zu individuellen Supportverträgen.

Anfragen an den Technical Support stellen Sie per Web-Formular:
support.industry.siemens.com/cs/my/src

### SITRAIN – Digital Industry Academy

Mit unseren weltweit verfügbaren Trainings für unsere Produkte und Lösungen unterstützen wir Sie praxisnah, mit innovativen Lernmethoden und mit einem kundenspezifisch abgestimmten Konzept.
Mehr zu den angebotenen Trainings und Kursen sowie deren Standorte und Termine erfahren Sie unter:
siemens.de/sitrain

### Industry Online Support App

Mit der App "Industry Online Support" erhalten Sie auch unterwegs die optimale Unterstützung.
Die App ist für iOS und Android verfügbar: