Siemens
Industry
Online
Support

ANWENDUNGSBEISPIEL

WinCC Unified Security Musterkonzept für eine Abwasser- und Wasserbehandlungsanlage

Leitfaden zur sicheren Projektierung V1.0

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. **Die Anwendungsbeispiele unterliegen nicht den Standardtests und Qualitätsprüfungen eines kostenpflichtigen Produkts und können funktionale und Leistungsdefekte sowie andere Fehler und Sicherheitslücken enthalten Sie sind verantwortlich für den ordnungsgemäßen und sicheren Betrieb der Produkte gemäß allen geltenden Vorschriften, einschließlich der Überprüfung und Anpassung des Anwendungsbeispiels für Ihr System, und stellen sicher, dass nur geschultes Personal es so verwendet, dass Sachschäden oder Verletzungen von Personen vermieden werden. Sie sind allein verantwortlich für jede produktive Nutzung.**

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. Jede weitere Verwendung der Anwendungsbeispiele ist ausdrücklich nicht gestattet und es werden keine weiteren Rechte gewährt. Sie dürfen die Anwendungsbeispiele in keiner anderen Weise verwenden, insbesondere ist jegliches direkte oder indirekte Training oder Verbesserungen von KI-Modellen ausdrücklich untersagt.

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 und Ihnen die Lizenz jederzeit zu kündigen. 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://www.siemens.com/global/en/general/terms-of-use.html).

Cybersecurity-Hinweise

Siemens bietet Produkte und Lösungen mit Industrial Cybersecurity-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 Cybersecurity-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 Cybersecurity finden Sie unter www.siemens.com/cybersecurity-industry.

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 Cybersecurity RSS Feed unter https://www.siemens.com/cert.

1. Vorwort

Cybersicherheit muss als ganzheitlicher Ansatz betrachtet werden, der nicht nur die Technologie, sondern auch die implementierten Prozesse auf Basis geltender Normen wie ISO 27001 (ISMS/IT) und IEC 62443 (IACS/OT) umfasst.

Daher erfordern industrielle Automatisierungs- und Leitsysteme (IACS) ein umfassendes und etabliertes Cybersicherheits-Framework, das Sicherheitsrichtlinien, -verfahren und -strategien berücksichtigt und gegebenenfalls umsetzt, um einen sicheren Betrieb der Anlage zu gewährleisten.

Dieses Security Musterkonzept soll Endkunden, Erstausrüstern und Systemintegratoren eine grundlegende Anleitung für die sichere Einrichtung von Wasser- und Abwasserbehandlungsanlagen bieten. Das Dokument dient als Mindestauslegungsreferent, das die Produktdokumentation der Automatisierungsgeräte ergänzt.

Erfahrungsgemäß fallen spätere Modernisierungen oder Anlagenerweiterungen viel leichter, wenn das Automatisierungsprojekt von Anfang an und soweit möglich als „konform mit Sicherheitsstandards" aufgesetzt wird. Dies bedeutet, dass Anwender bestimmte Grundregeln beachten müssen, um sicherzustellen, dass die Anforderungen an die Sicherheitsfunktionalität auch in Zukunft das erforderliche Sicherheitsniveau bieten.

Die empfohlene Methodik, das Defense-in-Depth-Konzept, beruht auf der Norm IEC 62443 und den Ergebnissen weitreichender praktischer Erfahrung.

SIMATIC WinCC Unified

Kern des Musterkonzepts ist SIMATIC WinCC Unified, das bevorzugte SCADA-System für kleine Wasser- und Abwasserbehandlungsanlagen. WinCC Unified vereint SIMATIC HMI und SCADA in einem Produkt und ermöglicht so die Konfiguration und das Management von Laufzeiten für verschiedene Gerätetypen über ein einheitliches Engineering-System. Dieser zentralisierte Ansatz gewährleistet die konsistente Implementierung von Sicherheitsrichtlinien, Schutzmaßnahmen und Systemhärtung auf allen in der Anlage verwendeten Visualisierungsgeräten.

HINWEIS

Bewertung der Risiken für Kundenprojekte

Für jedes Kundenprojekt muss eine Risikobewertung oder auch Threat and Risk Analysis (Bedrohungs- und Risikoanalyse, TRA), durchgeführt werden, selbst wenn das Musterkonzept genau wie beschrieben umgesetzt wird.

In der TRA, auf der das Musterkonzept basiert, wurden Annahmen über das Schutzniveau und die Auswirkungen auf die Anlage im Falle eines erfolgreichen Cyberangriffs getroffen. Diese Annahmen können je nach Kunde variieren, was auch in einer unterschiedlichen Risikostufe resultieren kann. Bei dem Musterkonzept handelt es sich um eine Modelllösung bzw. einen Vorschlag, wie Sicherheitsanforderungen u. a. aus der IEC 62443 mit Siemens-Produkten bestmöglich umgesetzt werden können.

Wenn das Kundensystem abweichend von diesem Musterkonzept aufgebaut ist, muss unbedingt eine Risikobewertung durchgeführt werden, um festzustellen, wie sich diese Abweichung auf die Sicherheit des Systems auswirken könnte.

2. Sicherheitsstrategien

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

Anlagenbetreiber, Systemintegratoren und Erstausrüster müssen mit hoher Priorität den Schutz von Automatisierungs- und Leitsysteme gegen Manipulation und Schadsoftware forcieren. Nur so können Verfügbarkeit und Qualität gesichert sowie nationale und internationale Normen und Anforderungen erfüllt werden.

Aufgrund der stetig wachsenden Vielfalt von Angriffen und der Komplexität in der Prozessindustrie ist es oft nicht leicht, Risiken und Bedrohungen zu identifizieren und die richtige IT- und OT-Sicherheitsstrategie anzuwenden. Konsequente, regelmäßige und gut geschützte Datensicherungen sowie die Implementierung einer umfassenden Strategie für die Cybersicherheit, einschließlich der Isolierung kritischer Systeme mittels geeigneter Software, Installation der neuesten Sicherheitspatches und der Einsatz einschlägig geschulter Mitarbeiter und Lieferanten sollten selbstverständlich sein.

2.1. Norm IEC 62443 – Übersicht

IEC 62443 ist eine internationale Normenreihe zur Verbesserung der Cybersicherheit von industriellen Automatisierungs- und Leitsystemen (IACS). Die Normen befassen sich mit unterschiedlichen Aspekten der Cybersicherheit industrieller Automatisierungssysteme, wie zum Beispiel Netzwerksicherheit, Systemintegration, Sicherheitsmanagement und Risikobewertung.

IEC 62443 soll eine einheitliche und umfassende Methodik für den Schutz von industriellen Automatisierungssystemen bieten. Die Normenreihe enthält ausdrückliche Richtlinien, Anforderungen und bewährte Verfahrensweisen, die Unternehmen bei der wirksamen Umsetzung von Maßnahmen zur Cybersicherheit in ihren industriellen Automatisierungssystemen unterstützen.

Eine Übersicht der einzelnen Teile der Norm ist in folgender Abbildung dargestellt.

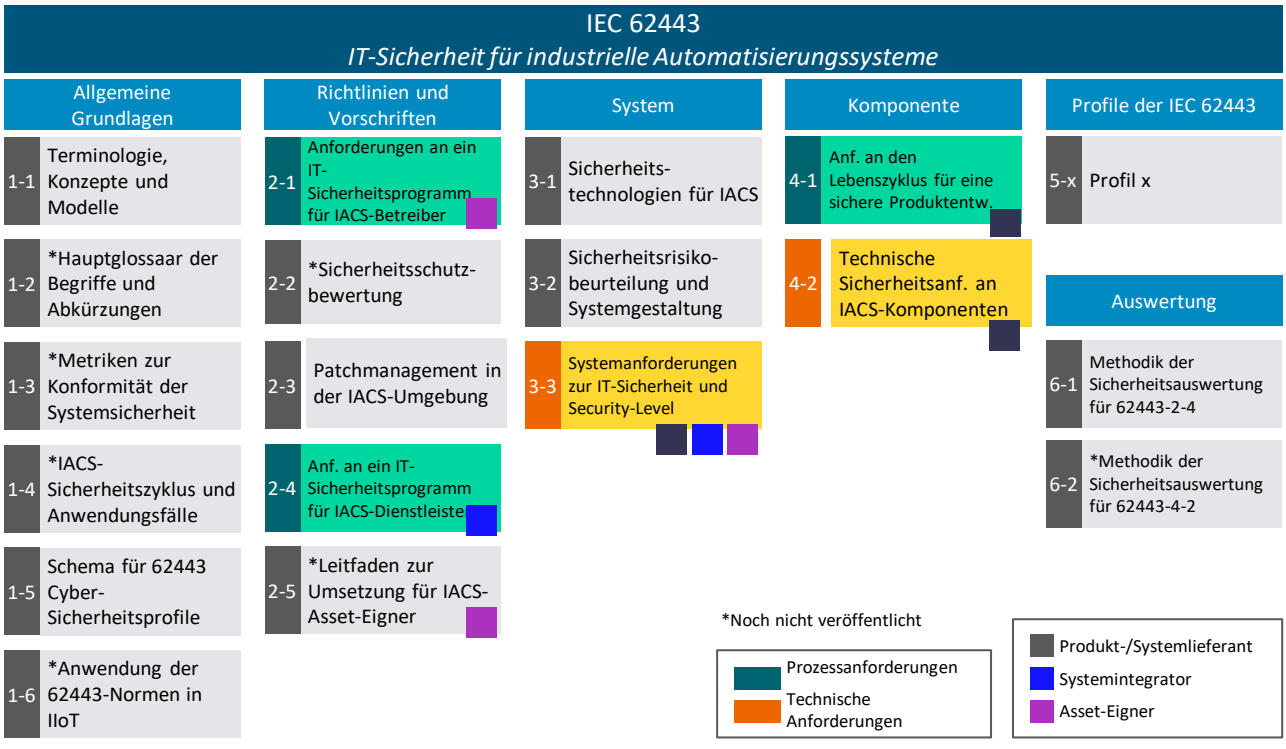

Abbildung 2-1: Übersicht über IEC 62443

Systemlebenszyklus

Sicherheitsrichtlinien unterstreichen, wie wichtig es ist, Industrial Security als Lebenszyklusaspekt zu betrachten. Um die Entwicklung sicherer Systeme zu gewährleisten, 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 wesentlichen Phasen: Produkt- oder Systementwicklung, Spezifikation, Integration und Inbetriebnahme, Betrieb und Instandhaltung und Außerbetriebnahme. Mit jeder dieser Phasen ist eine klare Verantwortung und ein primäres Ziel verknüpft.

Rollen und Anspruchsgruppen

Sicherheitsthemen müssen zwischen verschiedenen Rollen und Anspruchsgruppen koordiniert und kommuniziert werden (siehe Abbildung 2-2):

- Produktlieferanten implementieren im Rahmen des Produktentwicklungsprozesses Sicherheitsmaßnahmen wie Authentifizierung, sichere Kommunikationsmöglichkeiten oder robuste Kommunikations-Stacks in den Komponenten (IEC 62443 Teil 4-1 und IEC 62443 Teil 4-2).
- 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 (IEC 62443 Teil 3-3.) Systemintegratoren benötigen Sicherheitsinformationen vom Produktlieferanten, wie z. B. Handbücher und Richtlinien, um die Komponenten sicher projektieren zu können.
- Anlagenbetreiber und Dienstleister übernehmen den sicheren Betrieb und die Instandhaltung, hierunter fallen zum Beispiel die Benutzerverwaltung und die Handhabung von Berechtigungen oder das regelmäßige Aufspielen von Sicherheitspatches (IEC 62443 Teil 2-1, IEC 62443 Teil 2-3 und IEC 62443 Teil 2-4).

Diese Rollen müssen sich koordinieren und zusammenarbeiten, um über den gesamten Lebenszyklus eines Systems eine angemessene Sicherheit zu erreichen. Mangelnde Koordination, unzureichender Informationsaustausch oder eine unterschiedliche Interpretation von Sicherheitsthemen konterkariert die gemeinsamen Anstrengungen der verschiedenen Beteiligten.

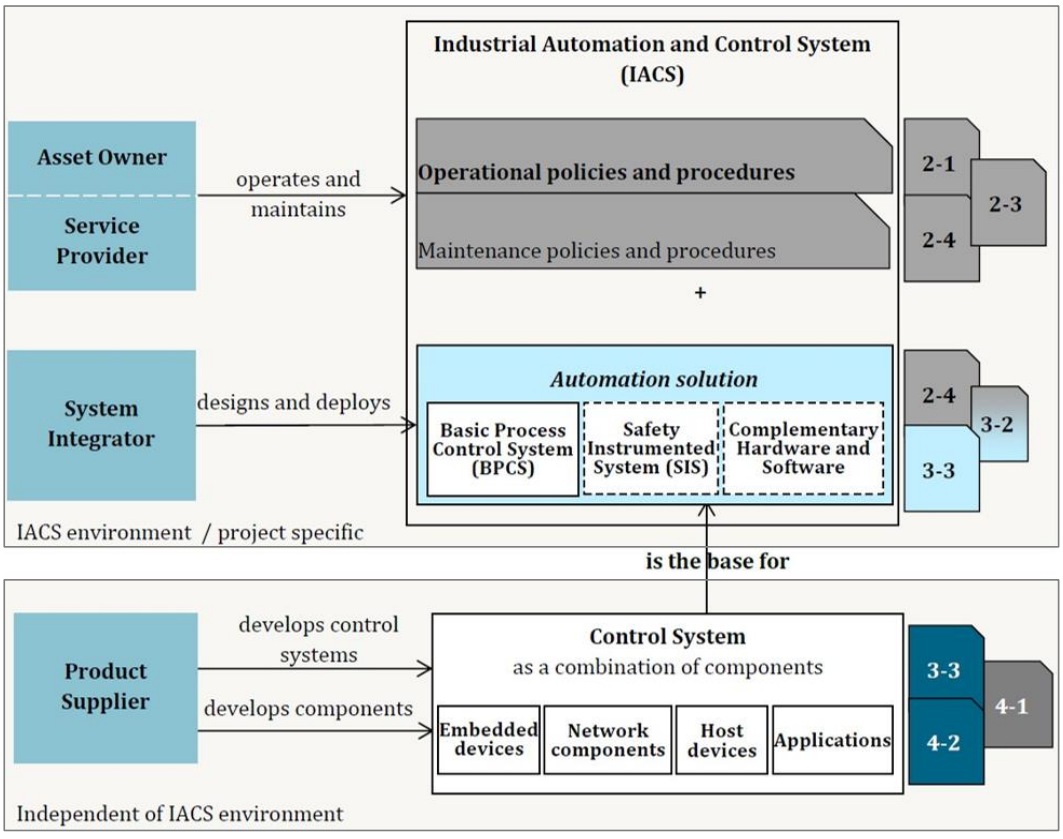

Abbildung 2-2: Rollen nach IEC 62443

2.2. Sicherheitskonzept „Defense-in-Depth“

Ein alles überspannender Schutz industrieller Einrichtungen gegen Cyberattacken muss auf allen Ebenen gleichzeitig gewährleistet sein, vom Gesamtbetrieb bis zum Einzelarbeitsplatz, von der Zugriffssteuerung bis zum Kopierschutz. Die Norm IEC 62443 empfiehlt daher das Konzept „Defense-in-Depth“ als Strategie für einen umfassenden Schutz. Dieser Ansatz für Operational Technology (OT) umfasst mehrere Schutzebenen, um ein Netzwerk oder System vor potenziellen Angriffen zu schützen, da kein einzelnes Sicherheitstool oder keine einzelne Sicherheitsmaßnahme für einen vollständigen Systemschutz ausreicht.

Das Defense-in-Depth-Konzept basiert auf dem Prinzip, dass der Einsatz verschiedener Sicherheitsebenen unerlässlich ist, um Angreifer dazu zu zwingen, mehrere Barrieren zu überwinden, bevor sie Zugriff auf ein System erhalten oder es kompromittieren können. Zu den identifizierten Sicherheitsebenen innerhalb dieses Konzepts gehören Anlagensicherheit, Netzwerksicherheit und Systemintegrität.

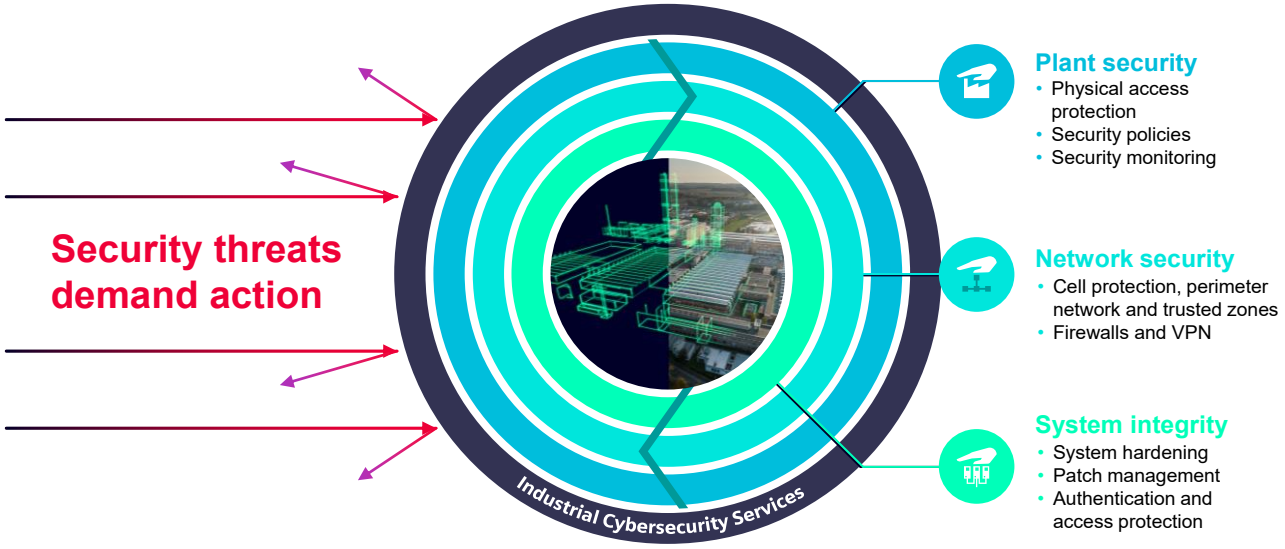

Abbildung 2-3: Sicherheitskonzept „Defense-in-Depth“

Durch die Umsetzung mehrere Schutzebenen kann ein Unternehmen oder eine Organisation dafür sorgen, dass ein Angreifer auch im Falle einer erfolgreichen Attacke nicht sofort auf das komplette System oder Netzwerk zugreifen kann. Eine Defense-in-Depth-Abwehr für ein Automatisierungs- und Leitsystem erfordert mehrere Schutz- und Aktionsebenen, was bedeutet, dass Anlagenbetreiber und Lösungsanbieter vielfältige und sehr unterschiedliche Sicherheitsthemen bearbeiten müssen. Hierbei reicht die Bandbreite von der Systemintegrität und Netzwerksicherheit bis zur Anlagensicherheit und zu organisatorischen Maßnahmen.

2.2.1. Anlagensicherheit

Physische Sicherheitsmaßnahmen

Kontrolle des physischen Zugangs zu Gebäuden, einzelnen Räumen, Schalt- und Steuerschränken, Geräten, Maschinen, Kabeln und Drähten. Zu den physischen Sicherheitsmaßnahmen sollten eigene Sicherheitszellen und benannte verantwortliche Personen gehören.

Ebenso wichtig ist die Umsetzung des physischen Schutzes auch an entfernten Einzelplatzsystemen. So stellen beispielsweise externe Pumpstationen oder Regenwasserbecken im Musterkonzept eigene Sicherheitszellen dar.

Sicherheitsmaßnahmen auf Organisationsebene

Hierzu gehören Sicherheitsrichtlinien, Sicherheitskonzepte, Sicherheitsstrategien, Sicherheitskontrollen, Risikoanalysen, Risikobewertungen und Risikoaudits, Maßnahmen zur Sicherheitsaufklärung und Schulungen.

2.2.2. Netzwerksicherheit

Unterteilung in Sicherheitszellen

In einer abgesicherten Netzwerkarchitektur ist das Steuerungsnetzwerk in verschiedene aufgabenbezogene Ebenen unterteilt. Zu diesem Zweck sollten Techniken der Perimeterzonierung angewandt werden. Dabei kommen Systeme im Perimeternetzwerk (DMZ) zum Einsatz, die durch eine oder mehrere Firewalls (Frontend-Firewall, Backend-Firewall oder Threehomed-Firewall) von anderen Netzwerken (z. B. Internet, Büronetzwerk) abgeschirmt werden.

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

Jede Sicherheitszelle sollte nur über einen einzigen Zugangspunkt verfügen (in der Regel durch eine Firewall realisiert), um Benutzer, Geräte und Anwendungen zu authentifizieren, eine richtungsbasierte Zugriffssteuerung zu implementieren, Zugriffsberechtigungen zuzuweisen und Eindringversuche zu erkennen.

Der so realisierte einzige Zugangspunkt fungiert als primärer Zugangspunkt zum Netzwerk einer Sicherheitszelle und dient als erster Kontrollpunkt für die Verwaltung von Zugriffsrechten auf Netzwerkebene.

Absicherung der Kommunikation zwischen zwei Sicherheitszellen über ein „unsicheres" Netzwerk

Bei Einsatz der Perimeterzonierungstechnik und Kommunikation über Zugangspunkte sollte immer eine zertifikatbasierte, authentifizierte und verschlüsselte Kommunikation praktiziert werden. Hierfür eignen sich Tunnelprotokolle wie PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol) und IPsec (IP Security).

Darüber hinaus kann die Kommunikation über Protokolle wie RDP (Remote Desktop Protocol) oder HTTPS abgesichert werden, die auf serverbasierten Zertifikaten basieren. In diesen Fällen findet die Kommunikation über die Firewall hinweg mit Technologien wie Transport Layer Security (TLS) oder Secure Sockets Layer (SSL) statt. Auch die vertikale Integration, von der Anlage bis hin zu übergeordneten Systemen, kann durch sicheren Kommunikationsprotokollen wie OPC UA abgesichert werden.

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

Systematische Vorgehensweisen beim Installieren von Aktualisierungen auf Anlagensystemen

Erkennung und Abwehr von Schadprogrammen

Einsatz geeigneter und richtig konfigurierter Virenscanner und Whitelisting von Software

2.3. Lösungskonzept

Angesichts der Vielzahl der Anforderungen ist es nur 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. In Abschnitt 2.2 werden zahlreiche technische Lösungen, Werkzeuge und bewährte Verfahren vorgestellt, die berücksichtigt werden sollten – aber Projektteams fehlt oftmals die Zeit und Erfahrung, geeignete Lösungen für jeden Sicherheitsaspekt auszuwählen. Daher konzentrieren sich Teams häufig intensiv auf bestimmte Themen und vernachlässigen dabei unbeabsichtigt andere Themen.

Um das Sicherheits-Engineering besser handhabbar zu machen, präsentiert Siemens an dieser Stelle eine Reihe von Musterkonzepten für Automatisierungs- und Leitsysteme. Diese Security Musterkonzepte bieten Unterstützung in Form von Verweisen auf bestimmte Ressourcen und gewährleisten, dass alle nach IEC 62443-2-4 vorgeschriebenen sicherheitsbezogenen Dokumente in technische Projekte einfließen. Dieser Ansatz entspricht sowohl der Norm IEC 62443-2-4 als auch der Norm IEC 62443-3-3.

Mit WinCC Unified als SCADA-System ist dieses Musterkonzept dafür vorgesehen, die Anforderungen einer bestimmten, aber dennoch typischen kleinen Wasser- und Abwasserbehandlungsanlage zu erfüllen.

3. Musterkonzept – Abwasserbehandlungsanlage

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

Die in diesem Dokument behandelte ABA bereitet zwischen 200 und 2.000 m³ pro Tag auf. Die meisten Teile der Anlage befinden sich in unmittelbarer Nähe zueinander, mit einer maximalen Entfernung von 1000 Metern. Dezentrale Gebäude, wie die externe Pumpstation und das Regenwasserbecken, sind über Remote Terminal Units (RTUs) verbunden.

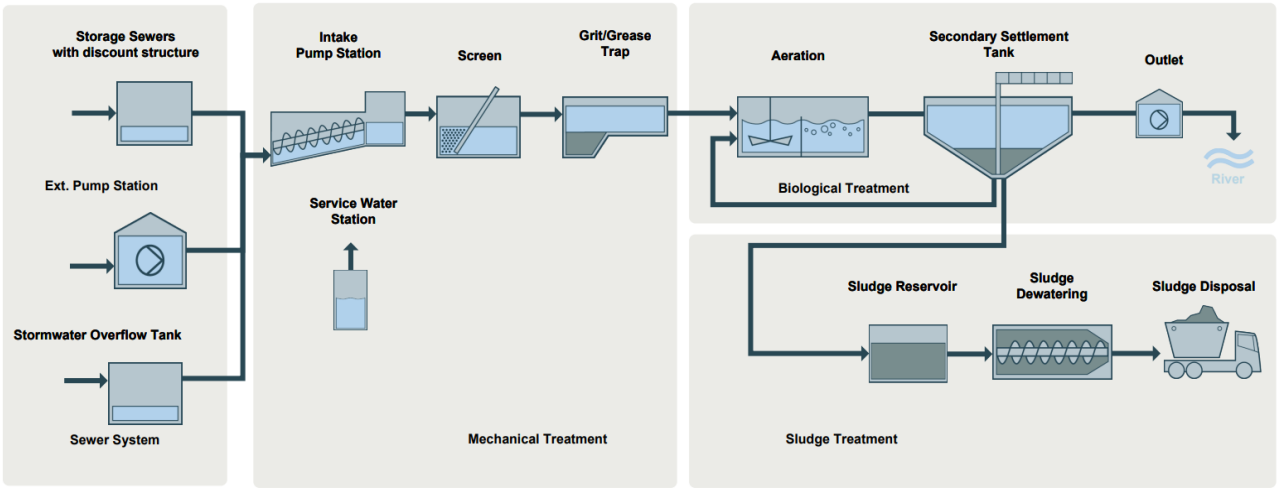

Abbildung 3-1: Abwasserbehandlungsanlage

Die Musterarchitektur kann auch als Referenz für eine Wasserbehandlungsanlage (WBA) verwendet werden. Die entsprechenden Prozesse sind in der folgenden Tabelle dargestellt.

Tabelle 3-1: Prozesse in Abwasser- und Wasserbehandlungsanlagen

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

3.1. Prozessbeschreibung

Eine kleine Abwasserbehandlungsanlage sammelt das Abwasser von ca. 1.000 bis 10.000 Haushalten und bereitet es auf, damit das behandelte Wasser wiederverwendet werden kann.

Die Abwasseraufbereitung erfolgt in vier Hauptschritten:

1. Kanalisation
2. Mechanische Behandlung
3. Biologische Behandlung
4. Schlammbehandlung

3.1.1. Kanalisation

Die Kanalisation bildet die Zulaufseite der Abwasserbehandlungsanlage und speist die Anlage über verschiedene 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 das Überlaufwehr im Regenwasserbecken und reduziert so 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.

3.1.2. 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 der 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 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.

3.1.3. 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. Der Schlamm, der schwerer als Wasser ist, setzt sich am Boden des Beckens ab. Ein kontinuierlich rotierender Räumer bewegt den überschüssigen Schlamm zu einem Sammelbecken. Rücklaufschlammpumpen fördern den Schlamm aus dem Sammelbecken zurück in das Belüftungsbecken. Überschüssiger Schlamm wird der Schlammbehandlung zugeführt.

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

3.1.4. Schlammbehandlung

Der letzte Schritt besteht in der Aufbereitung und Entsorgung des Klärschlamms. Schlamm ist großteils Wasser mit Anteilen von Feststoffen, die aus Abwasser entfernt wurden.

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

3.2. Systemarchitektur

Die WinCC Unified-Systemarchitektur für die Abwasserbehandlungsanlage ist in folgender Abbildung dargestellt.

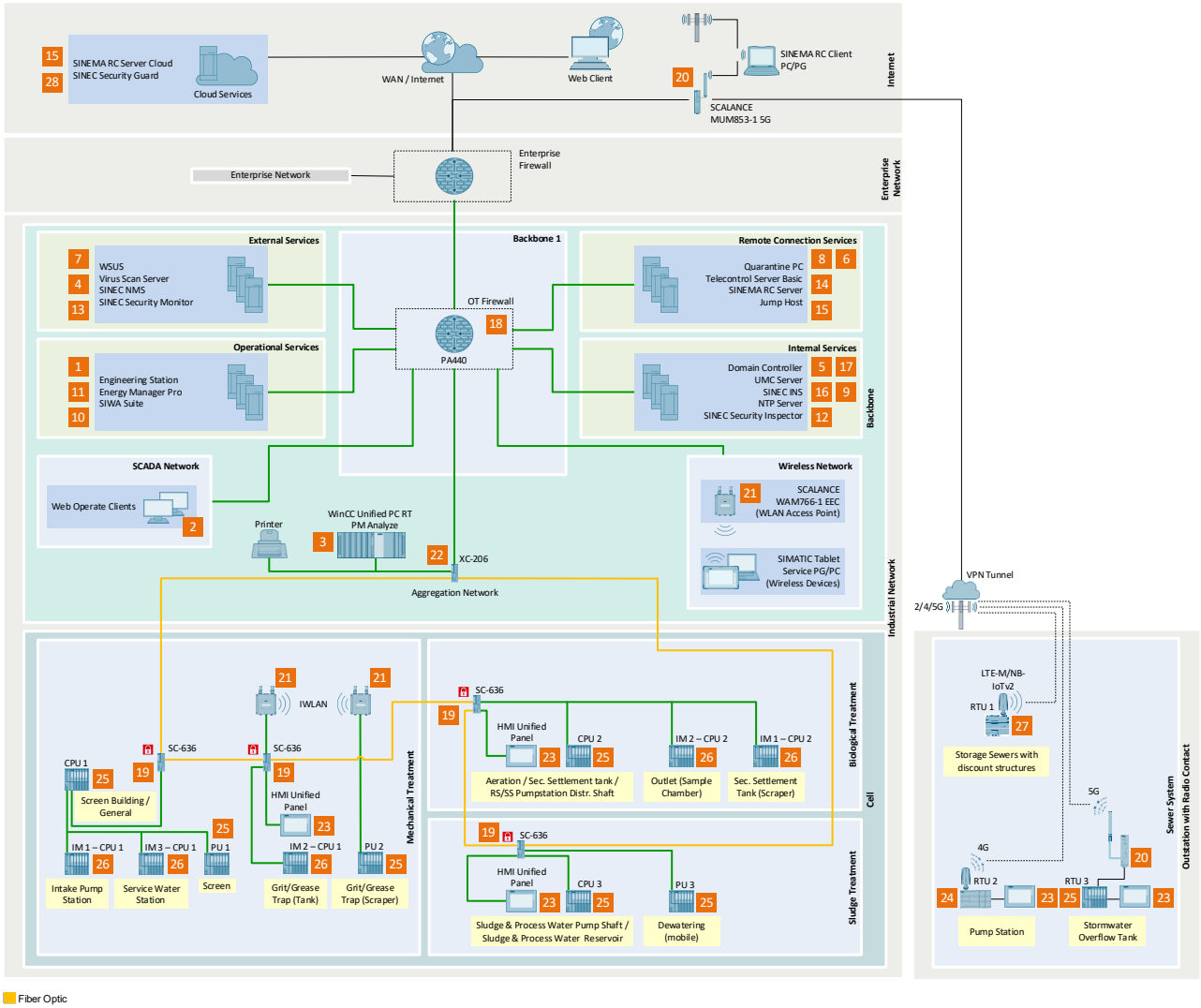

Abbildung 3-2: WinCC Unified-Systemarchitektur

3.2.1. Systemkomponenten für das Musterkonzept einer Abwasserbehandlungsanlage

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: Kommunikationsgerät, das den Datenfluss zwischen Geräten in einem Netzwerk ermöglicht bzw. begrenzt (z. B. Firewall), aber nicht direkt mit einem Steuerungsprozess interagiert.
- Eingebettetes Gerät: Spezielles Gerät mit eingebetteter Software zur Überwachung und Steuerung eines industriellen Prozesses (z. B. SPS, Sensoren, Stellantriebe, Remote-E/A usw.).

Die im Musterkonzept verwendeten Systemkomponenten sind in den folgenden Tabellen aufgeführt. Die SCI-Kennung (System Component Identifier) entspricht der Nummer, die in der Systemarchitektur zugewiesen ist (Abbildung 3-2).

Hosts/Anwendungen im OT-Netzwerk

Tabelle 3-2: Im Musterkonzept verwendete Hosts/Anwendungskomponenten

SCI	Komponente	Funktion
1	Engineering-Station	PC-Station für das zentralisierte anlagenweite Engineering: WinCC Unified-Geräte und -SPSen. • Projektierung der Hardware. • Projektierung der Kommunikationsnetzwerke. • Projektierung kontinuierlicher und sequenzieller Prozessreihenfolgen. • Bedien- und Beobachtungsstrategien. • Übersetzung und Download des Projekts auf Automatisierungsgeräte.
2	Web Operate Clients	Dienen der Steuerung und Überwachung. WinCC Unified-Clients greifen auf die Daten der WinCC Unified PC RT zu, um den Prozess zu visualisieren und zu beeinflussen.
3	WinCC Unified PC RT	PC-basiertes Visualisierungssystem für alle Arten von Applikationen – von Einzelplatzlösungen direkt an der Maschine bis hin zu komplexen SCADA-Lösungen. Kann in redundant konfiguriert werden, um hohe Verfügbarkeit und Zuverlässigkeit zu gewährleisten.
	PM ANALYZE	Add-on zum Vorbereiten und Erstellen spezieller Berichte in Konformität mit den Wasser- und Abwasservorschriften, beispielsweise der DWA.
4	SINEC NMS	Netzwerkmanagementsystem zum Überwachen und Verwalten industrieller Netzwerke.
5	Domain Controller	Unterstützt den Active Directory Service und liefert Zeitinformationen.
6	Jump Host	Bietet Zugriff auf die Anlage via Terminal oder Remote-Kommunikation.
7	Infrastruktur-PC – WSUS, Virenscan-Server	Wird für Aktualisierungen von Windows und Virenschutzanwendungen eingesetzt.
8	Quarantäne-PC	Dient dazu, potenziell schädliche Dateien oder Software zu analysieren, zu testen und einzudämmen.
9	SINEC Security Inspector	Tool für das Anlagenmanagement und zur Automatisierung von Sicherheitsprüfungen. Scannt und testet Netzwerkkomponenten und -systeme auf Schwachstellen und überprüft regelmäßig den Sicherheitsstatus des gesamten OT-Netzwerks.
10	SIWA Suite Server	Software für die Wasser- und Abwasserwirtschaft. Besteht aus SIWA Optim, LeakControl, Abwassersteuerung und Infrastruktursimulation.
11	Energy Manager Pro	Energiedatenmanagementsystem zum Erstellen der Grundlage für ein Energiebetriebsmanagement zum Steigern der Energieeffizienz und zum Senken der Energiekosten.
12	SINEC INS	Infrastructure Network Services. Tool für häufig benötigte zentrale Netzwerkdienste, insbesondere in OT-Netzwerken, wie RADIUS und Syslog.
13	SINEC Security Monitor	Tool zur Anomalieerkennung. Überwacht den Netzwerkverkehr und die Netzwerkressourcen mit Hinsicht auf abnormes Geräteverhalten und Netzwerkkommunikations-Anomalien.
14	TeleControl Server Basic	Für die industrielle Fernkommunikation und TeleControl-Anwendungen. Ermöglicht die Anbindung und Verwaltung von bis zu 5.000 SIMATIC RTUs an eine Leitstelle über Mobilfunkstandards wie GSM/GPRS und Ethernet-/Internetverbindungen.

SCI	Komponente	Funktion
15	SINEMA RC-Server	Bietet sicheren Fernzugriff über das Internet auf unterlagerte Netzwerke für Wartungs-, Bedienungs- und Diagnosezwecke.
16	UMC-Server	Zur Verwaltung von Benutzern und Benutzergruppen über Software- und Gerätegrenzen hinweg. Kann an das Active Directory angebunden werden, das auf dem Domain Controller gehostet wird.
17	NTP-Server	Gewährleistet eine genaue Zeitsynchronisierung auf allen vernetzten Geräten und Systemen.

Hosts/Anwendungen im Internet und Unternehmensnetzwerk

Tabelle 3-3: Hosts/Anwendungen im Internet und Unternehmensnetzwerk

SCI	Komponente	Funktion
15	SINEMA RC-Server-Cloud	Cloud-basierte Alternative zum lokalen SINEMA RC-Server, die im „Remote-Verbindungsdienste"-Netzwerk gehostet wird.
28	SINEC Security Guard	Cloud-basierte Schwachstellenmanagement-Lösung, um Daten zu Schwachstellen in Automatisierungsanlagen zu liefern.

Netzwerkkomponenten

Tabelle 3-4: Im Musterkonzept verwendete Netzwerkkomponenten

SCI	Komponente	Funktion
18	OT-Firewall	Schützt die OT-Prozesse vor Zugriffen aus äußeren Zonen wie dem Unternehmensnetzwerk und dem Internet und ermöglicht den Zugriff über zertifikatbasierte, verschlüsselte und signierte Kommunikation.
19	SCALANCE SC-636	Industrietaugliche Firewall zur Absicherung der Automatisierungszellen. Ist eine PROFINET-Kommunikation zwischen Automatisierungszellen erforderlich, müssen stattdessen Managed Switches wie der SCALANCE XC-206 2SPF zum Einsatz kommen.
20	SCALANCE MUM853-1 5G	Funkrouter für die leistungsstarke und sichere Anbindung von Ethernet-basierten Subnetzen über Mobilfunknetze – 5G, 4G (LTE) und 3G (UMTS) – oder in privaten 5G-Netzen.
21	SCALANCE WAM766-1 ECC	IWLAN-Zugangspunkt für die drahtlose Kommunikation auf der Grundlage von IEEE 802.11ax.
22	SCALANCE XC-206 – 2 SPF	Managed Layer-2-IE-Switch, der als Ring-Manager im Aggregationsnetzwerk fungiert.
-	SCALANCE XP-200-Serie	Familie von Managed Industrial Switches, die in Prozesszellen für die Bereiche Kanalisation, mechanische, biologische und die Schlammbehandlung eingesetzt werden. • XC-208: Zulaufpumpstation, Regenwasserbecken, externe Pumpstation, Rechen, Sand- und Fettfang, sekundäres Absetzbecken, Ablauf, Entwässerung. • XC-216: Rechenanlage/Allgemeines, Schlamm- und Prozesswasserbecken. • XC-224: Belüftung.

Eingebettete Geräte

Tabelle 3-5: Im Musterkonzept verwendete eingebettete Geräte

SCI	Komponente	Funktion
23	MTP1000 Unified Comfort	In den Zellen installierte HMI-Panels zur Prozesssteuerung und -überwachung.
24	S7-1200 PLC	S7-1200-Steuerung, die in der externen Pumpstation eingesetzt wird: • CPU 1214C Sie ist mit zusätzlicher Hardware ausgestattet: • CP 1243-7 LTE UE: Kommunikationsprozessor für die Anbindung eines SIMATIC S7-1200 an LTE-Netze im europäischen Frequenzbereich.
25	ET 200SP CPU	ET 200SP-Familie von Distributed Controllern, die in allen Zellen des Musterkonzepts eingesetzt werden: • CPU 1510SP-1 PN • CPU 1514SP-2 PN Sie sind mit zusätzlicher Hardware ausgestattet: • CP 1542SP-1: Kommunikationsprozessor für die Anbindung eines SIMATIC ET 200SP an Industrial Ethernet. • CP 1542SP-1 IRC: Kommunikationsprozessor für die Anbindung eines SIMATIC ET 200SP an TeleControl Server Basic mit IEC 60870-5-104 oder DNP3. • CM DP: Kommunikationsmodul für die Anbindung eines SIMATIC ET 200SP über PROFIBUS DP.
26	IM 155-6	Dezentrales Peripheriesystem IM 155-6PN BA. Kann zusammen mit zusätzlicher Hardware für die Anbindung an PROFIBUS-Netzwerke eingesetzt werden. • IE/PB LINK PN IO: Gateway zwischen Industrial Ethernet und PROFIBUS.
27	RTU 3051C	Kompakte, stromsparende Remote Terminal Unit, die mit Batterie oder Solarenergie betrieben wird. Wird in den Stauraumkanälen zur Überwachung des Wasserstands in der Kanalisation und des Überlaufwehrs installiert.

3.3. Zonen und vorgesehene Betriebsumgebung

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

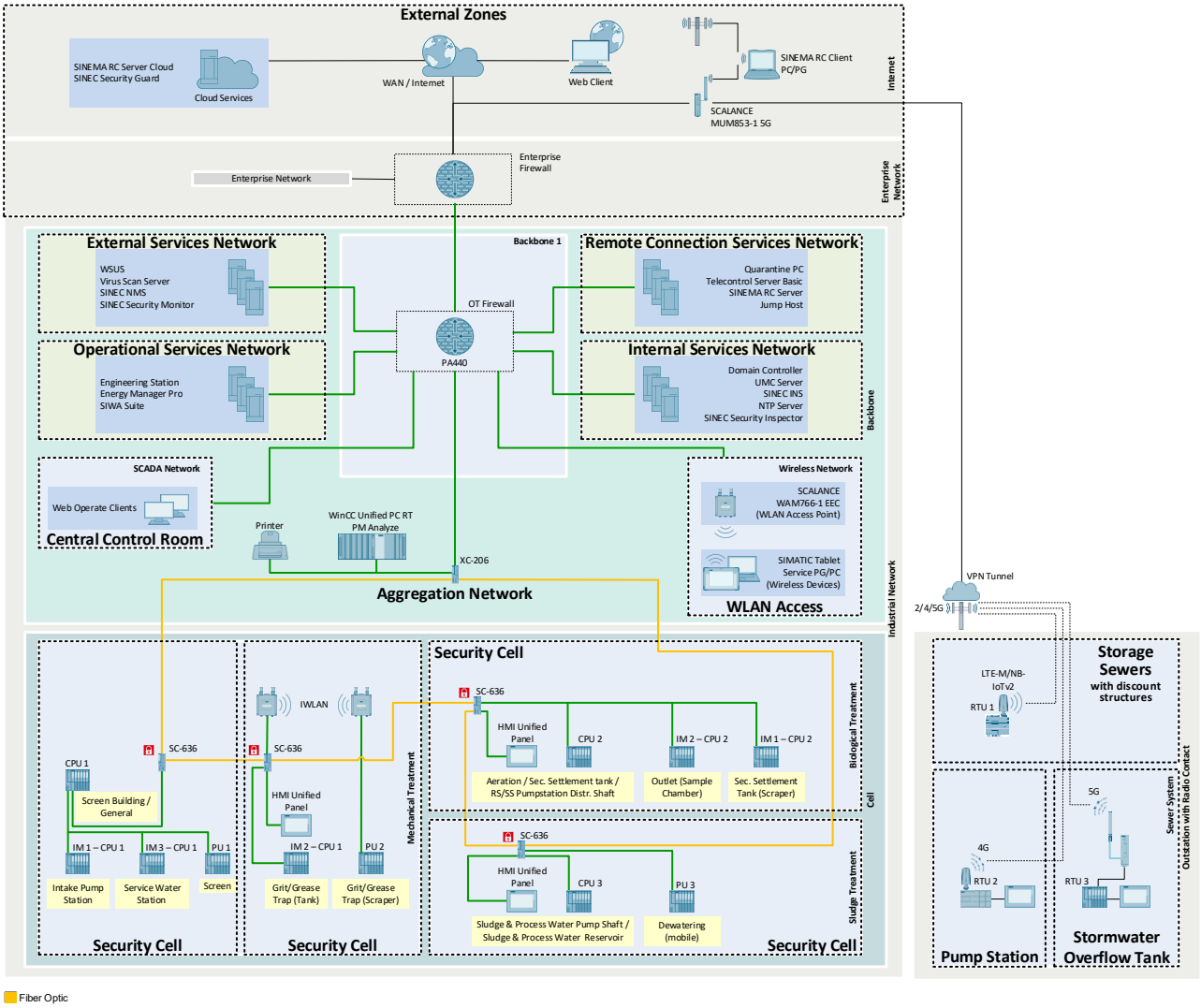

Abbildung 3-3: Zonen für das Musterkonzept einer Abwasserbehandlungsanlage

3.3.1. Räume und Schränke

Zentrale Leitwarte

In der zentralen Leitwarte befinden sich die Workstations der Bediener (Web Operate Clients) zur Überwachung, Steuerung und Erfassung von Daten aus dem Betrieb der Abwasserbehandlungsanlage. Der Zutritt zur zentralen Leitwarte ist auf autorisiertes Personal beschränkt.

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 (Tastatur, Video und Maus). Dieser fungiert als lokale Konsole für Server, die keinen KVM-Bildschirm in der zentralen Leitwarte haben. Der Zutritt zum Serverraum ist auf autorisiertes Personal beschränkt.

Engineering-Raum

Im Engineering-Raum befindet sich die TIA Portal-Engineering-Station, die zur Verwaltung und Konfiguration der WinCC Unified- und SIMATIC-Automatisierungsgeräte dient. Der Zutritt zum Engineering-Raum ist auf autorisiertes Personal beschränkt.

Field PGs können auch zur Verwaltung und Inbetriebnahme von Automatisierungsgeräten über die mit der OT-Firewall verbundene WLAN-Zugangszone verwendet werden. Siehe hierzu Abschnitt 3.3.2 – WLAN-Zugang.

Steuerschränke

Steuerschränke enthalten die ET 200SP Distributed Controllers, die sich an verschiedenen physischen Standorten im zentralen Anlagenbereich befinden. Diese Schränke sind über das Aggregationsnetzwerk miteinander verbunden.

3.3.2. Netzwerke

„Operative Dienste"-Netzwerk

Das „Operative Dienste"-Netzwerk umfasst alle Systeme, die für den Betrieb, die Überwachung oder die Verwaltung des Produktionsprozesses erforderlich sind.

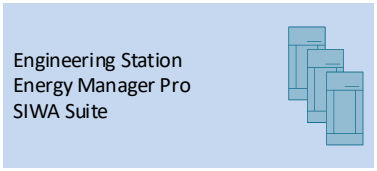

Abbildung 3-4: „Operative Dienste"-Netzwerk des Musterkonzepts

„Interne Dienste"-Netzwerk

Das „Interne Dienste"-Netzwerk beinhaltet alle sekundären Systeme, die im IACS-Netzwerk erforderlich sind. Diese System stellen wichtige Dienste bereit, wie Active Directory, NTP-Server etc. Die Systeme in diesem Perimeternetzwerk benötigen keine direkte Verbindung zu Nicht-OT bzw. externen Netzwerken.

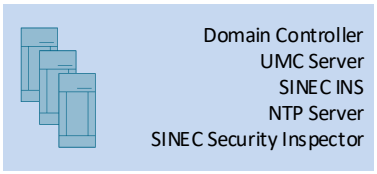

Abbildung 3-5: „Interne Dienste"-Netzwerk des Musterkonzepts

„Externe Dienste"-Netzwerk

Das „Externe Dienste"-Netzwerk ist vergleichbar mit dem „Interne Dienste"-Netzwerk. Es unterstützt alle sekundären Systeme, die eine Verbindung zu Nicht-OT- bzw. externen Netzwerken benötigen:

- Windows Update Server (WSUS) – Ruft die neuesten Windows-Updates ab.
- Virenscan-Server – Lädt die neuesten Virenerkennungsmuster herunter.
- SINEC NMS – Ermöglicht den Zugriff auf den Webserver vom Unternehmensnetzwerk auf die NMS Control. Falls SINEC NMS von überlagerten Netzwerken nicht zugänglich sein soll, sollte NMS Control im „Interne Dienste"-Netzwerk platziert werden.
- SINEC Security Monitor – Ruft Aktualisierungen für die SINEC Security Monitor Intelligence Database ab.

Abbildung 3-6: „Externe Dienste“-Netzwerk des Musterkonzepts

„Remote-Verbindungsdienste“-Netzwerk

„Remote-Verbindungsdienste“ ist das Netzwerk mit der höchsten Kritikalität betreffend ein mögliches Eindringen, denn hier befinden sich der Server für Remote-Verbindungen, die Jump Hosts für jeden Lieferanten und die Quarantänestation. Um die Anbindung und Verwaltung der Remote-Stationen zu erleichtern, wird in diesem Netzwerk TeleControl Server Basic eingesetzt.

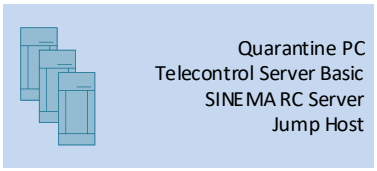

Abbildung 3-7: „Remote-Verbindungsdienste“-Netzwerk des Musterkonzepts

WLAN-Zugang

Die WLAN-Zugangszone ist mit der OT-Firewall verbunden und bietet beschränkten Zugang zu Geräten in der Abwasserbehandlungsanlage des Musterkonzepts – normalerweise begrenzt auf HTTPS-Zugang zum Webserver 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 SIMATIC-Tablets oder Service Field PGs/PCs zur Verfügung. Verbindungen zu den WLAN-Zugangspunkten müssen verschlüsselt werden, weshalb die WLAN-Clients den jeweiligen WLAN-Schlüssel „kennen“ müssen, oder sie müssen über das Protokoll 802.1x authentifiziert werden (RADIUS, Beschränkung des Netzwerkzugangs).

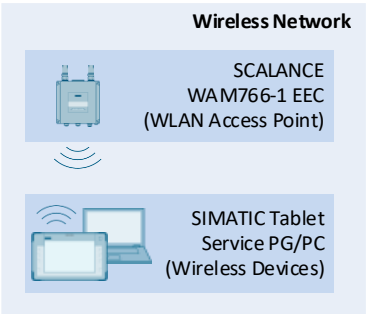

Abbildung 3-8: Drahtlosnetzwerk des Musterkonzepts

Aggregationsnetzwerk

Das Aggregationsnetzwerk führt alle darunterliegenden Fertigungsmaschinen-Netzwerke zusammen und verbindet die Sicherheitszellen mit der WinCC Unified PC RT. Diese Schicht ermöglicht sowohl vertikale Kommunikation (Maschine zum Rechenzentrum) wie auch horizontale Kommunikation (Maschine zu Maschine). Sie ist in einer Ringtopologie konfiguriert, wodurch Redundanz und eine hohe Verfügbarkeit gewährleistet sind.

Jede Automatisierungszelle ist durch eine industrielle Firewall vom darüberliegenden Aggregationsnetzwerk getrennt. Die Automatisierungsgeräte innerhalb der Zellen steuern die folgenden Hauptprozessbereiche.

- Mechanische Behandlung
- Biologische Behandlung
- Schlammbehandlung

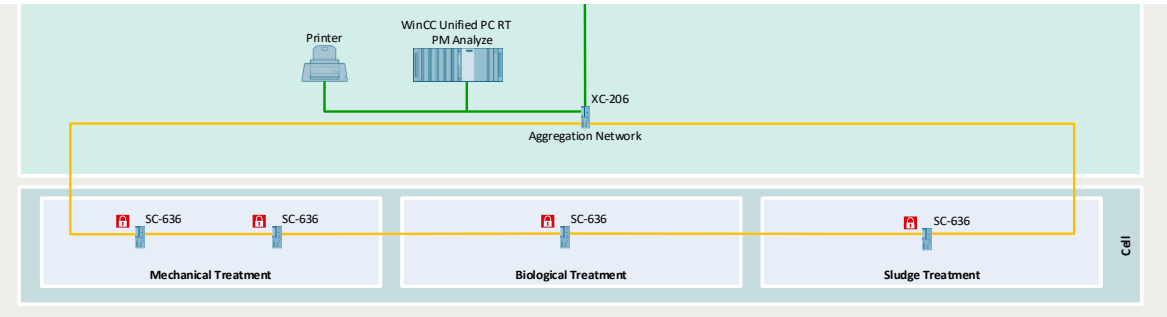

Abbildung 3-9: Aggregationsnetzwerk des Musterkonzepts

Externe Zonen

Das Musterkonzept der Abwasserbehandlungsanlage verfügt über zwei externe Zonen: Unternehmensnetzwerk und Internet.

Diese Zonen stellen konventionell Aktualisierungsdienste für die im „Externe Dienste"-Netzwerk laufenden Anwendungen bereit. Die notwendigen Netzwerkverbindungen für diese Dienste werden konventionsgemäß vom „Externe Dienste"-Netzwerk als Initiator (Quelle) zum jeweiligen Dienstanbieter (Ziel) im Unternehmensnetzwerk hergestellt. Einige wenige Dienste wie Web oder Remote Desktop Clients werden vom Unternehmensnetzwerk als Initiator zum „Externe Dienste"-Netzwerk hergestellt, z. B. Aktualisierungen für Windows oder Virenerkennungsmuster.

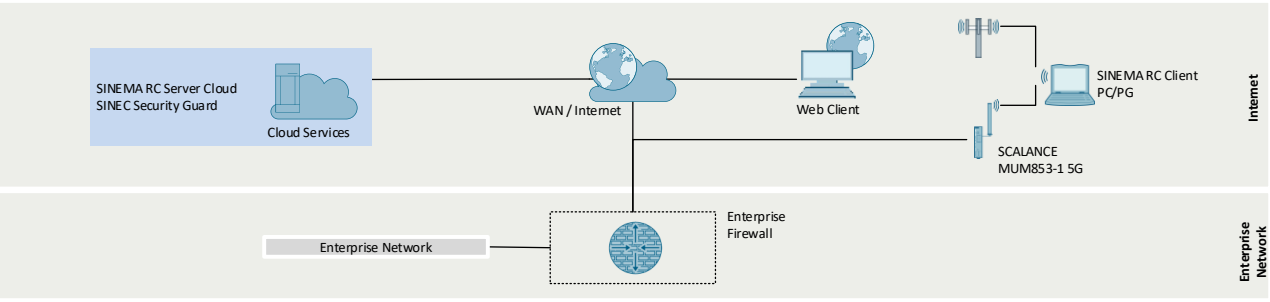

Abbildung 3-10: Externe Zonen

3.3.3. Remote-Stationen

Das Musterkonzept der Abwasserbehandlungsanlage verfügt über drei Remote-Stationen: die Stauraumkanäle mit Entlastungsstruktur, die externe Pumpstation und das Regenwasserbecken.

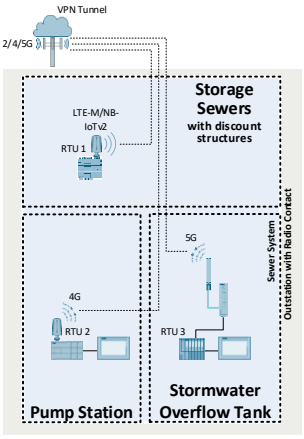

Abbildung 3-11: Remote-Stationen

Regenwasserbecken

Die Remote-Station dient bei Starkregenereignissen zur Aufnahme des hohen Abwasseranfalls und zum Verringern der Belastung des Zulaufs der Abwasserbehandlungsanlage, indem sie das überschüssige Wasser direkt zum Ablauf leitet.

Um eine sichere und gekapselte Kommunikation zwischen Remote-Station und zentralem Anlagenbereich zu gewährleisten, werden der Router SCALANCE MUM 853-1 und der CP 1542SP-1 IRC verwendet. Härtungsmaßnahmen und Projektierungsrichtlinien siehe Abschnitt 6.3 und 6.5.

- \31\ – Produktkatalog: CP 1542SP-1 IRC
- \33\ – Produktkatalog: SCALANCE MUM853-1

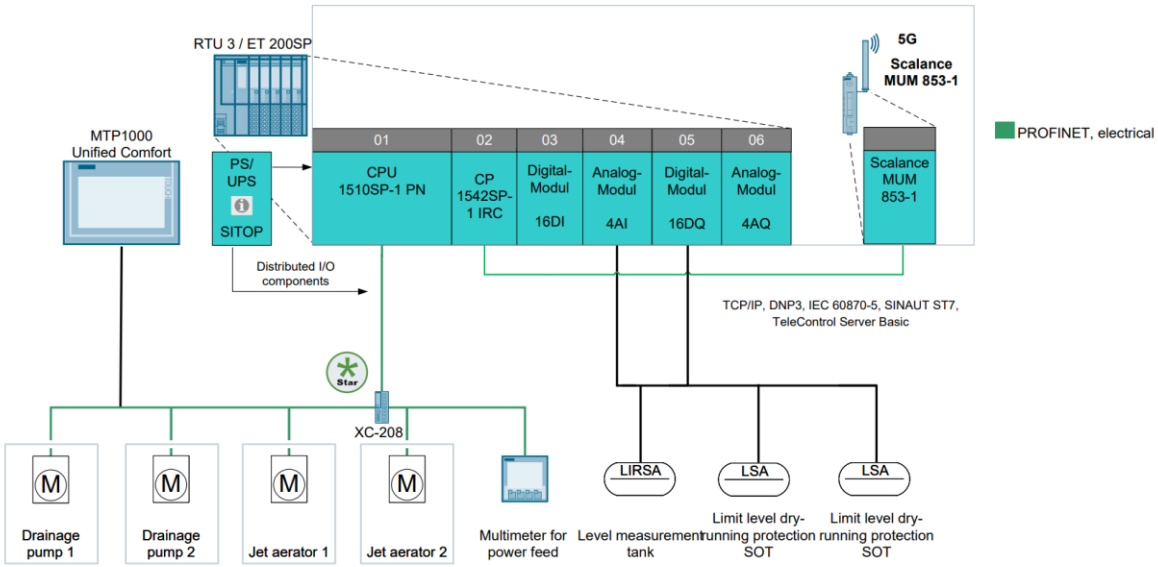

Abbildung 3-12: Komponenten und Netzwerkarchitektur des Regenwasserbeckens

Externe Pumpstation

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

Um die Kapselung der Kommunikation zwischen Remote-Station und zentralem Anagenbereich zu gewährleisten, wird der CP 1243-7 LTE-EU mit TC-SRC (TeleControl-Kommunikation über SINEMA Remote Connect) verwendet. Härtungsmaßnahmen siehe Abschnitt 6.6

- \29\ – Produktkatalog: CP 1243-7 LTE EU

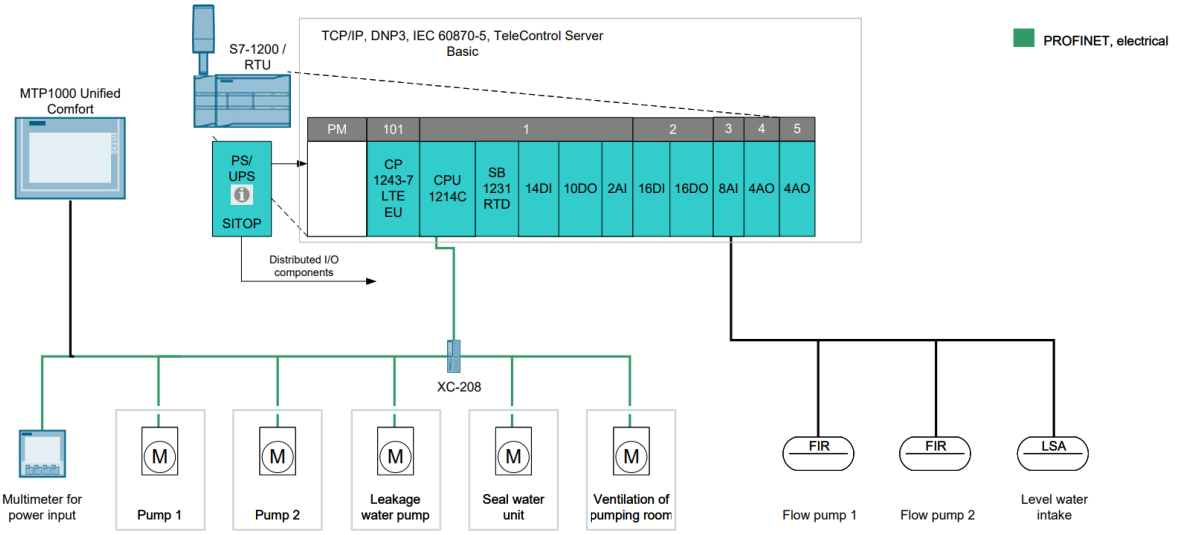

Abbildung 3-13: Komponenten und Netzwerkarchitektur der externen Pumpstation

Stauraumkanäle mit Entlastungsstruktur

Die Remote-Station dient zur Steuerung und Regulierung des Abwasserflusses im Entsorgungsbereich. Das Abwasser wird gesammelt, gepuffert und in der Kanalisation zwischengespeichert, wo ein Drosselmechanismus – die Entlastungsstruktur – die Abflussrate in die Behandlungsanlage steuert.

Um eine sichere und gekapselte Kommunikation zwischen Remote-Station und zentralem Anlagenbereich zu gewährleisten, wird die SIMATIC RTU 3051C verwendet. Härtungsmaßnahmen und Projektierungsrichtlinien siehe Abschnitt 6.7.

- \27\ – Produktkatalog: SIMATIC RTU 3051C

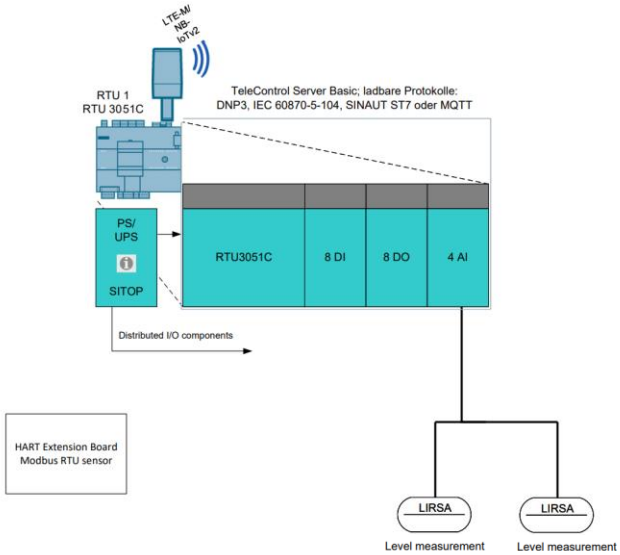

Abbildung 3-14: Komponenten und Netzwerkarchitektur der Stauraumkanäle mit Entlastungsstruktur

3.4. Datenaustausch zwischen Zonen

Eine allgemeine Übersicht über den Datenverkehr und die Verbindungen zwischen den Servern und Anwendungen in den jeweiligen Zonen ist in Abbildung 3-15 dargestellt.

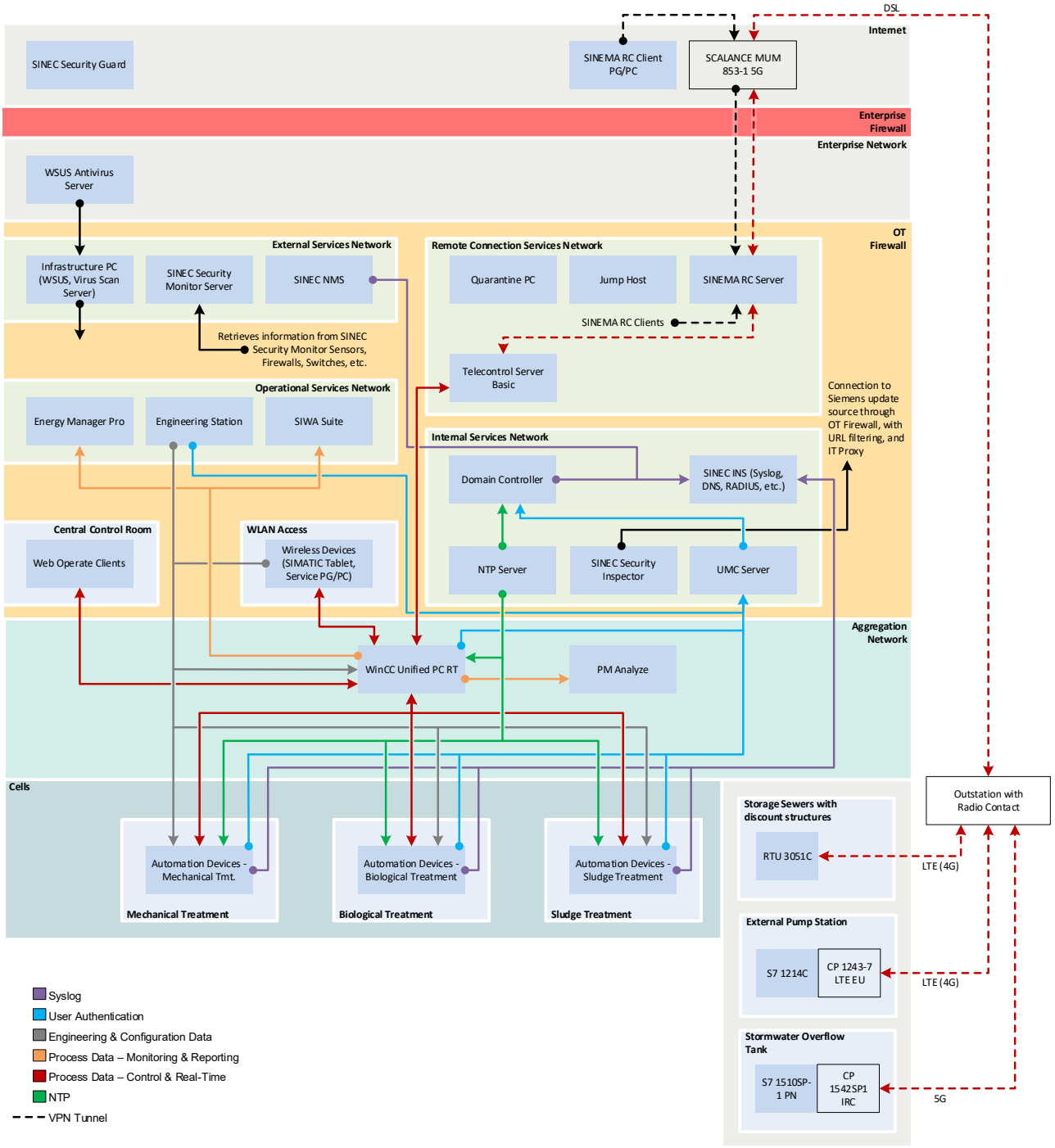

Abbildung 3-15: Datenaustausch im Musterkonzept einer Abwasserbehandlungsanlage

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 in diesem Abschnitt 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.

Tabelle 4-1: Schutzziele

Schutzziele	Beschreibung der Schutzziele	Zugehörige Hauptkomponenten / Assets
Vertraulichkeit	Sicherstellen, dass sensible Informationen vor unbefugtem Zugriff oder unbefugter Offenlegung geschützt bleiben. • Benutzerpasswörter • Informationen über Kunden-Assets • Prozessdaten, z. B. Messungen zur Wirksamkeit der Reinigungsprozesse • Projekt-Engineering-Daten, z. B. WinCC Unified-Skripte, SPS-Anwenderprogramm etc.	• Domain Controller, UMC-Server • Engineering-Station • SCADA – WinCC Unified PC RT • SPS und Unified Comfort Panels • Firewalls und Switches • SINEC NMS, SINEC INS
Integrität	Gewährleisten der Richtigkeit, Konsistenz und Zuverlässigkeit von Daten und Prozessen, Verhindern von unbefugten Änderungen, Beschädigungen oder Manipulationen. • Historian-Daten • Sicherheitsprotokolle • Messdaten, z. B. richtige Chemikaliendosierung • Projektkonfiguration und Engineering-Daten	• Engineering-Station • SCADA – WinCC Unified PC RT • SPS und Unified Comfort Panels (Audit Trail-System) • Firewalls und Switches • SINEC NMS, SINEC INS (Syslog-Server) • PM ANALYZE
Verfügbarkeit	Sicherstellen des ununterbrochenen Zugriffs auf kritische Systeme, Daten und Ressourcen und Minimieren von Ausfallzeiten und Unterbrechungen im Fertigungsbetrieb.	• SCADA – WinCC Unified PC RT und Web Operate Clients • SPS und Unified Comfort Panels • Firewalls und Switches

Schutzziele für Zonen

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

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

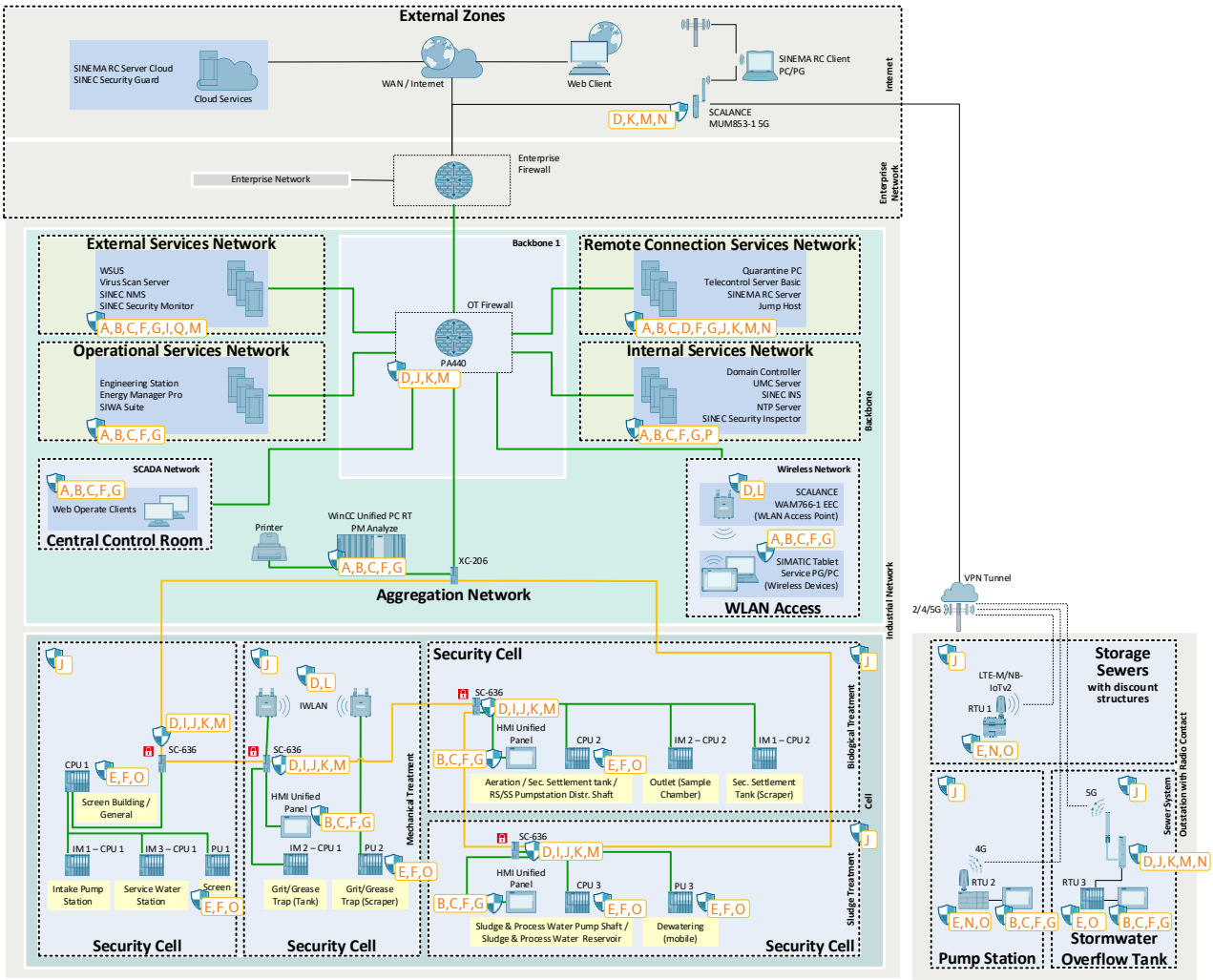

Abbildung 4-1: Schutzziele für Zonen

Bedrohungs- und Risikoanalyse

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 in diesem Musterkonzept durchgeführte generische Bedrohungs- und Risikoanalyse (Abschnitt 4.1 bis 4.5) bietet Hinweise auf mögliche Bedrohungen und Risiken, die für Abwasserbehandlungsanlagen relevant sind. Die Bedrohungs-

und Risikoanalyse muss jedoch für jede Anlage individuell durchgeführt werden, um sicherzustellen, dass standortspezifische Bedingungen, Konfigurationen und betriebliche Zusammenhänge berücksichtigt werden.

4.1. Physischer Zugang

Perimetersicherheit

Tabelle 4-2: Bedrohungen, Risiken und Gegenmaßnahmen in Bezug auf die Perimetersicherheit

Bedrohung und Risiko	Gegenmaßnahmen
Zugang zur Anlage zur Sabotage von Arbeitsvorgängen/Prozessen	Umzäunung und Barrieren, Überwachungskameras und Beleuchtung, Sicherheitspersonal
Physische Störung/Manipulation von Remote-Stationen	Umzäunung, Überwachungskameras und Beleuchtung
Beschädigung/Manipulation kritischer Infrastrukturen, z. B. Notstromversorgungssysteme	Manipulationssichere Siegel zur Erkennung unbefugter Zugangsversuche

Gesicherte Geräte, Systeme und Gebäude

Tabelle 4-3: Bedrohungen, Risiken und Gegenmaßnahmen in Bezug auf gesicherte Teile und Gebäude

Bedrohung und Risiko	Gegenmaßnahmen
Zugang zum zentralen Standort/zu den Gebäuden	Zutrittskontrolle, 2-Faktor-Authentifizierung für den Zugang
Physischer Zugriff zum Diebstahl von Daten	Überwachung von 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

Freiliegende Geräte, Systeme, Gebäude und Remote-Stationen (Ventile, Behälter, Pumpen, Zählerstationen usw.)

Tabelle 4-4: Bedrohungen, Risiken und Gegenmaßnahmen in Bezug auf freiliegende Geräte, Systeme, Gebäude und Remote-Stationen

Bedrohung und Risiko	Gegenmaßnahmen
Einfacher Zugang zu weniger gesicherten Systemen und Netzwerken	System- und Kommunikationsüberwachung in SCADA
Zerstörung/Deaktivierung von Systemen in Remote-Stationen	Redundante externe Systeme, z. B. Brunnen, Pumpen etc.
Änderung/Manipulieren der von diesen Stationen gesendeten und empfangenen Daten	Sichere Kommunikation, Zugriffskontrolle, Minimierung der Menge der geteilten Informationen auf das erforderliche Minimum

Netzwerk und Windows-PCs

Tabelle 4-5: Bedrohungen, Risiken und Gegenmaßnahmen in Bezug auf den physischen Zugriff auf Netzwerke und Windows-PCs

Bedrohung und Risiko	Gegenmaßnahmen
Zugriff auf das OT-Netzwerk	Überwachung von Netzwerkkomponenten, 802.1x, Industrial Anomaly Detection
Ungepatchte Sicherheitslücken in Windows-PCs	Updates und/oder Application Whitelisting

4.2. Stromversorgungssystem

Tabelle 4-6: Bedrohungen, Risiken und Gegenmaßnahmen in Bezug auf die Stromversorgungssysteme

Bedrohung und Risiko	Gegenmaßnahmen
Ausfall der Stromversorgung aus dem öffentlichen Netz	Echtzeitüberwachung, Backup-System
Fehlfunktion der internen USV	Überwachung und Instandhaltung der Backup-Systeme

4.3. WinCC Unified PC RT und Panels

Für die WinCC Unified-Geräte werden zwei getrennte Risikoanalysen durchgeführt – eine für die Engineering- und Inbetriebnahmephase und eine für die Betriebsphase.

Bedrohungen und Risiken während der Engineering- und Inbetriebnahmephase

Tabelle 4-7: Bedrohungen, Risiken und Gegenmaßnahmen in Bezug auf die Engineering- und Inbetriebnahmephase von WinCC Unified-Geräten

Bedrohung und Risiko	Gegenmaßnahmen
Unbefugter Zugriff auf das TIA Portal-Projekt	Schutz des TIA Portal-Projekts mit einem Projektadministrator
Abfangen und Manipulation von Projektübertragungen während der Inbetriebnahme	Aktivieren der verschlüsselten Übertragung auf Unified Comfort Panels sowie des sicheren Downloads in der WinCC Unified PC RT
Diebstahl, Verlust oder Entfernung von externen Speichergeräten, z. B. SD-Karten, USB-Laufwerken usw., mit sensiblen Daten von Unified Comfort Panels	Aufbewahren externer Speicher an sicheren Orten, Schutz der Panel-Schnittstellen vor unbefugtem Zugriff, z. B. abschließbare Schaltschränke, regelmäßiger Export archivierter Daten an einen zugriffsgeschützten Ort
Diebstahl oder unbefugter Zugriff auf sensible Daten aus WinCC Unified PC Runtime	• Dateibasierte Archivierung – SQLite: Verwendung zugriffsgeschützten Speicher, regelmäßiger Export von Daten an einen sicheren Ort • Datenbankarchivierung – Microsoft SQL: Schutz von Datenbanken mithilfe von Windows-Gruppen: „Simatic HMI" (Lesen/Schreiben) und „Simatic HMI Viewer" (schreibgeschützt)

Bedrohungen und Risiken im Betrieb

Tabelle 4-8: Bedrohungen, Risiken und Gegenmaßnahmen in Bezug auf die Betriebsphase von WinCC Unified-Geräten

Bedrohung und Risiko	Gegenmaßnahmen
Beabsichtigte oder unbeabsichtigte Prozessstörungen oder Schäden an Anlagen durch Bediener	Beschränkung des Betriebs auf autorisiertes Personal. Konfiguration von Zugriffsebenen zum Schutz von Geräten, Bildschirmen und Benutzeroberflächenelementen. Zuweisen der minimal erforderlichen Zugriffsrechte an Benutzer und Rollen.
Unbefugter Zugriff auf Tags in der Steuerung	Aktivierung der SPS-Zugangskontrolle, Konfiguration von Zugangspasswörtern für HMI-Verbindungen
Unbefugter Zugriff auf Windows-Systemfunktionen auf dem IPC mit WinCC Unified PC RT	Verwendung des Windows-Kioskmodus
Diebstahl oder Manipulation sensibler Daten und Übertragung von Schadprogrammen über SD-/USB-Anschlüsse	Deaktivierung unnötiger Schnittstellen, Verwendung physischer Schutzmaßnahmen, z. B. USB-Port-Schlösser, Installation von Schalttafeln in abschließbaren Schränken, Überwachung des Zugangs zur zentralen Leitwarte

Bedrohung und Risiko	Gegenmaßnahmen
Diebstahl oder Manipulation sensibler Daten und Übertragung von Schadprogrammen über Netzwerkschnittstellen	Deaktivierung ungenutzter Netzwerkschnittstellen, Implementierung physischer Schutzmaßnahmen
Abfangen oder Manipulation von Daten, die über das Netzwerk übertragen werden, und Vortäuschung der Identität von Kommunikationspartnern	Verwendung verschlüsselter, zertifikatbasierter Kommunikationsprotokolle für Server/Client-Kommunikation, Runtime-Kollaboration und OPC UA-Verbindungen

4.4. Firewalls

Tabelle 4-9: Bedrohungen, Risiken und Gegenmaßnahmen in Bezug auf die Netzwerk- und Firewall-Konfiguration

Bedrohung und Risiko	Gegenmaßnahmen
Netzwerk oder Geräte mit Kontakt zum Internet, höchste Sichtbarkeit selbst für Scriptkiddies	Sichere Konfiguration, Patching von Sicherheitslücken
Eindringen in das Netzwerk	Dauerhafte zentrale Überwachung von Firewall-Protokolldaten/Anomalieerkennung

4.5. Interne und organisatorische Maßnahmen

Tabelle 4-10: Bedrohungen, Risiken und Gegenmaßnahmen in Bezug auf interne und organisatorische Maßnahmen

Bedrohung und Risiko	Gegenmaßnahmen
Internes Personal mit Zugang zu Infrastruktur-PCs, interne Manipulation möglich, entweder absichtlich oder unabsichtlich	Mitarbeiterschulung, organisatorische Verfahren
Internes Personal mit Zugang zu Betriebs-PCs, interne Manipulation möglich, entweder absichtlich oder unabsichtlich	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 Software-/Betriebssystem-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 der 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 von Automatisierungs- und Leitsystemen und Netzwerken ist Netzwerksicherheit. Die Netzwerke von Automatisierungs- und Leitsystemen müssen vor unbefugtem Zugriff geschützt werden. Darüber hinaus müssen die Schnittstellen zu anderen Netzwerken, z. B. zum Unternehmensnetzwerk oder zum Internet, 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 Gemäß SR 5.1 RE 1 – Physische Netzwerksegmentierung SR 5.1 RE 2 Unabhängigkeit von nicht-automatisierungstechnischen Netzwerken

Netzwerksegmentierung ist der Schlüssel, um Sicherheitsbedrohungen zu minimieren und die Systemverfügbarkeit zu maximieren. Dabei soll das Netzwerk in unterschiedliche Segmente unterteilt werden, um kritische Systeme von nicht kritischen Teilen zu isolieren. Firewalls sind die gegenwärtige State-of-the-Art-Technik für die Netzwerksegmentierung.

Um ein OT-Netzwerk zu segmentieren, müssen die folgenden Kriterien berücksichtigt werden.

- Risiken und Kritikalität: Systeme, die als kritisch identifiziert wurden (auf Basis der Risikoanalyse aus der Planungsphase), müssen von Systemen mit geringerer Kritikalität getrennt werden, um die Verfügbarkeit dieser kritischen Systeme zu erhöhen.
- Automatisierungs-Echtzeitkommunikation: Die zwischen Steuerung und Gerät ausgetauschten Kommunikationsprotokolle unterliegen möglicherweise Echtzeitanforderungen. Deswegen müssen sich Geräte, die zur selben Automatisierungsanwendung gehören, im selben Netzwerksegment befinden, um die erforderliche deterministische Kommunikation bereitzustellen.

Basierend auf diesen Anforderungen und als Teil der Implementierung des Defense-in-Depth-Konzepts wird das Automatisierungssystem in verschiedene Sicherheitszonen segmentiert, wie in Abschnitt 3.3 beschrieben. Diese Zonen sind durch die OT-Firewall und die SCALANCE SC-636-Firewalls in den einzelnen Sicherheitszellen strategisch so aufgeteilt, dass Systemkomponenten mit ähnlichen Kommunikations- und Schutzbedürfnissen in jeder Zone zusammengefasst sind. Die Grenzen zwischen diesen Zonen werden als Vertrauensgrenzen bezeichnet, und die Kommunikation zwischen diesen Zonen muss überwacht und gesteuert werden, wie in Abschnitt 5.1.2 beschrieben.

HINWEIS

Zusätzlich zur physischen Separation über Firewalls können Netzwerke auch logisch durch in Managed Switches konfigurierte VLANs segmentiert werden. Diese logische Segmentierung verhindert die direkte Kommunikation zwischen VLANs, sodass der gesamte Datenverkehr zwischen den Segmenten durch eine Firewall geleitet werden muss, die Kommunikationseinschränkungen gemäß den konfigurierten Firewall-Regeln durchsetzt.

Dennoch kann die VLAN-basierte Segmentierung allein nur Security Level 1 gemäß der IEC 62443-3-3 erfüllen, während die physische Segmentierung mittels Firewalls Security Level 3 erreichen kann. Dies ergibt sich aus Folgendem:

- Netzwerküberlastungen oder Denial-of-Service-Angriffe (DoS) in einem VLAN können sich auf andere VLANs desselben physischen Segments (desselben physischen Switches) auswirken.
- VLANs sind leichter zu umgehen – beispielsweise führt ein Reset eines Switches in der Regel dazu, dass der Switch den gesamten Datenverkehr zulässt, während ein Reset einer Firewall dazu führt, dass die Firewall standardmäßig den gesamten Datenverkehr verweigert.

Um Security Level 4 zu erreichen, ist eine vollständige Isolierung kritischer Netzwerksegmente erforderlich.

Die als Teil dieses Musterkonzepts realisierte Netzwerksegmentierung entspricht den Empfehlungen in der sicheren Referenzarchitektur:

- \35\ – Sichere Referenzarchitektur, Abschnitt 4.1 (Netzwerksegmentierung)

5.1.2. Schutz der Zonengrenzen

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

Sämtliche Kommunikation zwischen den Sicherheitszonen muss genau überwacht und gesteuert werden. Um die erforderlichen Kommunikationsregeln durchzusetzen und einen sicheren Austausch zwischen verschiedenen Zonen zu gewährleisten, werden Firewalls mit VPN-Funktionalität als wesentliche Sicherheitsmaßnahme eingesetzt. Innerhalb des zentralen Anlagennetzwerks kann nur zugelassener Datenverkehr Zonengrenzen passieren – entsprechend den Firewall-Richtlinien, die strikt das Prinzip „Grundsätzlich ablehnen, Ausnahmen zulassen" verfolgen.

Zum Schutz der Grenze des zentralen Anlagennetzwerks bieten die Perimeternetzwerke – demilitarisierte Zone (DMZ) – zusätzliche Kontrollmechanismen auf Anwendungsebene. Die Kommunikation aus externen Zonen wird an die DMZ weitergeleitet, wodurch ein direkter Zugang zu internen Komponenten, z. B. der direkte Engineering-Zugang, verhindert wird. Stattdessen werden die erforderlichen Interaktionen innerhalb der DMZ über Proxys oder Hosts realisiert. 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 mit den Remote-Stationen wird durch SCALANCE S Firewall Appliances sowie die Unternehmens- und OT-Firewall abgesichert. Der Datenaustausch zwischen diesen Remote-Stationen und WinCC Unified PC RT im Aggregationsnetzwerk wird durch die OT-Firewall geleitet, sodass ein einziger, kontrollierter Verbindungspunkt zwischen dem OT-Netzwerk und den externen Netzwerken besteht. Diese über VPN-Tunnel gesicherte Verbindung wird über den SINEMA RC-Server und das in der DMZ gehosteten TeleControl Server Basic hergestellt, wie in Abschnitt 5.2.4 beschrieben.

Die Industrial WLAN (IWLAN) Access Area ermöglicht eine sichere drahtlose Konnektivität über SCALANCE W-WLAN-Zugangspunkte. Der drahtlose Zugriff wird durch die drahtlosen Sicherheitsfunktionen und die sichere Konfiguration der Zugangspunkte geschützt, in Verbindung mit der zusätzlichen Einschränkung, dass nur bestimmten drahtlosen Clients Zugriff gewährt wird. Darüber hinaus unterliegt jeder drahtlose Zugriff den Beschränkungen, die durch die Grenzschutzeinrichtungen zwischen den verschiedenen Anlagenbereichen auferlegt werden.

Neben den netzwerkbasierten Firewalls werden auch die PC-basierten Host-Firewalls genutzt, um eine zusätzliche Schutzschicht zu bieten.

Diese Grenzschutzmaßnahmen werden durch anpassungsfähige Sicherheitsprotokollierungs- und Überwachungsmechanismen weiter verbessert (siehe Abschnitt 5.6).

5.1.3. Netzwerkzugriffsschutz

IEC 62443-3-3	SR 2.2 Nutzungskontrolle von Funkverbindungen SR 2.2 RE 1 Nicht genehmigte drahtlose Geräte erkennen und anzeigen

Zwar spielen Firewalls eine wichtige Rolle beim Schutz von Netzwerkzonen an den Außengrenzen, ebenso wichtig ist es jedoch, geeignete Maßnahmen zur Einschränkung des Zugriffs auf das lokale Netzwerk zu implementieren. Dies trägt dazu bei, das Risiko lokaler Angriffe auf die Netzwerke innerhalb einzelner sicherer Anlagenzonen unter Berücksichtigung ihrer jeweiligen Kritikalität und Gefährdungsstufen zu verringern. Im Kontext des Musterkonzepts einer Abwasserbehandlungsanlage werden für eine sichere Konfiguration und einen sicheren Betrieb folgende Maßnahmen empfohlen.

- Mobile Geräte: Alle Zugriffe mit mobilen Geräten, wie z. B. Laptops von Servicetechnikern, sollten einer gründlichen Überprüfung unterzogen werden, um ihre Notwendigkeit und die damit verbundenen möglichen Risiken zu bewerten. Bei Bedarf sollten nur sicher verwaltete und konfigurierte Geräte mit klar definierten Zugriffspfaden und Einschränkungen verwendet werden, die innerhalb der Zugriffsschutzmechanismen der Anlage konfiguriert sind.
- Drahtloser Zugriff: Alle Benutzer, Softwareprozesse oder Geräte, die über drahtlose Kommunikation auf das Netzwerk zugreifen, müssen identifiziert und authentifiziert werden. Eine weithin akzeptierte Sicherheitsmaßnahme beinhaltet die Verwendung moderner Sicherheitsprofile mit robuster Authentifizierung und Verschlüsselungsprotokollen nach dem Standard 802.11 für die Drahtloskommunikation (WLAN-Standard). Dadurch wird sichergestellt, dass der Zugriff authentifiziert und autorisiert wird und Nutzungsbeschränkungen für Drahtlosverbindungen durchgesetzt und überwacht werden.
- Härten: Um das Risiko eines unbefugten Zugriffs auf einen Teil des zentralen Anlagennetzwerks weiter zu minimieren, müssen gängige Maßnahmen wie die Härtung der eingesetzten Netzwerkgeräte und die Deaktivierung aller ungenutzten Ethernet-Anschlüsse und anderer physischer Schnittstellen, wie z. B. USB-Ports, implementiert werden. Die empfohlenen Härtungsmaßnahmen und sicheren Konfigurationseinstellungen werden in Abschnitt 6 beschrieben.

Die als Teil dieses Musterkonzepts realisierten Härtungsmaßnahmen entsprechen den Empfehlungen des „Security Leitfadens für SIMATIC WinCC Unified- and SIMATIC HMI Unified-Bediengeräte“.

- \3\ – „Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices“, Section 4.1.1 (Protect SD and USB ports) und Section 4.1.2 (Disable network interfaces)

5.1.4. Administration der Netzwerkgeräte

Eine sichere Administration und Konfiguration der Netzwerkgeräte ist von höchster Wichtigkeit angesichts der zentralen Rolle dieser Geräte bei der Sicherstellung der Verfügbarkeit der internen und externen Kommunikation einer Anlage sowie der Realisierung und Durchsetzung einer Netzwerksegmentierung.

Alle administrativen Zugriffe auf Netzwerkgeräte (z. B. Router, Switches, Firewalls und WLAN-Zugangspunkte), die im Rahmen des Musterkonzepts eingesetzt werden, geschehen anhand von Kommunikationsprotokollen, die durch neueste kryptographische Verfahren geschützt sind. Dieser Schutz wird entweder durch webbasierte Kommunikation über HTTPS oder SSH erreicht, mit beidseitiger Authentifizierung und starker Verschlüsselung aller ausgetauschten Daten. Veraltete und anfällige Methoden wie HTTP oder Telnet – wenn überhaupt unterstützt – sind standardmäßig deaktiviert, um Sicherheitsrisiken zu minimieren.

Die Verwaltung des menschlichen Benutzerzugriffs auf solche Geräte erfolgt über eine rollenbasierte Zugriffssteuerung, wobei die Zugriffsrechte der Benutzer auf ein Minimum eingeschränkt werden, um den administrativen Zugriff auf autorisiertes Personal zu beschränken. Die Benutzerverwaltung und die Zugriffssteuerung für administrative Zwecke sind über SINEC NMS – das Netzwerkmanagementsystem von Siemens – in Microsoft Active Directory integriert.

Mit SINEC NMS können Netzwerkadministratoren Firmware-Updates zentral auf alle verwalteten SCALANCE-Netzwerkgeräte ausspielen (siehe Abschnitt 6.9.4).

5.1.5. Schutzmaßnahmen gegen Dienstblockade

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

Um Wasser- und Abwasserlösungen vor Angriffen in Form einer Dienstblockade (Denial of Service, DoS) zu schützen, müssen zwei wichtige Aspekte betrachtet werden.

Erstens können DoS-Angriffe auf die Gesamtverfügbarkeit des zentralen Anlagennetzwerks oder einzelner Geräte abzielen, indem diese mit überflüssigem Netzwerkverkehr überflutet werden. Hier erfordert die Automatisierungslösung die Fähigkeit, den Betrieb auch während eines DoS-Ereignisses in einem Notfallmodus fortzusetzen.

Zweitens 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. Soe sollten solche Pakete entweder ignorieren oder in einen definierten Zustand wechseln, um mögliche Schäden zu mindern.

Hauptmaßnahmen zum Schutz gegen DoS-Angriffe in verschiedenen Netzwerken im Musterkonzept:

- OT-Firewall – Der Einsatz der Next-Generation-Firewall von Palo Alto bietet allgemeinen Schutz gegen gewöhnliche DoS-Angriffe auf Netzwerkebene. Härtungsmaßnahmen und Konfigurationen für diese Firewall werden in Abschnitt 6.2.1 beschrieben.
- Die im Musterkonzept eingesetzten SCALANCE-Netzwerkgeräte werden anhand definierter Testverfahren strengen Tests gegen verschiedene DoS- oder DDoS-Angriffe unterzogen.
- Als Teil des umfassenden Konzepts für Industrial Security von Siemens folgt der Entwicklungsprozess für alle Automatisierungsgeräte und -software dem sicheren Entwicklungsprozess gemäß IEC 62443-4-1, der Sicherheitsüberlegungen und regelmäßige Penetrationstests umfasst.

Bewährte Verfahrensweisen zur Abwehr von DoS-Angriffen auf die Next-Generation-Firewall von Palo Alto sind in der offiziellen Dokumentation zu finden.

- \36\ – Palo Alto – DoS and Zone Protection Best Practices

Eine vollständige Liste der zertifizierten Siemens-Geräte ist in folgender Dokumentation zu finden.

- \4\ – Certification and standards „TÜV Süd certification based on IEC 62443“
- \5\ – „IEC 62443-4-1 Secure product development lifecycle“ for Digital Industries (DI)

5.2. Identitäts- und Zugriffsmanagement

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

- Betriebssystemkonten
- Engineering-Konten, z. B. TIA Engineering-Station
- Konten für administrativen Zugriff auf Netzwerkgeräte, z. B. SCALANCE-Geräte, SINEC NMS, SINEC INS etc.
- Bedienerkonten für Anwendungen mit Benutzerschnittstellen, z. B. Web Operate Clients, HMI Unified Comfort Panels, Webschnittstellen etc.
- Benutzerkonten für Automatisierungsgeräte, z. B. ET 200SP Distributed Controller: Online-Anbindung über TIA Portal, Webserver, 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 Windows-basierten Rechner in der DMZ und in den Aggregationsnetzwerken abdeckt, zentral verwaltet werden. Siehe Abschnitt 7.1.

HINWEIS **Ausnahmen für eindeutige Benutzerkonten in OT-Umgebungen**

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 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

Benutzer und Gruppen zur Überwachung und Konfiguration von Netzwerkgeräten können über UMC – die in das Active Directory integriert werden kann – zentral verwaltet oder lokal in SINEC NMS konfiguriert 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 konfiguriert 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

Um einen sicheren Betrieb zu gewährleisten, müssen die Bildschirme der Bediengeräte – WinCC Unified Panels und PC Runtime – vor unbefugtem Zugriff geschützt werden, der zu Prozessstörungen oder Anlagenschäden führen könnte. WinCC Unified-Geräte implementieren eine benutzerbasierte Zugriffskontrolle, bei der jeder Benutzer eindeutig identifiziert und bestimmten Rollen zugewiesen wird.

Wenn eine nicht autorisierte Person versucht, mit einem geschützten WinCC Unified-Gerät oder Bildschirmobjekt zu interagieren, wird ein Anmeldedialogfeld angezeigt, in dem gültige Benutzeranmeldedaten abgefragt werden. Die Benutzerkonfiguration in WinCC Unified wird im Rahmen des TIA Portal-Projekts verwaltet. Die Benutzerverwaltung kann entweder global über UMC oder lokal über die Benutzerverwaltung und Zugriffssteuerung von TIA umgesetzt werden.

Ebenso erfolgt der Zugriff auf SIMATIC-Controller benutzerbasiert. So wird sichergestellt, dass Benutzer, die eine Verbindung herstellen möchten, eindeutig identifiziert und authentifiziert werden. Die Benutzerverwaltung global über UMC (für S7-1500 und ET 200SP Distributed Controller mit FW 4.0 und höher) oder lokal über die Benutzerverwaltung und Zugriffssteuerung von TIA abgewickelt werden. Ausnahmen, die eine gruppenbasierte Authentifizierung erfordern, können über die zugriffsebenenbasierte Kontrolle des Controllers realisiert werden. Diese beruht auf Passwörtern, die verschiedenen Zugriffsebenen zugewiesen sind.

Weitere Informationen zur Zugriffskontrolle auf Automatisierungsgeräte sind in Abschnitt 6.10 zu finden. Die Informationen im Musterkonzept zur Benutzerauthentifizierung stammen aus den unten aufgeführten Gerätehandbüchern.

- \3\ – „Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices“, Section 2.6 (Creating user administration), Section 3.1 (Operation of configured plant screen) und Section 3.4.1 (Enable access protection for the Control Panel)
- \6\ – „SIMATIC S7-1500 Redundantes System S7-1500R/H“, Abschnitt 11.3 (Lokale Benutzerverwaltung) und Abschnitt 11.4 (Zentrale Benutzerverwaltung)
- \7\ – „Anbindung von WinCC Unified an die zentrale Benutzerverwaltung (UMC)“, Abschnitt 2.4 (Konfiguration der WinCC Unified PC-Station) und Abschnitt 2.5 (Konfiguration des Unified Comfort Panel)

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 Passwörtern für die Konten der Windows Domain über den Windows AD Domain Controller. Dies schließt Mechanismen für Wiederstellung und Rücksetzung von Passwörtern ein.

Durch zentralisierte Verwaltung und Integration in den 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. Bei Automatisierungsgeräten kann die Benutzerverwaltung global über UMC (für S7-1500 und ET 200SP Distributed Controller mit FW 4.0 und höher) oder lokal über die Benutzerverwaltung und Zugriffssteuerung von TIA abgewickelt werden.

Benutzerverwaltung & Zugriffssteuerung (UMAC)

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

Die Benutzerverwaltung in diesem Musterkonzept entspricht den Empfehlungen aus folgenden Dokumenten:

- \3\ – „Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices“, Section 2.6 (Creating user administration)
- \18\ – Zentrales Benutzermanagement mit der „User Management Component (UMC)“
- \54\ – „Benutzer und Rollen projektieren (RT Unified)“

5.2.3. Kontenverwaltung und Projektierung von Zugriffsrechten und Privilegien

Die Handhabung der Kontenverwaltung (Benutzer und Gruppen) findet über das Active Directory statt. Es werden Zugänge mit den wenigsten Berechtigungen eingerichtet, 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 oder Geräten verwendet wurden, müssen entfernt werden.

Für die zentrale Benutzerauthentifizierung für die Software-, Netzwerk- und Automatisierungsgeräte von Siemens wird UMC eingesetzt. UMC unterstützt jedoch keine Benutzerautorisierung, d. h. die Zuweisung und Verwaltung von Benutzerzugriffsrechten und -privilegien. Daher müssen die Zugriffsrechte innerhalb jeder Softwareanwendung (SINEC NMS, TIA Portal), SCALANCE-Routern und Switches, WinCC Unified-Systemen und Automatisierungsgeräten lokal konfiguriert werden. Systemadministratoren definieren diese Zugriffsrechte direkt in den Softwareanwendungen oder innerhalb von TIA Portal-Projekten, die auf der Engineering-Station ausgeführt werden, von wo aus sie während der Inbetriebnahme auf die Automatisierungsgeräte heruntergeladen werden.

Für die WinCC Unified PC RT und Web Operate Clients kann mit dem Windows-Kioskmodus zusätzliche Sicherheit erreicht werden. Dieser Modus beschränkt Benutzer auf eine einzige Anwendung – beispielsweise Microsoft Edge für den Zugriff auf das SCADA-System – und verhindert so den Zugriff auf die Windows-Umgebung, Systemeinstellungen und andere Anwendungen.

Die Zugriffsrechte und Privilegien in diesem Musterkonzept entsprechen den Empfehlungen aus folgenden Dokumenten:

- \3\ – „Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices“, Section 3.5 (SIMATIC WinCC Unified PC RT – Windows Kiosk mode)

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

Da die Lösung im Musterkonzept durch Firewalls (Unternehmens- und OT-Firewall) und eine DMZ geschützt wird, besteht keine Zugriffsmöglichkeit für Benutzer aus externen Netzwerken, die standardmäßig als nicht vertrauenswürdig eingestuft sind. Benutzer, die eine Remote-Verbindung herstellen, können nur auf Rechner innerhalb der DMZ und des Aggregationsnetzwerks zugreifen, die speziell projektiert und geschützt sind, um weiteren Zugriff auf Anwendungsebene zu autorisieren.

Fernzugriff

Im Musterkonzept der Abwasserbehandlungsanlage wird der sichere Fernzugriff durch SINEMA Remote Connect realisiert, wobei der SINEMA RC-Server im „Remote-Verbindungsdienste“-Netzwerk installiert ist. In Kombination mit einer Jump Host-Lösung wird so ein hochsicherer Fernzugriff ermöglicht, sodass autorisierte Benutzer eingeschränkten Zugriff auf die Anlage haben.

Im Szenario Fernzugriff melden sich die Benutzer zunächst beim SINEMA RC-Server an, um eine sichere VPN-Verbindung herzustellen, über die sie unsichere Netzwerke wie das Internet passieren können. Diese VPN-Verbindung wird dann dazu genutzt, eine RDP-Verbindung zum Jump Host in der DMZ aufzubauen. Von dort aus können autorisierte Benutzer über die OT-Firewall eine Verbindung zu anderen Systemen wie der Engineering-Station herstellen. Dabei ist anzumerken, dass die Engineering-Station vor Gewährung des Zugriffs auf Schadsoftware und unbefugte Dateiübertragungen überwacht wird.

TeleControl Basic

Im Rahmen der TeleControl-Kommunikation mit den Remote Terminal Units arbeiten SINEMA Remote Connect und TeleControl Server Basic zusammen, um sichere VPN-Verbindungen zwischen der zentralen Anlage und den Remote-Stationen herzustellen.

Sobald die VPN-Tunnel eingerichtet sind, kann TeleControl Server Basic (im „Remote-Verbindungsdienste“-Netzwerk der Anlage) Prozesswerte, Alarme und Steuerbefehle über TeleControl-Protokolle wie IEC 60870-5-104 oder DNP3 sicher mit den Remote-Stationen austauschen.

Der SINEMA RC-Server verwaltet diese Verbindungen zentral und setzt Zugriffskontrollrichtlinien durch, um sicherzustellen, dass nur autorisierte Geräte miteinander kommunizieren können.

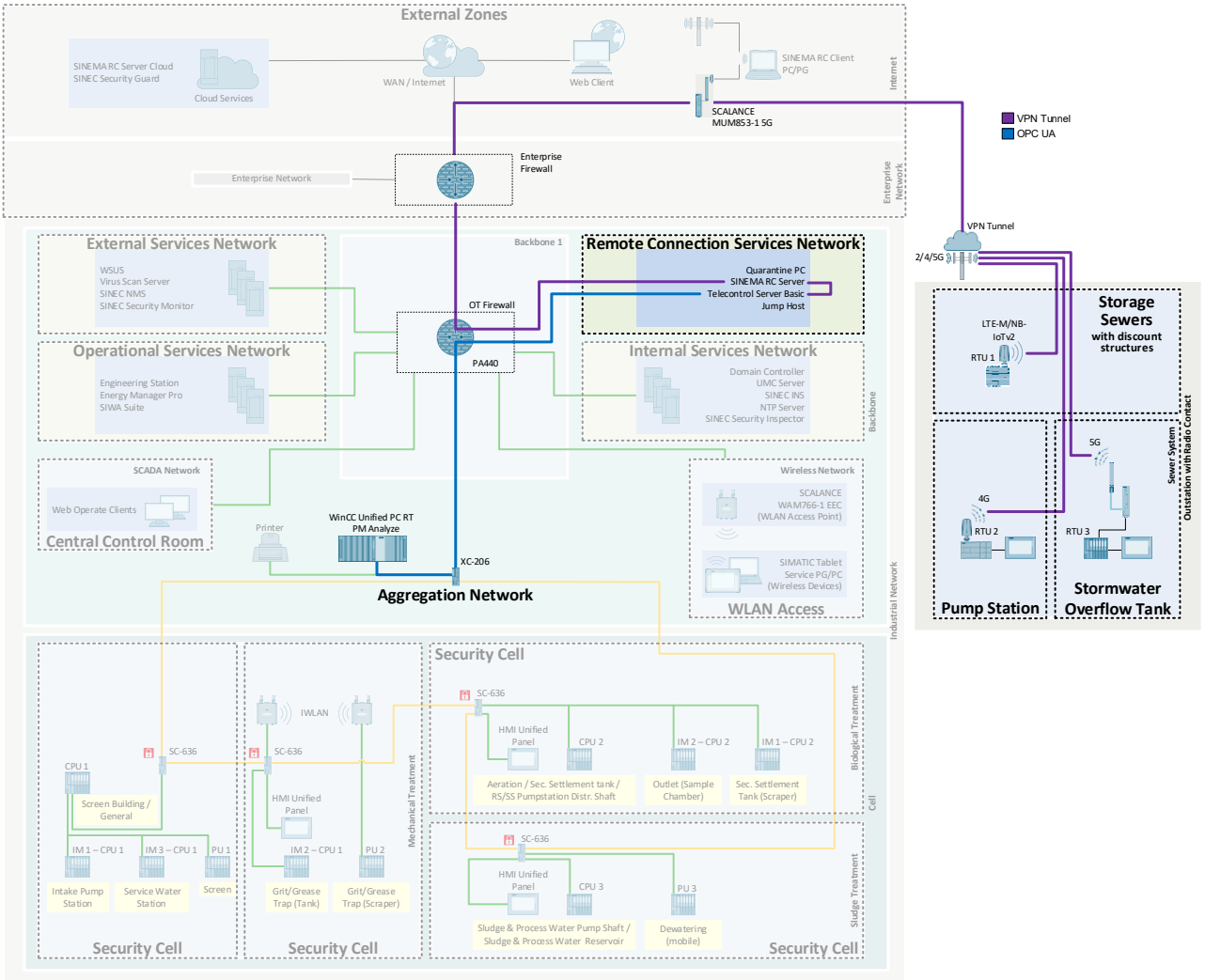

Abbildung 5-1: Remote-Verbindung zwischen WinCC Unified PC RT und den Remote-Stationen

5.3. Reduzierung der Angriffsfläche

In einem Automatisierungssystem wird ein erheblicher Teil der Angriffsfläche für Cyberbedrohungen von seinen Schnittstellen gebildet.

5.3.1. Minimierung des Funktionsumfangs

Um die Angriffsfläche zu reduzieren, wird das Prinzip der Minimierung des Funktionsumfangs umgesetzt. Dabei handelt es sich um zwei Sicherheitsmaßnahmen, die als „Härtung" bezeichnet werden.

- Deaktivierung aller unnötigen Schnittstellen.
- Schutz notwendiger Schnittstellen durch entsprechende Projektierung.

Typische Maßnahmen zum Schutz solcher Schnittstellen, die im Musterkonzept angewendet werden:

- Deaktivierung physischer Kommunikationsschnittstellen wie USB-Anschlüssen, Ethernet-Anschlüssen, Diagnoseschnittstellen und Drahtloskommunikation.
- Schutz der Funktionalität auf Systemebene, insbesondere bei Schnittstellen zu externen Komponenten, durch Eliminierung unnötiger Funktionen, Entfernen ungenutzter Softwareanwendungen und Deaktivieren von Kommunikationsports, Protokollen und/oder Diensten.

Diese Maßnahmen werden auf verschiedenen Komponentenebenen implementiert, einschließlich Anwendungen, Betriebssystemen und Schnittstellen auf unteren Ebenen im BIOS.

Empfohlene Härtungsmaßnahmen mit dem Ziel, die Angriffsfläche der oben beschriebenen Bereiche zu reduzieren, sind in Abschnitt 6.9 aufgeführt. Darüber hinaus spielen auch physische Schutzmaßnahmen wie Schlösser oder zutrittsbeschränkte Räume eine wichtige Rolle. Diese werden als Teil der vorgesehenen Betriebsumgebung der Zonen in Abschnitt 3.3 beschrieben.

Zudem ist es unerlässlich, dass die Entfernung aller vorübergehend aktivierten Funktionen nach der Inbetriebnahme, z. B. Fehlerbehebungs- und Testschnittstellen, sichergestellt ist und die Angriffsfläche während des Anlagenbetriebs minimiert wird, indem die Konten auf die unbedingt notwendigen beschränkt werden.

Weitere Informationen zur Minimierung des Funktionsumfangs in WinCC Unified-Systemen sind im Security Leitfaden zu finden.

- \3\ – „Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices", Section 4.1.1 (Protect SD and USB ports) und Section 4.1.2 (Disable network interfaces)

5.4. Sichere Kanäle und Verschlüsselung

Eine sichere Kommunikation gewährleistet die Integrität und Vertraulichkeit von Nachrichten, die über Netzwerke übertragen werden, und beinhaltet eine Endpoint-Authentifizierung.

5.4.1. Sichere Kanäle

Verschlüsselte Kanäle sind eine Kernmaßnahme zum Schutz von Daten während der Übertragung durch nicht vertrauenswürdige Zonen. Für Verkehr in einer vertrauenswürdigen Zone 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 VPN geschützte Kanäle zwischen Hauptanlage und allen Remote-Stationen, um Unabhängigkeit von den Sicherheitsfähigkeiten der Kommunikationsinfrastruktur zu erreichen (z. B. WWAN oder WLAN-Funk).
- Sichere Kommunikation innerhalb von vertrauenswürdigen Zonen für die Übertragung sensibler Daten (z. B. HTTPS, SSL, OPC UA, Secure OUC etc.). Die Anforderungen an die Echtzeitkommunikation müssen berücksichtigt werden.
- Verschlüsselung der vertraulichen Daten der SPS (z. B. private Schlüssel) durch Passwortschutz.

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, Blockierung von Komponenten oder 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 im Zusammenhang mit der Aktualisierung von Software und Projektierung und zusätzlichen Maßnahmen wie digital signierten Softwareaktualisierungen lässt sich der Schutz des Systems gegen Schadprogramme und unbefugte Änderungen durch den Einsatz von Virenscannersoftware und Whitelisting-Technologien implementieren.

Virenscannersoftware

Virenscannersoftware erkennt, blockiert und entfernt Schadprogramme (wenn notwendig und projektiert).

Für die Betriebsumgebung des Musterkonzepts gelten spezifische Projektierungsempfehlungen, siehe Abschnitt 8. Diese sind wichtig, um sicherzustellen, dass der Einsatz von Virenscannersoftware auf den Rechnern eines Automatisierungssystems nicht den Prozess 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.
- Die Projektierung wird angepasst, um potenzielle 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 oder nicht freigegebene Tools, werden blockiert.
- Whitelisting, regelbasiert: 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 auf dem neuesten Stand zu halten. Diese Aufgabe übernimmt ein Infrastrukturserver im „Externe Dienste“-Netzwerk. Die Stationen und Server für das Musterkonzept arbeiten auch mit Whitelisting-Software. Abschnitt 8 beschreibt diese Schutzmaßnahmen im Detail.

Es ist wichtig, neue Schadprogramme zu identifizieren, die Schwachstellen in den installierten Softwarekomponenten und Diensten ausnutzen. Daher müssen Virenscanner und Whitelisting-Lösungen durch Aufspielen aktueller Sicherheitspatches ergänzt werden. Die Patchmanagementverfahren für das Musterkonzept werden in Abschnitt 9 beschrieben.

5.5.2. Nachweis der Sicherheitsfunktionalität

Dieser ist wichtig, um die korrekte Funktionsweise der implementierten Sicherheitsmaßnahmen sicherzustellen. Der Nachweis ihrer vorgesehenen Funktion wird mittels geeigneter Sicherheitsprüfungen bei der Werksabnahme (FAT) oder beim Standortabnahmetest (SAT) empfohlen. Der Nachweis sollte danach auf regelmäßiger Grundlage wiederholt werden (z. B. im Rahmen der planmäßigen Wartung), um die Integrität der Sicherheitsinfrastruktur aufrechtzuerhalten.

5.5.3. Eingangsvalidierung, Ausgangsüberwachung und Fehlerbereinigung

Das Musterkonzept für die Abwasserbehandlungsanlage beruht auf der WinCC Unified SCADA-Lösung. WinCC Unified gewährleistet Funktionen wie Eingangsvalidierung und Ausgangsüberwachung in einem durchgängig sicheren Entwicklungsprozess. Dieser sichere Entwicklungsprozess ist nach dem Rahmenwerk der Norm IEC 62443 für Sicherheit in industriellen Leitsystemen zertifiziert, insbesondere Teil 4-1, in dem die Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung beschrieben werden.

- \5\ – „IEC 62443-4-1 Secure product development lifecycle“ for Digital Industries (DI)

5.5.4. Support für die Sicherung und Wiederherstellung von Leitsystemen

Das Ziel der Sicherung und Wiederherstellung besteht darin, dass der Bediener oder Asset-Eigner einen bekannten Systemzustand 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

Die Zeitsynchronisierung innerhalb des Musterkonzepts erfolgt über einen NTP-Server, der im „Interne Dienste“-Netzwerk gehostet wird. Der Domain Controller ruft Zeitsignale vom NTP-Server ab und verteilt sie an alle Domain-Mitglieder, z. B. OS-Clients und -Server, OPC UA-Server usw. Das SCADA-System (WinCC Unified PC RT), WinCC Unified Comfort Panels und mit dem Aggregationsnetzwerk verbundene Automatisierungsgeräte erhalten das Zeitsignal direkt vom NTP-Server.

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 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 wichtigen Systemkomponenten hinweg. Zusätzlich zu der auf den Prozess fokussierten Protokollierung und Überwachung, die von den Fähigkeiten regulärer Automatisierungs- und Leitsysteme 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 mit SINEC Security Monitor weitere Fähigkeiten zur Erkennung industrieller Anomalien implementiert werden. Weitere Einzelheiten sind im Abschnitt 5.7.3 zu finden.

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 erfolgen durch die OT-Firewall und durch die PC-basierten Systeme innerhalb der DMZ. Damit werden alle Zugriffe auf Benutzer- oder Systemebene sowie Kommunikationssitzungen auf Netzwerkebene (TCP/IP) abgedeckt.

5.6.2. Protokollierung sicherheitsbezogener Ereignisse

PC-basierte Systeme führen Sicherheitsprotokolle für Ereignisse sowohl auf Anwendungsebene als auch auf Betriebssystemebene. Sicherheitsprotokolle können über standardisierte Kommunikationsprotokolle wie Syslog oder SNMP zu zentralen Servern exportiert werden. Diese zentralen Server erfassen die Sicherheitsprotokollinformationen von den Systemkomponenten und bieten Schnittstellen, die in SIEM-Lösungen (Security Information Event Management) des Asset-Eigners integriert werden können. Weitere Informationen über SIEM-Funktionalitäten sind in Abschnitt 5.7.4 zu finden.

Für die Überwachung der Palo Alto OT-Firewall wird Panorama Management Software eingesetzt. Der Zugriff auf Sicherheitsprotokolle wird 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.

Für die geschützten Zonen des Musterkonzepts, wie Gebäude und zentrale Anlagenzonen, wird eine Sicherheitsprotokollierung durchgeführt. Dabei werden sowohl die WinCC Unified PC RT, WinCC Unified Comfort Panels als auch SCALANCE-Netzwerkgeräte und SIMATIC-SPSen abgedeckt.

Für die Weiterleitung sicherheitsrelevanter Ereignisse werden Syslog-Clients auf SPSen, Netzwerkgeräten und dem Netzwerkmanagementsystem SINEC NMS projektiert. SIMATIC-SPSen verwenden einen separaten Meldungsspeicher, um Benutzeranmeldungen, Projektierungsänderungen oder Betriebszustandsänderungen aufzuzeichnen. SINEC NMS und SCALANCE-Netzwerkgeräte protokollieren Systemereignisse, Netzwerkereignisse, Audit Trail-Ereignisse und Systemalarmmeldungen. Die konfigurierbare Weiterleitung an externe Syslog-Server oder SIEM-Systeme ermöglicht die Integration dieser Geräte in bestehende Sicherheitsüberwachungslösungen.

SINEC INS, das im „Interne Dienste"-Netzwerk eingesetzt wird, hostet den Syslog-Server, um sicherheitsrelevante Ereignisse zentral zu erfassen und zu speichern.

HINWEIS **Vermeiden des lokalen Zugriffs auf Geräte während des Betriebs**

Der physische Zugriff auf Geräte (WinCC Unified PCs und Panels, SPSen oder SCALANCE Netzwerkkomponenten) sollte strikt auf die anfängliche Inbetriebnahmephase beschränkt und während des regulären Betriebs, einschließlich Wartungsarbeiten, vermieden werden.

Daher dürfen administrative Aufgaben wie Aktualisierungen oder Projektierungsänderungen nicht direkt am Gerät durchgeführt werden. Stattdessen müssen sie über die dafür vorgesehene Infrastruktur ausgeführt werden, um sicherzustellen, dass alle Änderungen systematisch über zentrale Plattformen nachverfolgt und verwaltet werden, wodurch die Verantwortlichkeit und Rückverfolgbarkeit verbessert und das Risiko unbefugter Änderungen minimiert wird.

Um direkten physischen Zugriff zu verhindern, müssen Geräte in verschlossenen Schränken oder sicheren Gehäusen untergebracht werden. Während der Inbetriebnahme können die Schränke aus praktischen Gründen offen bleiben, müssen jedoch gesichert werden, sobald das System in Betrieb genommen wird.

- \40\ – „SIMATIC NET Netzwerkmanagement SINEC INS“
- \41\ – „SIMATIC NET Industrial Ethernet Security SCALANCE SC-600“, Abschnitt 4.4.13 (Syslog-Client)
- \42\ – „SIMATIC NET Industrial Ethernet Switches SCALANCE Layer 2 Switches“, Abschnitt 6.4.14 (Syslog-Client)
- \43\ – Netzwerkmanagement SINEC NMS, Abschnitt 6.2.18 (Operation-Parameterprofile (Control) – Syslog-Einstellungen), Abschnitt 6.7.5 (Control-Administration – Syslog-Einstellungen) und Anhang 7 (Syslog-Meldungen)
- \38\ – „Meldungen einer SIMATIC S7-1200/S7-1500 CPU per Syslog an SINEC INS senden“
- \39\ – „SIMATIC S7-1500/ET 200MP, S7-1500R/H, Drive Controller, S7-1500 Software Controller, ET 200SP, ET 200pro Syslog Messages“

5.6.3. Audit Trail

Um die Anforderungen im Hinblick auf das Änderungsmanagement zu erfüllen, werden alle Änderungen entweder über das WinCC Unified Audit Trail-System 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.

- \37\ – „WinCC Audit (RT Unified)“
- \43\ – Netzwerkmanagement SINEC NMS, Abschnitt 5.3 (Audit-Trail)

5.7. Zusätzliche Sicherheitsmaßnahmen

Die in Abschnitt 5 beschriebenen Sicherheitsmaßnahmen gewährleisten zusammen mit der in Abschnitt 6 beschriebenen Projektierung und Härtung 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 der Maßnahmen, die Siemens anbietet.

5.7.1. Threat Prevention Subscription für Palo Alto OT-Firewall

Die in Abschnitt 6.2.1 beschriebenen Palo Alto Next Generation Firewalls können um die Option Threat Prevention Subscription (TPS) erweitert werden. TPS wird dringend empfohlen, wenn der Fernzugriff implementiert ist, und muss für jede Next Generation Firewall bestellt werden. TPS beinhaltet ein Intrusion Prevention and Detection System (IPS/IDS), das einen integrierten Schutz gegen netzwerkseitige Bedrohungen wie Datenabgriffe, Schadprogramme, Command-and-Control-Datenverkehr, verschiedene Hackerwerkzeuge etc. durch die IPS-Funktionalität und eine datenstrombasierte Blockierung von Millionen bekannter Schadprogramme bietet.

5.7.2. 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 einer globalen Strategie für das Patchmanagement ist es notwendig, Hardware- und Softwarekomponenten laufend zu überwachen, um eventuelle Schwachstellen zu identifizieren und zu beheben. Der Industrial Vulnerability Manager bietet die folgenden Merkmale:

- Zugänglich über eine geschützte Web-Schnittstelle.
- Hosting einer Liste der in das ICS eingebetteten Komponenten, die im Laufe der Zeit auf Sicherheitsschwächen überwacht werden sollen.
- Freie Zuweisung der Komponenten zu der aufgestellten Überwachungsliste.
- Integration mit:
  - SIMATIC Management Console
  - SINEC NMS
  - TIA Portal
  - Proneta
  - SINEC Security Inspector
- 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.
  - 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").

SINEC Security Inspector

SINEC Security Inspector ist ein Sicherheits-Framework, das zur Automatisierung von Sicherheitstestprozessen in IT-/OT-Umgebungen entwickelt wurde. Es führt automatisierte Scans, Tests und Schwachstellenanalysen durch, um konsistente, reproduzierbare und zuverlässige Sicherheitstestergebnisse zu liefern. Es werden detaillierte Berichte erstellt, um die

Testergebnisse zusammenzufassen und so Werksabnahmetests, Standortabnahmetests und Konformitätsprüfungen zu ermöglichen. SINEC Security Inspector kann auch zur Unterstützung von Penetrationstests und manuellen Tests für sicherheitskritische Produkte und Umgebungen eingesetzt werden.

Im Musterkonzept der Abwasserbehandlungsanlage wird SINEC Security Inspector innerhalb des „Interne Dienste"-Netzwerks in der DMZ gehostet.

- \45\ – Industrial Ethernet Security SINEC Security Inspector, Section 7 (Asset discovery and vulnerability detection in factories)

SINEC Security Guard

SINEC Security Guard ist eine Cloud-basierte Sicherheitsplattform, mit der Betreiber von Siemens-OT-Anlagen das Risiko- und Sicherheitsmanagement in einem einzigen Tool zentralisieren können. SINEC Security Guard analysiert kontinuierlich Sicherheitshinweise von Lieferanten, um bekannte Schwachstellen mit Assets in der Produktionsumgebung abzugleichen. Betreiber können die zu beachtenden Sicherheitsrisiken bewerten, empfohlene Sicherheitsmaßnahmen priorisieren und Aufgaben zum Schwachstellenmanagement in ein Aufgabenmanagementsystem integrieren.

- \46\ – SINEC Security Guard

5.7.3. Industrial Anomaly Detection

SINEC Security Monitor

SINEC Security Monitor ist eine modulare, nicht intrusive Sicherheitsüberwachungssoftware, mit der 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 betroffene Geräte zu identifizieren. Darüber hinaus versteht die Software, wie die normale Kommunikation im Netzwerk aussieht, und kann mithilfe von KI-basierter Analyse Anomalien erkennen.

- \34\ – „Industrial Ethernet Security SINEC Security Monitor Operating Instructions"

5.7.4. Security Information Event Manager (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 eingesetzt werden.

Ein SIEM-System sammelt kontinuierlich Daten von Netzwerk- und Sicherheitsgeräten, korreliert und analysiert diese Informationen und stellt sie über eine zentrale Schnittstelle dar. Auf Grundlage dieser Analyse lassen sich geeignete Sicherheitsmaßnahmen ableiten. Damit können sicherheitsrelevante Vorfälle schneller erkannt, Anlagenbetreiber umgehend informiert und Gegenmaßnahmen so schnell wie möglich eingeleitet werden.

5.7.5. Industrial Cybersecurity Services

Zwar bieten viele SIMATIC-Produkte integrierte Konfigurationen zur Verbesserung der Cybersicherheit, doch aufgrund begrenzter interner Fachkenntnisse kommen diese Funktionen in der Praxis nur selten zum Einsatz.

Siemens schließt diese Lücke mit einer Reihe von Industrial Cybersecurity Services, die auf SIMATIC-Automatisierungssysteme zugeschnitten sind und internationalen Normen wie IEC 62443 und der europäischen NIS 2-Richtlinie entsprechen. Diese Services sollen:

- für Transparenz hinsichtlich des aktuellen Sicherheitsstatus und der Einhaltung von Sicherheitsnormen sorgen.
- Implementierung und Projektierung von Sicherheitsfunktionen nach dem neuesten Stand der Technik sicherstellen.
- langfristige Unterstützung zur Aufrechterhaltung und Verbesserung des Security Level über den gesamten Lebenszyklus des Systems/der Anlage hinweg bieten.

Das Industrial Cybersecurity Services-Portfolio von Siemens ist gemäß dem Defense-in-Depth-Konzept in drei Hauptkategorien unterteilt.

1. Plant Security Services

- Security Assessments – Identifizierung von Sicherheitslücken und Festlegung von Gegenmaßnahmen nach IEC 62443 und auf NIS 2 basierten Evaluierungen.
- Scanning Services – Transparenz über Assets und Schwachstellen.
- Industrial Security Consulting – Unterstützung bei Richtlinien, sicherer Netzwerkauslegung, Implementierung und Vorfallanalyse.
- Cybersecurity Trainings – Vermittlung des notwendigen Wissens, um das „schwächste Glied" abzusichern.
- Remote Industrial Operations Services (RiOPS) – 24/7-Fernüberwachung und -verwaltung von IT/OT-Infrastrukturen.

2. Network Security Services
   - Industrial Next Generation Firewall – Durchgängiger Netzwerkschutz mit Next Generation Firewalls.
   - Industrial DMZ Infrastructure – Sicherer Datenaustausch zwischen IT und OT.
   - Remote Platform Software as a Service – Sicherer Fernzugriff auf Industriegeräte.
3. System Integrity Services
   - Endpoint Protection – Durchgängiger Endpunktschutz mit Antivirensoftware und Application Control.
   - Vulnerability Services – Vulnerability Intelligence und Vulnerability Management.
   - Patch Management – Verwaltung kritischer Updates in Microsoft-Produkten.
   - Backup and Restore – Vorkonfigurierte IT-Infrastruktur für die Notfallwiederherstellung.

Die Industrial Cybersecurity Services von Siemens können über den Siemens-Ansprechpartner vor Ort bestellt werden.

- \8\ – „Siemens Industrial Cybersecurity Services"

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. Abweichungen vom Musterkonzept erfordern eine neue Bedrohungs- und Risikoanalyse. Die entsprechenden Härtungsmaßnahmen und Projektierungen müssen überprüft und entsprechend angepasst werden.

6.1. Annahmen

IEC 62443-3-3	SR 1.7 Stärke der Authentifizierung durch Passwörter SR 1.7 RE1 Erzeugung und Lebensdauerbeschränkungen von Passwörtern für menschliche Benutzer 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 Anlagenbetreibers liegen.

Nach 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 Remote-Stationen wird durch physische Maßnahmen verhindert. Der Zugang zu den Remote-Stationen wird überwacht, z. B. mit Hilfe von Türschaltern, und nur autorisiertes Personal hat Zugang.
- Alle Schränke haben eine Schließanlage mit Halbzylindern.
- Alle Schränke, sowohl im Hauptteil der Abwasserbehandlungsanlage als auch in den Remote-Stationen, sind in abschließbaren Schalt- oder Serverräumen installiert. Der Zugang zu Schalt- und Serverräumen ist auf autorisiertes Personal (Instandhaltung) beschränkt.
- Das Aggregationsnetzwerk ist in einem Gebäude mit hochgradigem physischem Schutz installiert, wie in Abbildung 3-3 dargestellt. Wenn das Aggregationsnetzwerk nicht auf ein Gebäude beschränkt ist, muss es physisch geschützt werden, um Abhörangriffe zu verhindern.

Für alle im Musterkonzept 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 \1\.
- Für alle Komponenten sind die neuesten freigegebenen Patches zu installieren. Die Patches für Siemens-Komponenten sind über den Siemens Industry Online Support verfügbar \1\. Weitere Informationen zum Patchmanagement sind in Abschnitt 9 zu finden.
- Auf allen Betriebssystemen sollten die neuesten veröffentlichten Sicherheitspatches installiert sein. Weitere Informationen sind in Abschnitt 9.1 zu finden.
- Für die Virenscanner der Workstations und Server sind immer die neuesten Virenerkennungsmuster zu installieren.
- Für die Endpunktschutz-Software der Workstations und Server sind immer die neuesten Softwareaktualisierungen, Erkennungsmuster usw. zu installieren. Das Ändern der Projektierung, das Deinstallieren oder Deaktivieren der Endpunktschutz-Software muss passwortgeschützt sein. Weitere Informationen zur Endpunktschutz-Software sind unter „Continuous endpoint protection against malware" zu finden \9\.

- 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 der „Checkliste für die Einrichtung von SCALANCE-Geräten“ \10\ in Betracht zu ziehen und zentral von SINEC NMS abzuarbeiten.

6.2. Firewalls für sichere Kommunikation zwischen den Zonen

Die Kommunikation zwischen Sicherheitszonen muss überwacht und gesteuert werden, siehe Abschnitt 5.1.2.

Die Grenze des Anlagennetzwerks wird durch die OT-Firewall geschützt. Diese Firewall bildet eine demilitarisierte Zone. Härtungsmaßnahmen und Projektierung der Firewall werden in Abschnitt 6.2.1 beschrieben.

Die Kommunikation zwischen den Sicherheitszellen innerhalb des Aggregationsnetzwerks wird durch SCALANCE Netzwerksicherheitsgeräten geschützt. Härtungsmaßnahmen und Projektierung dieser Geräte werden in Abschnitt 6.2.2 beschrieben.

6.2.1. Palo Alto 440 NGFW

OT-Firewall

Schützt die Netzwerke in der DMZ („Externe Dienste“-Netzwerk, „Remote-Verbindungsdienste“-Netzwerk, „Operative Dienste“-Netzwerk, „Interne Dienste“-Netzwerk) und die internen Netzwerke (WLAN-Zugangsnetzwerk, SCADA-Netzwerk, Aggregationsnetzwerk) vor nicht vertrauenswürdigen externen Netzwerken wie dem Unternehmensnetzwerk und dem Internet.

Darüber hinaus ermöglicht sie es Servern in der DMZ, geschützt mit öffentlichen Servern im Internet und den Remote-Stationen der Abwasserbehandlungsanlage zu kommunizieren. Sowohl ausgehende als auch eingehende Daten werden mittels Deep Package Inspection (DPI) durchsucht.

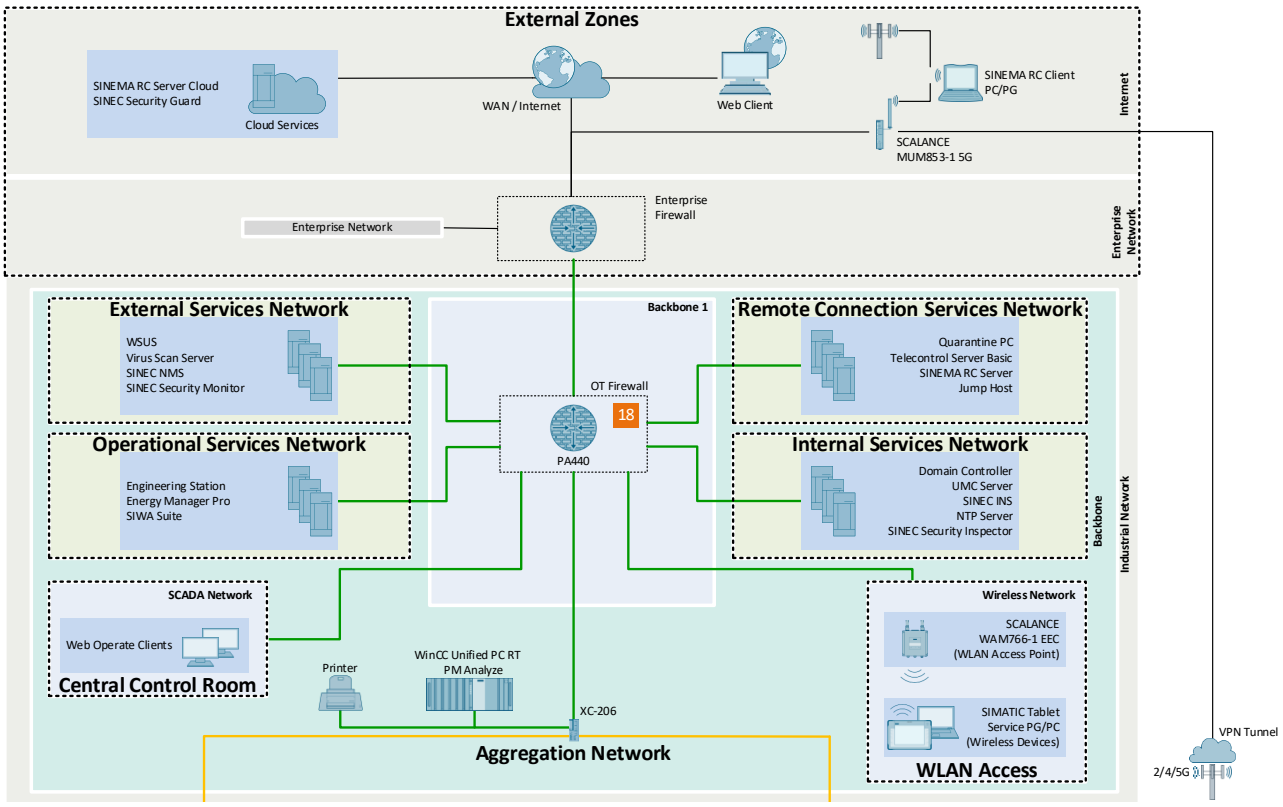

Abbildung 6-1: OT-Firewall

Die empfohlenen Härtungsmaßnahmen und Projektierungen für die OT-Firewall sind nachstehend aufgeführt.

Tabelle 6-1: OT-Firewall

SCI	Lieferant	Typ	MLFB	Funktion
18	Palo Alto	440 NGFW	9LA1110-6SY12-1AB1	OT-Firewall

Tabelle 6-2: Härtungsmaßnahmen für die OT-Firewall

Nr.	Sicherheitsthema	Härtungsmaßnahme
1	Beschränkung von IP-Adressen	Beschränkung des Zugriffs auf diejenigen IP-Adressen, die notwendig sind
2	Beschränkung von Diensten	Blockieren des Zugriffs über unsichere Protokolle (HTTP oder Telnet). Erforderlich ist SSH und/oder HTTPS.
3	Änderung von Admin-Berechtigungen/Benutzerverwaltung	• Änderung des Standardbenutzernamens und Standardpassworts • Projektierung eines Kontos für jeden Benutzer, der Zugriff benötigt, und nur Erteilung der minimal erforderlichen Zugriffsrechte • Einsatz von Mehrfaktorauthentifizierung (RADIUS oder SAML) • Projektierung strenger Passwortregeln
4	Dedizierte Managementschnittstelle	Einsatz der dedizierten Managementschnittstelle in einem separaten Management-LAN oder Management-VLAN
5	Sicherheitsrichtlinie mit Regeln und Profilen	• Durchsuchung des gesamten Verkehrs zur Managementschnittstelle auf Bedrohungen • Erstellung eines Sicherheitsprofils, Aktivierung einer erweiterten Paketerfassung • Projektierung von Inbound Inspection und SSL Forward Proxy
6	Protokollierung	• Einrichtung einer Protokollierung für Projektierungsänderungen • Einrichtung einer Protokollierung für unbefugte Anmeldeversuche
7	SNMP	• Einsatz von SNMP v3 • Einrichtung eines nicht leicht zu erratenden SNMP-Strings • Aktivieren von SNMP nur an internen Schnittstellen
8	Zertifikate	Ersetzen des Standardzertifikats durch ein vom Enterprise-CA der Organisation signiertes Zertifikat
9	Aktualisierungen	Halten des PAN-OS und aller Softwarepakete auf dem neuesten Stand

Weitere Informationen zur sicheren Projektierung der Palo Alto Next Generation Firewall sind zu finden in:

- \11\ – PAN-OS Administrator’s Guide
- \12\ – Palo Alto – PAN-OS
- \13\ – Palo Alto – Best Practices for Securing Administrative Access

6.2.2. SCALANCE-Netzwerksicherheitsgeräte

Die sichere Kommunikation zwischen den Zellen des Aggregationsnetzwerks und zwischen dem zentralen Anlagengebäude und den Remote-Stationen wird durch den Einsatz von SCALANCE-Netzwerksicherheitsgeräten implementiert, wie in Abbildung 3-2 dargestellt.

Im Musterkonzept werden die folgenden SCALANCE-Netzwerksicherheitsgeräte eingesetzt:

Tabelle 6-3: SCALANCE-Netzwerksicherheitsgeräte

SCI	Lieferant	Typ	MLFB	Funktion
19	Siemens	SCALANCE SC-636	6GK5636-2GS00-2AC2	Sichere Kommunikation zwischen Sicherheitszellen und anderen Netzwerken
20	Siemens	SCALANCE MUM 853-1 5G	6GK5853-2EA00-2DA1	Leistungsstarke und sichere Konnektivität über 5G-Netzwerke
21	Siemens	SCALANCE WAM766-1 EEC	6GK5766-1GE00-7TX0	Zugangspunkt für die sichere drahtlose Kommunikation mit mobilen Geräten

Für die in Tabelle 6-3 aufgeführten SCALANCE-Geräte müssen die folgenden allgemeinen Härtungsmaßnahmen in Betracht gezogen werden:

Tabelle 6-4: Härtungsmaßnahmen für SCALANCE-Netzwerksicherheitsgeräte

Nr.	Sicherheitsthema	Härtungsmaßnahme	Dokumentation
1	Sicheres Netzwerk	• Priorität für Quality of Service (QOS) auf „DSCP“ einstellen • Spanning Tree deaktivieren, wenn nicht erforderlich • Passives Mithören deaktivieren	\10\ – Abschnitt 3.10. \10\ – Abschnitt 3.11.2. \10\ – Abschnitt 3.11.3.
2	Identitäts- und Zugriffsmanagement	• Zentrale Authentifizierung über RADIUS/UMC/AD verwenden • Passwortregeln (Komplexität und Änderungshäufigkeit) festlegen • Änderungen zentral und regelmäßig über SINEC NMS verbreiten	\10\ – Abschnitt 3.6. \14\ – Benutzerverwaltung für SCALANCE-Geräte mit RADIUS-Protokoll
3	Reduzierung der Angriffsfläche	• Unverschlüsselter und nicht erforderliche Protokolle deaktivieren • PROFINET-Schnittstelle deaktivieren • Ungenutzte Ports deaktivieren • Alle nicht erforderlichen Dienste wie DHCP oder DNS deaktivieren	\10\ – Abschnitt 3.3 \10\ – Abschnitt 3.7. \10\ – Abschnitt 3.9.1. \10\ – Abschnitt 3.14.1.
4	Sichere Kanäle und Verschlüsselung	Keine Maßnahmen erforderlich	
5	Systemintegrität	Einsatz von NTP zur Uhrzeitsynchronisation. Falls verfügbar, die sichere NTP-Variante verwenden.	\10\ – Abschnitt 3.2.
6	Protokollierung und Überwachung	Syslog-Client aktivieren.	Abschnitt 5.6.2. Abschnitt 5.7.4.

Protokolleinstellungen

Die folgende Tabelle zeigt die Einstellungen für die Protokolle, die von den SCALANCE-Geräten im Musterkonzept verwendet werden.

Tabelle 6-5: Protokolleinstellungen

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

IPSec-VPN- und Firewall-Konfiguration

Die sichere Kommunikation mit externen Zonen wird durch IPsec-VPN und die interne Firewall gewährleistet. Tabelle 6-6 und Tabelle 6-7 zeigen die IPSec- bzw. Firewall-Einstellungen.

Tabelle 6-6: IPsec-VPN-Konfiguration

Nr.	Thema	Einstellungen
1	Ferne Gegenstelle	Remote-Modus: Standard Remote-Typ: Manuell
2	Verbindung	KEYing-Protokoll: IKEv2
3	Authentifizierung	CA-signierte Zertifikate
4	Phase 1	Voreingestellte Ciphers verwenden Mindestens zu verwenden: • Verschlüsselung: AES128 GCM 16 • Authentifizierung: SHA256 • Schlüsselableitung: DH-Gruppe 14
5	Phase 2	Voreingestellte Ciphers und automatische Firewall-Regeln verwenden Mindestens zu verwenden: • Verschlüsselung: AES128 GCM 16 • Authentifizierung: SHA256 • Schlüsselableitung: DH-Gruppe 14

Tabelle 6-7: Firewall-Einstellungen

Nr.	Thema	Einstellungen
1	IPv4 vordefiniert	Alle nicht erforderlichen Dienste für VLANs deaktivieren

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

- \10\ – „Checkliste für die Einrichtung von SCALANCE-Geräten“
- \14\ – „Benutzerverwaltung für SCALANCE-Geräte mit RADIUS-Protokoll“

6.3. Netzwerkkomponenten für die Drahtloskommunikation

Drahtloskommunikation mittels IWLAN wird im Musterkonzept eingesetzt, um SIMATIC-Tablets und Service Field PGs/PCs einen drahtlosen Zugang zu den Geräten und Systemen in der DMZ und im Aggregationsnetwork zu ermöglichen. Darüber hinaus werden drahtlose Verbindungen zwischen Automatisierungsgeräten hergestellt, die sich im Bereich mechanische Behandlung befinden, sowie zwischen der Funkgegenstation, die das zentrale Anlagengebäude mit den Remote-Stationen verbindet.

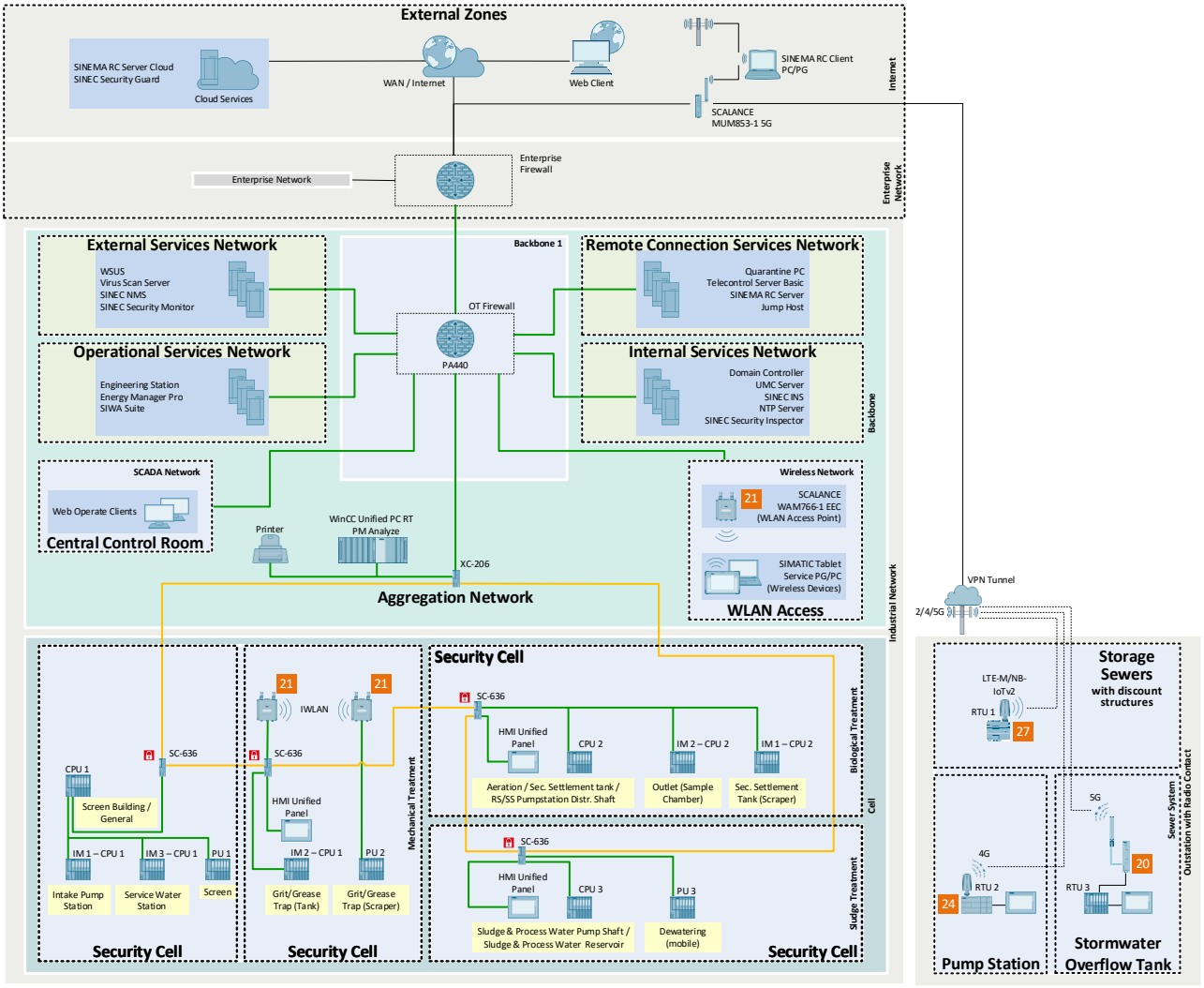

Abbildung 6-2: Drahtloskommunikation

Tabelle 6-8: Drahtlosgeräte

SCI	Lieferant	Typ	MLFB	Funktion
20	Siemens	SCALANCE MUM 853-1 5G	6GK5853-2EA00-2DA1	Leistungsstarke und sichere Konnektivität über 5G-Netzwerke
21	Siemens	SCALANCE WAM766-1 EEC	6GK5766-1GE00-7TX0	Zugangspunkt für die sichere drahtlose Kommunikation
24	Siemens	CPU 1214C mit CP 1243-7 LTE EU	6GK7243-7KX30-0XE0	Sichere Verbindung zwischen der SIMATIC S7-1200 CPU in der externen Pumpstation und dem zentralen Anlagenbereich

SCI	Lieferant	Typ	MLFB	Funktion
27	Siemens	RTU 3051C mit integriertem Modem für LTE-M/NB-IoTv2	6NH3112-5BB00-0XX0	Sichere Verbindung zwischen der RTU in den Stauraumkanälen und dem zentralen Anlagengebäude

Die Härtungsmaßnahmen für die SCALANCE-Geräte sind in Tabelle 6-4 und Tabelle 6-5 aufgeführt.

Neben diesen allgemeinen Härtungsmaßnahmen und der Projektierung sind die folgenden Härtungsmaßnahmen für SCALANCE-Drahtlosgeräte in Betracht zu ziehen:

Tabelle 6-9: Zusätzliche Härtungsmaßnahmen für SCALANCE W

Nr.	Sicherheitsthema	Härtungsmaßnahme	Dokumentation
1	WLAN-Verschlüsselung	Aktivieren der AES-Verschlüsselung für iPCF	\10\ – Abschnitt 3.12.1.
2	Tunnel WLAN Schicht 2	Mac-Modus auf „Layer-2-Tunnel" einstellen. Diese Einstellung wird nur unterstützt, wenn ausschließlich SCALANCE-Geräte verwendet werden.	\10\ – Abschnitt 3.12.2.
3	WLAN iPCF	iPCF verwenden, wenn zeitkritische Daten, z. B. PROFINET, auf der Funkverbindung übertragen werden.	\10\ – Abschnitt 3.12.3

Die Härtungsmaßnahmen für den drahtlosen TeleControl CP 1243-7 LTE EU sind in Abschnitt 6.6 beschrieben.

6.4. Netzwerkkomponenten – SCALANCE XC

Die Managed Layer-2-Switches der SCALANCE XC-200-Serie sorgen für die Konnektivität zwischen Automatisierungsgeräten innerhalb der Prozesszellen.

Tabelle 6-10: SCALANCE XC-Switches

SCI	Lieferant	Typ	MLFB	Funktion
22	Siemens	SCALANCE XC-206 – 2SFP	6GK5206-2BS00-2AC2	Ring-Manager im Aggregationsnetzwerk
-	Siemens	SCALANCE XC-208	6GK5208-0BA00-2AC2	Switch zur Bereitstellung von Layer-2-Netzwerkkonnektivität für Geräte in: Zulaufpumpstation, Regenwasserbecken, externe Pumpstation, Rechen, Sand- und Fettfang, sekundäres Absetzbecken, Ablauf, Entwässerung.
-	Siemens	SCALANCE XC-216	6GK5216-0BA00-2AC2	Switch zur Bereitstellung von Layer-2-Netzwerkkonnektivität für Geräte in: Rechenanlage/Allgemeines, Schlamm- und Prozesswasserbecken.
-	Siemens	SCALANCE XC-224	6GK5224-0BA00-2AC2	Switch zur Bereitstellung von Layer-2-Netzwerkkonnektivität für Geräte in: Belüftungsprozess.

Die Härtungsmaßnahmen für die SCALANCE-Switches sind in Tabelle 6-4 und Tabelle 6-5 aufgeführt.

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

Tabelle 6-11: Zusätzliche Härtungsmaßnahmen für SCALANCE XC-200

Nr.	Sicherheitsthema	Härtungsmaßnahme	Dokumentation
1	Ringredundanz	Ringredundanz deaktivieren, wenn das Gerät nicht in einer Ringtopologie betrieben wird	\10\ – Abschnitt 3.11.1
2	PROFINET	Wenn das SCALANCE-Gerät in einem PROFINET-Netzwerk verwendet wird, muss die Schnittstellenfunktionalität für PROFINET aktiviert werden.	\10\ – Abschnitt 3.7

6.5. TeleControl CP 1542SP-1 IRC

Der Kommunikationsprozessor CP 1542SP-1 IRC verbindet ET 200SP-CPUs über TeleControl-Protokolle wie TeleControl Basic, DNP3 und IEC 60870-5-104 mit Leitstellen.

Im Musterkonzept arbeitet der CP 1542SP-1 IRC in Verbindung mit dem drahtlosen SCALANCE MUM 853-1, um eine sichere TeleControl-Kommunikation zwischen dem Regenwasserbecken und TeleControl Server Basic im zentralen Anlagengebäude herzustellen. Siehe Abbildung 3-12.

Im Folgenden sind die Härtungsmaßnahmen für den CP 1542SP-1 IRC aufgeführt.

Tabelle 6-12: Härtungsmaßnahmen für CP 1542SP-1 IRC

Nr.	Sicherheitsthema	Härtungsmaßnahme	Dokumentation
1	VPN	Einsatz von SINEMA RC (OpenVPN)	\32\ – Abschnitt 1.6 \32\ – Abschnitt 1.7
2	SNMP	Deaktivierung von SNMP oder Einsatz von SNMP v3	\32\ – Abschnitt 1.7

6.6. TeleControl CP 1243-7 LTE

Der Kommunikationsprozessor CP 1243-7 LTE EU dient zur Verbindung von SIMATIC S7-1200-CPUs mit LTE-Netzen, die in europäischen Frequenzbändern betrieben werden.

Für die Abwasserbehandlungsanlage ist das Kommunikationsmodul mit TC-SRC (TeleControl-Kommunikation über SINEMA Remote Connect) projektiert, um die Verbindung zwischen der externen Pumpstation und dem zentralen Anlagenbereich zu schützen. Siehe Abbildung 3-13.

Die folgenden Härtungsmaßnahmen werden empfohlen:

Tabelle 6-13: Härtungsmaßnahmen für CP 1243-7 LTE

Nr.	Sicherheitsthema	Härtungsmaßnahme	Dokumentation
1	VPN	Einsatz von VPN-Tunneln: • IPsec • SINEMA RC (OpenVPN)	\30\ – Abschnitt 1.5
2	Firewall	Aktivierung der Firewall: • IP-Firewall mit Stateful Packet Inspection (Schichten 3 und 4) – Zustandsorientierte Paketüberprüfung • Firewall für „Non-IP“ Ethernet Frames nach IEEE 802.3 (Schicht 2) • Begrenzung der Übertragungsgeschwindigkeit zur Einschränkung von Flood- und DoS-Angriffen • Globale Firewall-Regeln	\30\ – Abschnitt 1.5
3	Webserver-Zugriff auf die CPU	Nur Einsatz von HTTPS	\30\ – Abschnitt 1.5
4	NTP	Einsatz von NTP (Secure) für eine sichere Übertragung während der Zeitsynchronisation, wenn die TeleControl-Kommunikation deaktiviert ist	\30\ – Abschnitt 1.5

6.7. TeleControl RTU 3051C

Die kompakte SIMATIC RTU 3051C dient zum Überwachen von Stauraumkanälen mit Entlastungsstrukturen. Diese Remote-Station ist geografisch verteilt und besitzt keinen Anschluss an ein Spannungsversorgungsnetz.

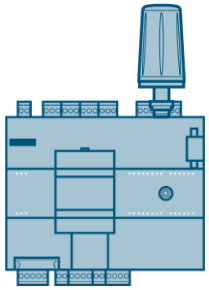

Abbildung 6-3: RTU 3051C

Die Remote Terminal Unit kann Prozessdaten speichern und über mobile Drahtloskommunikation an eine Masterstation übertragen. Um eine sichere Kommunikation zwischen der RTU 3051C in der Remote-Station und TeleControl Server Basic im zentralen Anlagengebäude zu gewährleisten, wird eine verschlüsselte Kommunikation über den SINEMA RC-Server hergestellt. Siehe Abbildung 3-14.

Im Folgenden sind die Härtungsmaßnahmen für die RTU 3051C aufgeführt.

Tabelle 6-14: Härtungsmaßnahmen für RTU 3051C

Nr.	Sicherheitsthema	Härtungsmaßnahme	Dokumentation
1	VPN	Einsatz von OpenVPN: RTU als OpenVPN-Client projektieren	\28\ – Abschnitt 3.8 \28\ – Abschnitt 6.15.1
2	HTTPS für WAN	• HTTPS für WAN aktivieren • SMS-Eingang sperren	\28\ – Abschnitt 6.13
3	Webserver-Zugriff	Nur Einsatz von HTTPS	\28\ – Abschnitt 6.15.3

6.8. NTP-Server

Der NTP-Server verwaltet zentral die Zeitsynchronisation in der gesamten Anlage und befindet sich im „Interne Dienste"-Netzwerk.

Der Domain Controller empfängt das Zeitsignal vom NTP-Server und verteilt es an die Workstations und Server in der DMZ. Eingebettete Geräte wie die WinCC Unified PC RT, Unified Comfort Panels oder die ET 200SP Distributed Controllers erhalten das Zeitsignal direkt vom NTP-Server.

Die empfohlenen Sicherheitsmaßnahmen sind:

- Einsatz von NTP (Secure), z. B. Network Time Security (NTS)
- Einsatz von SNMPv3

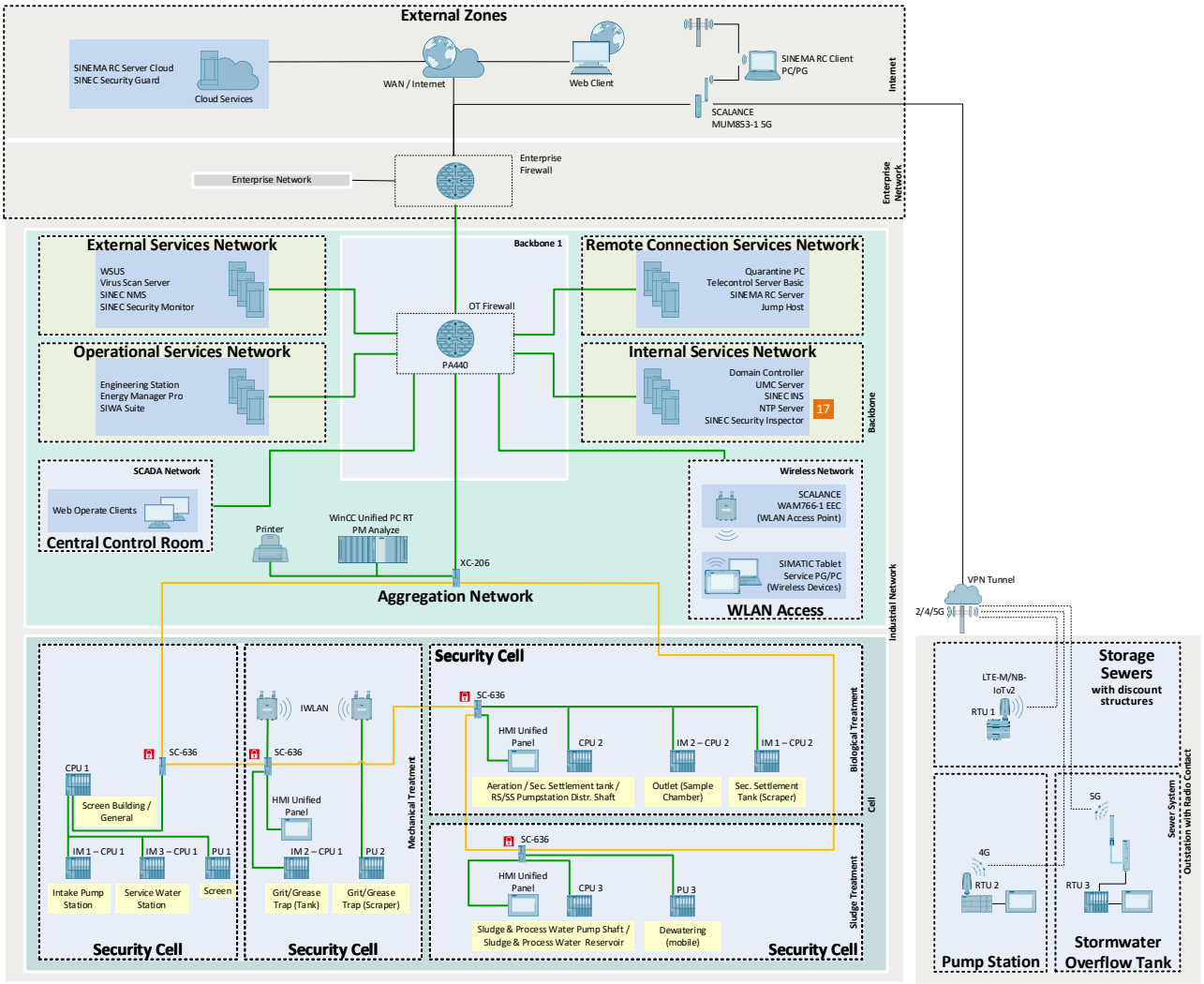

Abbildung 6-4: NTP-Server

6.9. Workstations und Server

Im Musterkonzept der Abwasserbehandlungsanlage sind die Softwareanwendungen und WinCC Unified PC RT auf den Siemens Industrial Workstations (IPCs) installiert.

6.9.1. Workstations und Server

Die folgenden Härtungsmaßnahmen müssen sowohl für die WinCC Unified PC RT Workstation als auch für die Server in der DMZ implementiert werden.

Tabelle 6-15: Allgemeine Härtungsmaßnahmen für Workstations und Server

Nr.	Sicherheitsthema	Härtungsmaßnahme	Dokumentation
1	Sicheres Netzwerk	Einsatz der Windows-Firewall	\47\ – Abschnitt 2.1 \47\ – Abschnitt 5.1
2	Identitäts- und Zugriffsmanagement	• BIOS-Einstellungen einrichten • Benutzerverwaltung mit Active Directory projektieren	-
3	Reduzierung der Angriffsfläche	• Unnötige Windows-Komponenten entfernen • Windows-Dienste deaktivieren • Serverfunktionalität Automation License Manager (ALM) deaktivieren, wenn die Anlage in Betrieb ist • SMB-Signierung aktivieren • SMVv1. deaktivieren • Blockierung von USB-Speichermedien: - Sperren oder mit anderen mechanischen Mitteln deaktivieren - Zugriff mit Windows-Gruppenrichtlinie beschränken • USB-Anschlüsse – Autorun und Autoplay deaktivieren	\47\ – Abschnitt 2.1 \47\ – Abschnitt 4.8 \47\ – Abschnitt 4.10 \47\ – Abschnitt 4.11
4	Sichere Kanäle und Verschlüsselung	Verschlüsselte Kommunikation in der SIMATIC Shell aktivieren	-
5	Systemintegrität	• Einsatz von Whitelisting-Technologien • Installation von Virenscannersoftware • Einsatz digitaler Signaturen zum Nachweis, dass Anwendungen, Binärdateien und Bibliotheken nicht geändert wurden • Patching des Betriebssystems • Sicherung von Engineering-Daten und Systemdaten	-

Nr.	Sicherheitsthema	Härtungsmaßnahme	Dokumentation
6	Protokollierung und Überwachung	• Einsatz der Ereignisanzeige, um Sicherheitsprotokolle, Systemprotokolle und Anwendungsprotokolle zu überwachen • Weiterleitung der Protokolle mittels Windows Event Forwarding (WEF) oder Syslog an den zentralen Server	-

Einige der oben aufgeführten Härtungsmaßnahmen können in den Gruppenrichtlinienobjekten (GPOs) von Windows projektiert werden. Im Musterkonzept werden die GPOs zentral am Domain Controller verwaltet. Siehe Abschnitt 7.1.

Weitere Sicherheitseinstellungen für Windows- und Linux-basierte IPCs sind in der folgenden Dokumentation zu finden.

- \47\ – Empfohlene Sicherheitseinstellungen für IPCs im Industrieumfeld (Windows)
- \48\ – SIMATIC IPC – Security Leitfaden für Linux-Systeme

6.9.2. WinCC Unified PC RT

Für die WinCC Unified PC RT und Web Operate Clients kann mit dem Windows-Kioskmodus zusätzliche Sicherheit erreicht werden. Dieser Modus beschränkt Benutzer auf eine einzige Anwendung – beispielsweise Microsoft Edge für den Zugriff auf das SCADA-System – und verhindert so den Zugriff auf die Windows-Umgebung, Systemeinstellungen und andere Anwendungen.

Tabelle 6-16: Härtungsmaßnahmen für WinCC Unified PC Runtime

Nr.	Sicherheitsthema	Härtungsmaßnahme	Dokumentation
1	Windows-Kioskmodus	Einsatz des Windows-Kioskmodus, um den Zugriff auf Windows-Standardfunktionen zu unterbinden	\3\ – Abschnitt 3.5

Weitere Härtungsmaßnahmen im Zusammenhang mit der Nutzung von Diensten und Anwendungen in WinCC Unified sind im Security Leitfaden zu finden.

- \3\ – „Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices“, Section 5 (Risk analysis when using services and apps)

6.9.3. PM ANALYZE

PM ANALYZE ist ein WinCC-Add-on, das leistungsstarke Tools für die Archivierung, Analyse und Berichterstellung bietet und damit die Funktionalität des SCADA-Systems erweitert. Es wird im Musterkonzept eingesetzt, um spezielle Berichte gemäß DWA (Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V.) zu erstellen, und besteht aus den folgenden Modulen:

- PM-SERVER: Zentrale Plattform für die Datenarchivierung und -verwaltung
- PM-AGENT: Verwaltet die Datenübertragung von der WinCC Unified PC RT zum PM-SERVER. Alle eingehenden Alarme und Prozesswerte werden an den Server weitergeleitet, wo sie in den konfigurierten Alarm- oder Prozesswertarchiven aufgezeichnet werden.
- PM-CLIENT: Stellt die Benutzeroberflächenkomponente bereit, die Visualisierungs- und Analysefunktionen für Betreiber und Analysten bietet.

In der Abwasserbehandlungsanlage werden sowohl der PM-SERVER als auch der PM-AGENT auf derselben Workstation wie die WinCC Unified PC RT gehostet. Der PM-CLIENT wird in der zentralen Leitwarte eingesetzt und ermöglicht den Bedienern den Zugriff auf archivierte Daten und Berichte sowie deren Visualisierung.

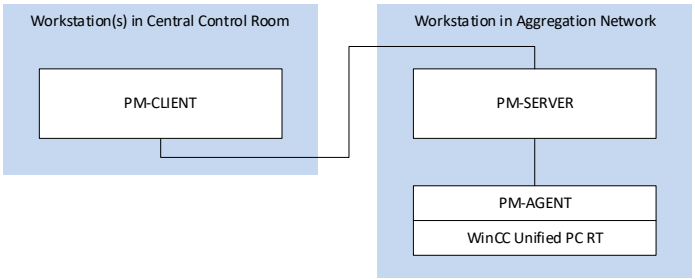

Abbildung 6-5: Implementierung von PM ANALYZE

Es gelten alle in Abschnitt 6.9.1 genannten Härtungsmaßnahmen. Der Einsatz von Whitelisting auf dem PM ANALYZE Server wird jedoch nicht empfohlen.

Weitere Informationen zu PM ANALYZE sind im folgenden Dokument zu finden.

- \49\ – PM-ANALYZE Systembeschreibung

6.9.4. SINEC NMS

SINEC NMS ist ein Netzwerkmanagementsystem zur Überwachung und Administration von Netzwerken und deren Geräten. Es unterstützt eine verteilte Systemarchitektur, die aus einer zentralen „Steuerungskomponente“ und einer oder mehreren verteilten „Operation“-Instanzen in verschiedenen Netzwerksegmenten (z. B. im Aggregationsnetzwerk oder im WLAN-Zugangsnetzwerk) besteht.

- NMS Control: Verwaltet Konfigurationsleitlinien, analysiert Diagnosedaten und liefert einen Überblick über die gesamte OT-Netzwerkinfrastruktur. NMS Control bietet auch Northbound-Schnittstellen für die Integration in darüberliegende Systeme und Dienste; diese umfassen Syslog-Weiterleitung, URL-Adresse, Bestandsliste und E-Mail-Benachrichtigungen.
- NMS Operation: Überwacht und sammelt automatisch Geräteinformationen, um Leistungsstatistiken zu erstellen, und sendet periodisch Berichte an die zentrale NMS Control. Ereignisse können direkt durch NMS Operation-Komponenten erkannt werden, oder die Geräte können Benachrichtigungen und Alarme senden. Änderungen, beispielsweise in der Gerätekonfiguration oder durch Firmware-Updates, werden durch NMS Control angestoßen und durch NMS Operation ausgeführt.

SINEC NMS unterstützt sowohl die lokale als auch die zentrale Benutzerverwaltung über UMC. Im Musterkonzept erfolgt die Benutzerauthentifizierung über UMC, was eine zentrale Benutzerverwaltung, die Integration von UMC-Benutzergruppen in SINEC NMS und die Unterstützung von Web Single Sign-On (Web SSO) ermöglicht. So können Benutzer zwischen den Webschnittstellen von NMS Control und NMS Operation wechseln, ohne sich mehrfach anmelden zu müssen.

Obwohl der UMC-Server zusammen mit SINEC NMS auf demselben PC installiert werden kann, werden sie in diesem Musterkonzept getrennt, um den Anforderungen der Netzwerksegmentierung zu entsprechen. NMS Control wird im „Externe Dienste“-Netzwerk bereitgestellt, um Webserver-Zugriff auf Unternehmensebene zu ermöglichen, während der UMC-Server im „Interne Dienste“-Netzwerk der DMZ ausgeführt wird.

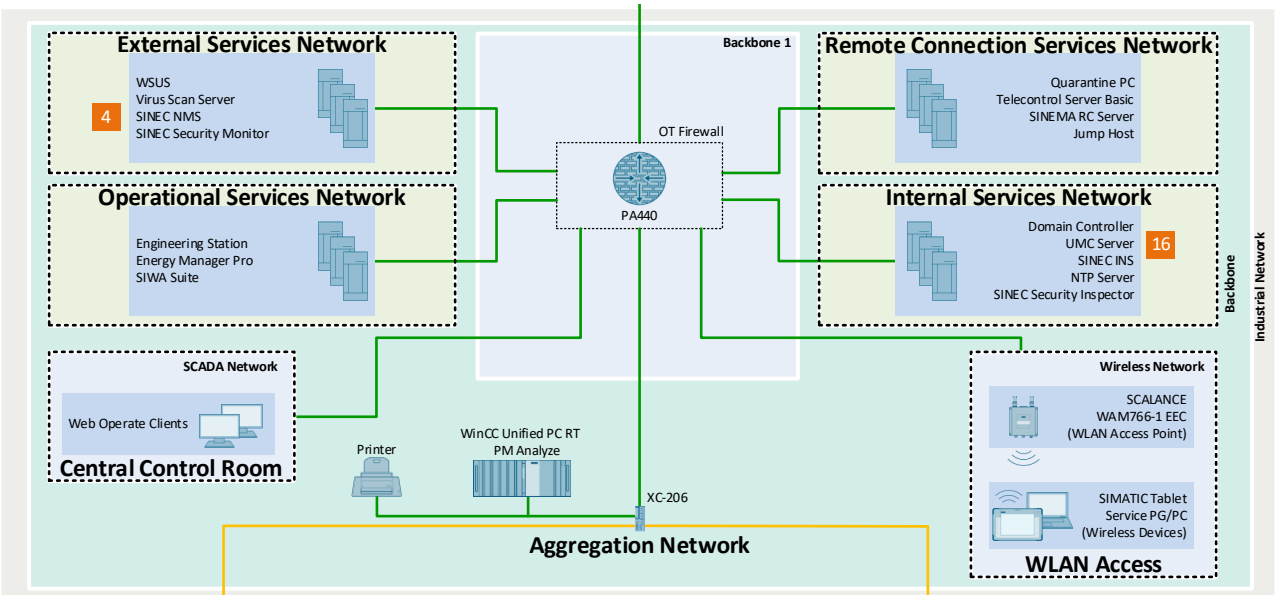

Abbildung 6-6: SINEC NMS und UMC-Server

HINWEIS **Einsatz von NMS Control**

Im Musterkonzept der Abwasserbehandlungsanlage wird NMS Control im „Externe Dienste“-Netzwerk gehostet, um Webserver-Zugriff auf Unternehmensebene zu ermöglichen. Falls SINEC NMS von überlagerten Netzwerken nicht zugänglich sein soll, sollte NMS Control im „Interne Dienste“-Netzwerk platziert werden.

Neben den in Abschnitt 6.9.1 genannten 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 beeinträchtigt werden kann.

Weitere Informationen zu SINEC NMS sind in den folgenden Dokumenten zu finden.

- \43\ – Netzwerkmanagement SINEC NMS
- \44\ – Erste Schritte mit SINEC NMS

6.9.5. SIMATIC Energy Manager Pro

SIMATIC Energy Manager Pro ist ein Energiemanagementsystem für die Industrie und nach ISO 50001 zertifiziert. Damit werden Energieströme und Verbrauchswerte in Prozessen detailgenau visualisiert. Diese Werte werden den relevanten Verbrauchern oder Kostenstellen zugeordnet, sodass Unternehmen den Energieverbrauch überwachen, steuern und optimieren können.

Neben den in Abschnitt 6.9.1 aufgeführten Härtungsmaßnahmen empfiehlt es sich, den Richtlinien im Installationshandbuch zu folgen.

- \50\ – „SIMATIC Energy Manager V7.2 – Installation“, Abschnitt 3 (Energy Manager installieren)

Weitere Informationen über SIMATIC Energy Manager Pro sind in den folgenden Dokumenten zu finden.

- \51\ – „SIMATIC Energy Manager PRO V7.5 – Bedienung“
- \52\ – „SIMATIC Energy Manager V7.5 – Acquisition“
- \53\ – „SIMATIC Energy Manager V7.5 – Systembeschreibung“

6.10. Automatisierungsgeräte

6.10.1. WinCC Unified Comfort Panels

WinCC Unified Comfort Panels werden in verschiedenen Prozesszellen innerhalb der Abwasserbehandlungsanlage eingesetzt, um den Betrieb zu überwachen und zu steuern. Basierend auf der in Abschnitt 4.3 durchgeführten Bedrohungs- und Risikoanalyse sind die folgenden Härtungsmaßnahmen erforderlich, um eine sichere Inbetriebnahme und einen sicheren Betrieb der MTP1000 Unified Comfort Panels zu gewährleisten.

Tabelle 6-17: Härtungsmaßnahmen für WinCC Unified Comfort Panels

Nr.	Sicherheitsthema	Härtungsmaßnahme	Dokumentation
1	Zugriffskontrolle	• Schutz des TIA Portal-Projekts • Lokalen und/oder globalen Benutzern nach dem Prinzip der geringsten Rechte Rollen zuweisen • Zugriffsschutz auf dem HMI-Panel aktivieren	\3\ – Abschnitt 2.1 \3\ – Abschnitt 2.6 \3\ – Abschnitt 3.4.1
2	Erweiterungsanschlüsse	Ungenutzte USB- und SD-Kartenschnittstellen deaktivieren	\3\ – Abschnitt 4.1.1
3	Netzwerksicherheit	• Ungenutzte Ports und Netzwerkadapter deaktivieren • Verschlüsselte Kommunikation verwenden, um Daten sicher mit Steuerungen, Engineering-Stationen und anderen Unified-Geräten auszutauschen	\3\ – Abschnitt 2.5 \3\ – Abschnitt 2.9 \3\ – Abschnitt 4.1.2
4	Protokollierung und Überwachung	Das Audit Trail-System verwenden, um nachzuweisen, welcher menschliche Benutzer welche Änderungen vorgenommen hat	\37\ – Audit Trail-System
5	Sichere Inbetriebnahme	• Projektübertragung im laufenden Betrieb deaktivieren • Verschlüsselte Projektübertragung während der Inbetriebnahme aktivieren	\3\ – Abschnitt 2.7.3

Abbildung 6-7: MTP1000 Unified Comfort

Weitere Härtungsmaßnahmen im Zusammenhang mit der Nutzung von Diensten und Anwendungen sind im Security Leitfaden für WinCC Unified zu finden.

- \3\ – „Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices“, Section 5 (Risk analysis when using services and apps)

6.10.2. SIMATIC-Controller

SIMATIC S7-1200 Basic Controller und SIMATIC ET 200SP Distributed Controller werden im Musterkonzept zur Steuerung der Prozesse des Abwassersystems, der mechanischen Behandlung, der biologischen Behandlung und der Schlammbehandlung eingesetzt.

Die folgenden Härtungsmaßnahmen gelten für alle SIMATIC-Controller, die im Musterkonzept verwendet werden.

Tabelle 6-18: Härtungsmaßnahmen für SIMATIC-Controller

Nr.	Sicherheitsthema	Härtungsmaßnahme	Dokumentation
1	Zugriffskontrolle	Zugriffskontrolle aktivieren, um den Benutzerzugriff auf bestimmte SPS-Funktionalitäten einzuschränken	\56\ – Abschnitt 1.3
2	Sichere Kommunikation	Einsatz von sicheren Kommunikationsmethoden: • Nur sichere PG/PC- und HMI-Kommunikation zulassen • Sign&Encrypt für die OPC UA-Kommunikation verwenden • Secure Open User Communication (OUC) mit TLS v1.3 verwenden	\55\ – Abschnitt 2.2 \57\ – Abschnitt 2.4 \57\ – Abschnitt 2.6 \57\ – Abschnitt 2.7
3	Schutz der vertraulichen Konfigurationsdaten der SPS	Passwortbasierten Schutz zur Verschlüsselung vertraulicher Projektierungsdaten der SPS aktivieren	\55\ – Abschnitt 2.3

HINWEIS

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.

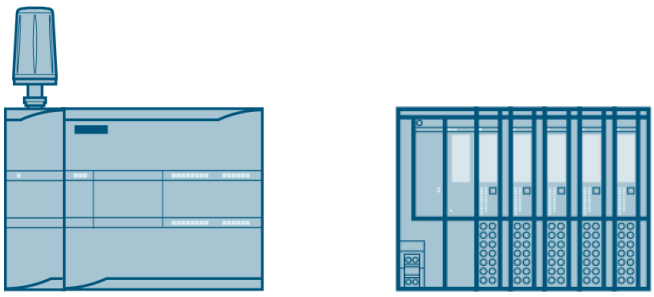

Abbildung 6-8: CPU 1214C mit CP 1243-7 LTE und ET 200SP Distributed Controller

6.10.3. Dezentrale Peripherie

Die dezentrale Peripherie wird eingesetzt, um Sensoren und Stellantriebe auf Feldebene über die PROFINET IO-Kommunikation mit den Steuerungen zu verbinden. Die Härtungsmaßnahmen für diese Geräte orientieren sich an den Spezifikationen der PROFINET Security Class 1.

Nr.	Sicherheitsthema	Härtungsmaßnahme	Dokumentation
1	GSD-Dateien	GSDX zur Sicherstellung der Integrität und Authentizität von GDS-Dateien während des Imports	\58\ – Security Class 1 for PROFINET Security, Section 4
2	SNMP	Deaktivierung von SNMP	\58\ – Security Class 1 for PROFINET Security, Section 5
3	DCP	Festlegung des DCP-Modus auf schreibgeschützt	\58\ – Security Class 1 for PROFINET Security, Section 6

Abbildung 6-9: IM 155-6 PN BA

6.10.4. Remote Terminal Units

Remote Terminal Units (RTUs) werden zum Überwachen und Steuern von Außenstationen ohne Anschluss an das Stromversorgungsnetz eingesetzt. RTUs unterstützen die folgenden Kernfunktionen.

- Energiesparbetrieb
- Prozessanschluss – über die vorhandenen Ein- und Ausgänge und über eine Erweiterungskarte
- Steuerung – für einfache Steuerungsaufgaben
- Speichern/Protokollieren von Prozessdaten – wenn keine Verbindung zum Kommunikationspartner besteht
- TeleControl-Kommunikationsprotokolle
- Positionsbestimmung und Zeitsynchronisation über GPS

Die Härtungsmaßnahmen für die Remote Terminal Unit RTU 3051C des Musterkonzepts sind in Abschnitt 6.7 definiert.

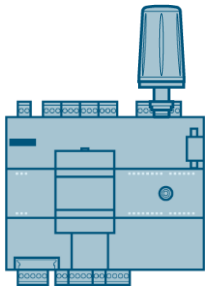

Abbildung 6-10: RTU 3051C

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 Domain-Benutzerkonten 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.

7.1. Domain Controller

Der Domain Controller im Musterkonzept wird innerhalb des „Interne Dienste“-Netzwerks der DMZ gehostet. Diese Platzierung gewährleistet einen sicheren und kontrollierten Zugriff – über die OT-Firewall – auf Authentifizierungs- und Verzeichnisdienste für Geräte, Anwendungen, Server und Workstations, die sich sowohl in der DMZ als auch in den Aggregationsnetzwerken befinden.

Durch die Zentralisierung der Benutzerverwaltung im „Interne Dienste“-Netzwerk der DMZ kann eine einheitliche Durchsetzung von Richtlinien in der gesamten OT-Umgebung erreicht werden.

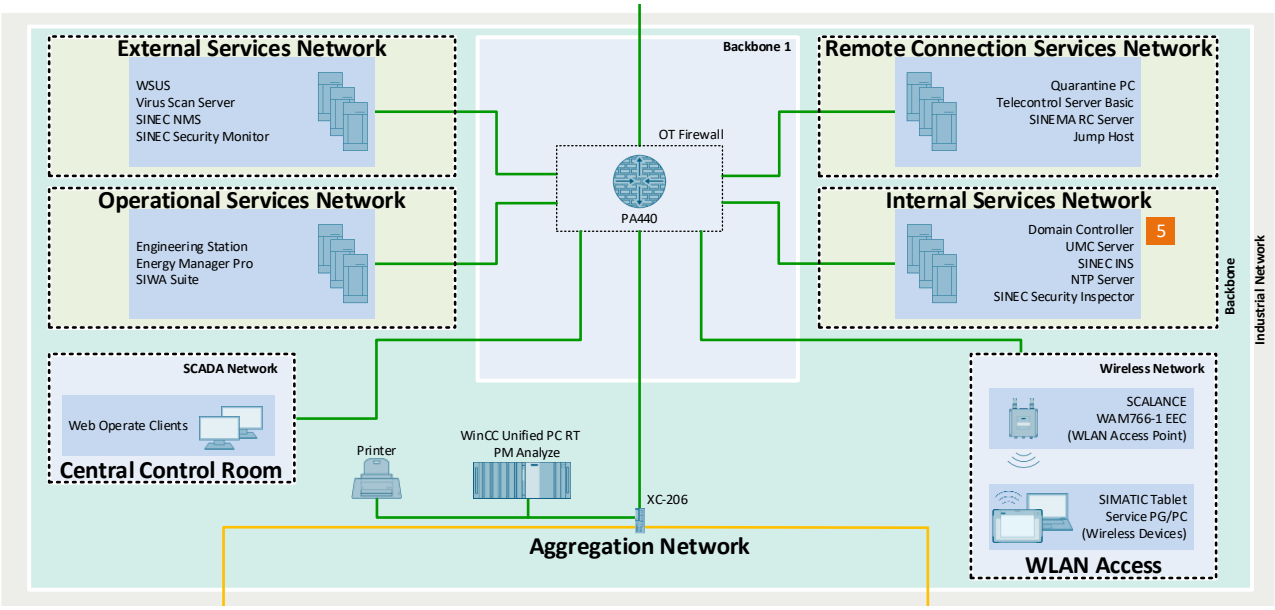

Abbildung 7-1: Domain Controller im Musterkonzept einer Abwasserbehandlungsanlage

7.2. User Management Component

Mit der User Management Component lässt sich ein zentrales System zur Verwaltung von Benutzern und Benutzergruppen über verschiedene Siemens-Software und -Geräte hinweg einrichten. Sie kann in Microsoft Active Directory integriert werden, sodass vorhandene Benutzer und Gruppen importiert und synchronisiert werden können.

7.2.1. UMC-Ring-Server

Der UMC-Ringserver dient als zentrale Konfigurationsplattform für die Benutzerverwaltung innerhalb der UMC-Domain und befindet sich im „Interne Dienste“-Netzwerk. Auf diesem Server sind Benutzer mit den entsprechenden Gruppenzuweisungen für die UMC-Domain definiert. Um die Übertragung von Benutzern und Gruppen aus dem Active Directory zu ermöglichen, muss der UMC-Ring-Server-PC zur AD-Domain hinzugefügt werden.

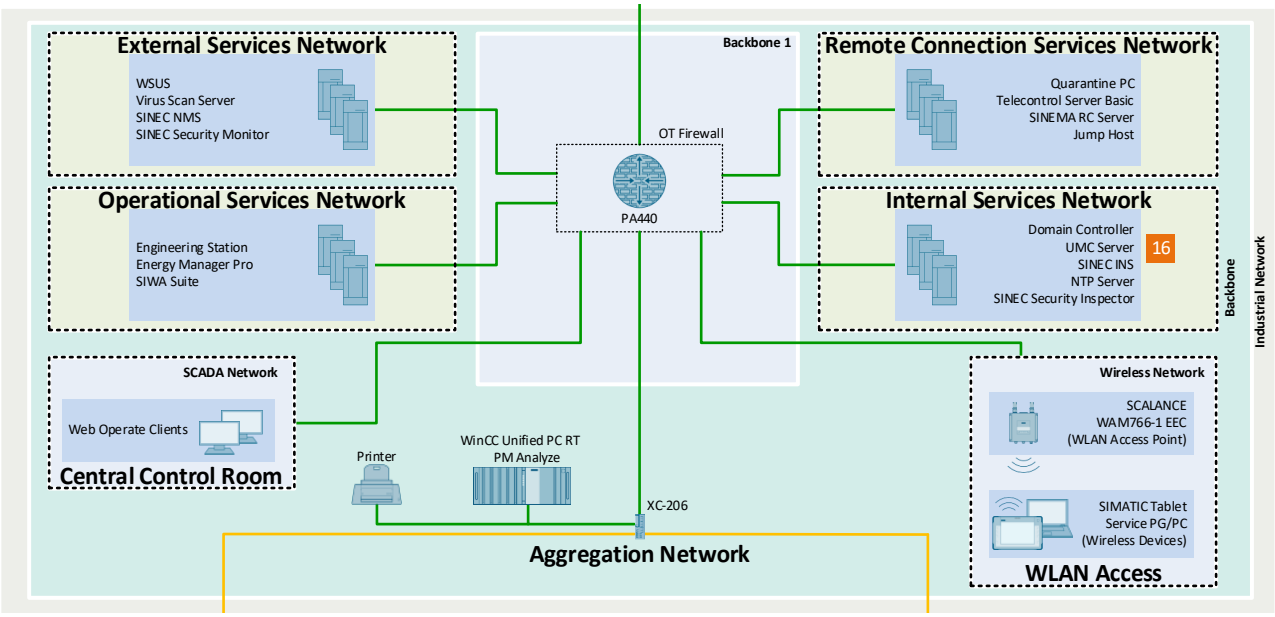

Abbildung 7-2: UMC-Ring-Server im Musterkonzept einer Abwasserbehandlungsanlage

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

- \18\ – Zentrales Benutzermanagement mit der „User Management Component (UMC)“

7.3. Authentifizierung und Autorisierung der Benutzer für WinCC Unified

WinCC Unified bietet sichere Mechanismen, um sicherzustellen, dass nur authentifizierte Benutzer auf das System zugreifen können und dass ihre Aktionen entsprechend ihrer zugewiesenen Rollen eingeschränkt sind. Die Authentifizierung, mit der die Identität der Benutzer überprüft wird, kann entweder lokal oder zentral über UMC abgewickelt werden. Die Autorisierung, die festlegt, was authentifizierte Benutzer tun dürfen, wird immer lokal auf dem Laufzeitgerät durchgesetzt.

Die rollenbasierte Zugriffskontrolle, die sich am Prinzip der geringsten Rechte orientiert, stellt sicher, dass Benutzer nur die für die Ausführung ihrer jeweiligen Aufgaben erforderlichen Engineering-/Laufzeitrechte erhalten. Rollen können entweder vordefiniert sein – HMI-Bediener, HMI-Administrator, HMI-Monitor, HMI-Monitor-Client – oder individuell definiert werden, um spezifischen betrieblichen Anforderungen gerecht zu werden.

Im Musterkonzept der Abwasserbehandlungsanlage wird die zentrale Authentifizierung mithilfe von UMC in Verbindung mit Microsoft Active Directory implementiert. Dabei melden sich die Benutzer mit ihren Domain-Anmeldedaten an, und Benutzer- und Gruppeninformationen werden zwischen der AD-Domain und dem UMC-Ring-Server synchronisiert.

- \54\ – „Benutzer und Rollen projektieren (RT Unified)“

7.3.1. Vorteile der Verwendung von Active Directory und UMC für die Benutzerauthentifizierung

Ein Active Directory-System ermöglicht die Durchsetzung von Passwortrichtlinien über den Gruppenrichtlinien-Editor. Bei erzwungenen Einstellungen müssen alle Benutzer die definierten Sicherheitsstandards einhalten, wodurch das technische TIA Portal-Projekt und WinCC Unified-Geräte vor Schwachstellen in Verbindung mit schwachen Passwörtern geschützt werden.

Neben der Durchsetzung von Passwortrichtlinien ermöglicht ein Active Directory-basierter Mechanismus zur Benutzerauthentifizierung die Synchronisierung von Benutzern und Gruppen innerhalb einer Domain. Dies erleichtert die Benutzerverwaltung und -administration. Mit UMC kann die Benutzerauthentifizierung zentral verwaltet werden, sodass keine individuellen TIA Portal-Downloads auf jedem WinCC Unified Panel bzw. jede PC RT mehr erforderlich sind.

8. Schutz gegen Schadprogramme und Application Control

Die Integrität des Systems muss gegen unbefugte Änderungen an Software und Daten geschützt werden, und solche Änderungen müssen erkannt, aufgezeichnet und gemeldet werden. Im Musterkonzept wird der Schutz gegen Schadprogramme und unbefugte Änderungen durch den Einsatz von Antivirensoftware und Whitelisting-Technologien implementiert.

Antivirensoftware

Die Workstations und Server des Musterkonzepts arbeiten mit der neuesten Version von Trellix Endpoint Security (ENS) Trellix Endpoint Security ist mehr als eine herkömmliche Antivirensoftware, da es zusätzliche erweiterte Funktionen bietet. Diese sind im Datenblatt des Produkts aufgeführt.

- \24\ – Datenblatt zu Trellix Endpoint Security

Whitelisting von Software

Die Workstations und Server des Musterkonzepts arbeiten mit der neuesten Version von Trellix Application and Change Control.

- Trellix Application Control kann dafür genutzt werden, den Start unzulässiger oder unbekannter Anwendungen zu blockieren. Nach der Installation und Aktivierung von Trellix Application Control sind alle ausführbaren Anwendungen und Dateien gegen Modifikation geschützt.

  Im Gegensatz zu einfachen Ausnahmelisten-Konzepten verwendet Trellix Application Control ein dynamisches Vertrauenswürdigkeitsmodell. Dadurch entfallen die langwierigen, manuellen Aktualisierungen von Listen zugelassener Anwendungen. Aktualisierungen der autorisierten Anwendungen in der Liste können integriert werden durch:

  - Vertrauenswürdige Benutzer
  - Vertrauenswürdige Hersteller
  - Vertrauenswürdige Verzeichnisse
  - Binäre Dateien
  - Aktualisierungsprogramme wie Windows Update oder Virenscanner

  Darüber hinaus bietet Trellix Application Control Funktionen, die den Hauptspeicher überwachen, im Hauptspeicher ausgeführte Dateien schützen und Schutz vor Pufferüberläufen bieten.
- Trellix Change Control verhindert unbefugte Änderungen an wichtigen Systemdateien, Verzeichnissen und Projektierungen und vereinfacht gleichzeitig die Implementierung neuer Richtlinien und Konformitätsmaßnahmen. Es bietet Funktionen zur Überwachung der Dateiintegrität und zur Verhinderung von Änderungen, setzt Änderungsrichtlinien durch und überwacht kontinuierlich kritische Systeme. Darüber hinaus erkennt und blockiert es unerwünschte Änderungen an dezentralen und fernen Standorten.

Zentrales Sicherheitsmanagement

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 im „Externe Dienste“-Netzwerk der DMZ installiert. Dies vereinfacht die Verwaltung und Durchsetzung von Richtlinien auf den Workstations und Servern.

- \23\ – Trellix Endpoint Security
- \25\ – Trellix Application and Change Control
- \26\ – Trellix ePolicy Orchestrator

9. Patchmanagement

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 wichtige Maßnahme zum Schutz der Integrität eines Automatisierungs- und Leitsystems ist das Patchmanagement, das Teil der ganzheitlichen Sicherheitsstrategie ist.

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

- Patches für das Betriebssystem Microsoft Windows: Diese Kategorie beinhaltet Aktualisierungen, Servicepacks, Featurepacks und ähnliche Installationen aller Art, unabhängig davon, ob diese mit Sicherheit zu tun haben.
- Sicherheitsaktualisierungen für Microsoft Windows: Diese Aktualisierungen beziehen sich speziell auf sicherheitsrelevante Probleme.
- Patches für Firmware und Software: Diese Patches beseitigen Schwachstellen in Software und Produkten von Siemens sowie Fremdkomponenten.

Bei Software und Produkten von Siemens werden Sicherheitsschwachstellen von der verantwortlichen Siemens-Produkteinheit abgewickelt. Dies gilt auch für Schwachstellen von Fremdkomponenten in Siemens-Produkten. Bei Fremdkomponenten, die sich nicht im Eigentum von Siemens befinden, trägt jedoch der Anlagenbetreiber die Verantwortung dafür, dass diese Komponenten über ihren gesamten Lebenszyklus hinweg mit den neuesten Patches stets auf dem aktuellen Stand gehalten werden.

Siemens veröffentlicht monatlich Hinweise für alle Produkte, einschließlich Fremdkomponenten.

- \19\ – Siemens ProductCERT and Siemens CERT

9.1. Patchmanagement für Microsoft Windows

Der Infrastruktur-PC in der DMZ verwaltet die Windows-Patches für das Automatisierungs- und Leitsystem. Im Folgenden sind einige der Tools zum Verwalten von Windows-Patches aufgeführt.

Windows Server Update Service (WSUS)

Der WSUS wird auf dem Infrastruktur-PC installiert und kann Windows-Patches entweder vom Microsoft Update-Server oder vom Server im Unternehmensnetzwerk erhalten. Der WSUS verteilt die Patches an alle Windows-basierten PCs des Automatisierungs- und Leitsystems.

HINWEIS **Ankündigung der Einstellung von WSUS im Jahr 2025**

Microsoft hat 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.

Windows Autopatch, Microsoft Intune und Azure Update Manager

Zwar bleibt der WSUS-Dienst in Windows Server 2025 verfügbar, Microsoft empfiehlt Organisationen jedoch den Umstieg auf Cloud-Tools wie Windows Autopatch und Microsoft Intune für die Verwaltung von Client-Updates sowie Azure Update Manager für die Verwaltung von Server-Updates.

- \20\ – Microsoft Autopatch
- \21\ – Microsoft Intune
- \22\ – Azure Update Manager

9.2. Patchmanagement für Automatisierungs- und Netzwerkkomponenten

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

- \59\ – Updates für SIMATIC WinCC Unified PC Runtime V20
- \60\ – Image-Downloads für SIMATIC HMI Bediengeräte: Unified Comfort Panels
- \61\ – Firmware-Update S7-1500 CPUs inkl. Displays und ET 200 CPUs (ET 200SP, ET 200pro)
- \62\ – Firmware-Update für CPU 1214C, DC/DC/DC, 14DI/10DO/2AI

10. Sicherung und Wiederherstellung

Die Fähigkeit zur Wiederherstellung und Zurückversetzung eines Automatisierungs- und Leitsystems (IACS) in einen bekannten, betriebsfähigen Zustand nach einer Störung oder einem Ausfall ist ein wichtiger Aspekt im Konzept „Defense-in-Depth“ und wird in der Norm IEC 62443 empfohlen.

Bei einer Strategie zur Sicherung und Wiederherstellung ist es wichtig, alle notwendigen Daten für das Zurückversetzen des IACS in einen bekannten Zustand und ihren Speicherort im System zu identifizieren. Die Häufigkeit der Speicherung von Sicherheitskopien, die Art der Sicherung (komplett, differentiell oder inkremental) und der Speicherort der Sicherungskopien werden in dieser Strategie beschrieben.

Systemsicherung

Eine Systemsicherung stellt ein vollständiges Abbild des Systems dar, z. B. eine Momentaufnahme oder einen „Schnappschuss“ des aktuellen Systems zu einem bestimmten Zeitpunkt. Dabei werden die folgenden Daten einbezogen:

- Hardwarespezifische Dateien, z. B. 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

Sicherung der TIA Portal-Projekte, mit denen die WinCC Unified-Visualisierungssysteme und Automatisierungsgeräte, wie z. B. die S7-1200-SPSen und ET 200SP Distributed Controller, projektiert wurden.

Komponentenspezifische Daten

Komponentenspezifische Sicherungen umfassen Daten wie Datenbanken oder die individuelle Projektierung eingebetteter Geräte oder Netzwerkgeräte.

Für WinCC Unified Panels stehen folgende Sicherungsmechanismen zur Verfügung.

- Sichern & Wiederherstellen: Vollständige Sicherung der Panel-Daten, die auf einem Gerät desselben Modells wiederhergestellt werden können. Die Sicherungsdatei kann nicht bearbeitet werden und enthält alle Projektierungsdaten.
- Automatische Sicherung: Kontinuierliche, automatisierte Sicherung prozessbezogener Daten auf einer SIMATIC HMI-SD-Speicherkarte.

Bei SCALANCE-Netzwerkgeräten werden Sicherungs- und Wiederherstellungsvorgänge über das SINEC NMS-Konfiguration-Verzeichnis verwaltet.

- \3\ – „Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices“, Section 4.1.4 (Backup and restoration of panel data)
- \43\ – Netzwerkmanagement SINEC NMS, Abschnitt 4.5 (Gerätekonfiguration-Verzeichnis)
- \44\ – Getting Started: SINEC NMS verstehen und anwenden – Weiterführende Dokumentation (Sicherung)

HINWEIS **Bereitschaft zur Systemwiederherstellung**

Eine Wiederherstellung von Systemen ist oft kritischer als die Anfertigung von Sicherheitskopien. Wiederherstellungsprozesse müssen im Voraus getestet werden und reproduzierbar sein, um die Systemverfügbarkeit in Notfällen zu gewährleisten und Ausfallzeiten zu minimieren.

10.1. Entsorgung von Komponenten

Sensible Daten wie Passwörter, kryptographisches Material und Konfigurationen können missbraucht werden, wenn sie unbefugten Personen zugänglich gemacht werden. Asset-Eigner müssen alle Kundeninformationen auf den Geräten, die nicht mehr benötigt werden, sicher löschen.

Diese Anforderung gilt für alle Geräte, auch Wechselmedien.

Tabelle 10-1: Entsorgung von Komponenten, die sensible und vertrauliche Kundendaten enthalten

Gerät	**Kunden-/vertrauliche Informationen**	**Entsorgung der Komponente**
Eingebettete Geräte	Benutzerprogramm, Skripte, kryptographische Schlüssel usw.	SPSen und HMI-Panels auf die Werkseinstellungen zurücksetzen und den Flash-Speicher sicher löschen.
Netzwerkgeräte	Firewall-Regeln	SCALANCE-Komponenten auf den Werkszustand zurücksetzen. SINEC NMS kann Resets über bestimmte Geräteprofile durchführen.
Speichermedien	Je nach Nutzung	USB-Laufwerke, CDs, DVDs und andere Medien müssen vollständig gelöscht oder zur sicheren Entsorgung abgegeben werden (z. B. Schreddern).
Hosts	Konfiguration, Passwörter, kryptographische Schlüssel usw.	Vollständige Systeme, z. B. IPCs, müssen zur sicheren Entsorgung abgegeben werden.

11. Anhang

11.1. 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:

11.2. Links und Literatur

Nr.	Thema
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link zur Beitragsseite dieses Anwendungsbeispiels https://support.industry.siemens.com/cs/ww/de/view/109780322
\3\	Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices https://support.industry.siemens.com/cs/ww/de/view/109481300
\4\	Certification and standards „TÜV Süd certification based on IEC 62443“ https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity/certification-standards.html
\5\	IEC 62443-4-1 Secure product development lifecycle https://assets.new.siemens.com/siemens/assets/api/uuid:b78aadd6-2ec7-44e6-9fd1-e221f4c2a988/secure-product-development-lifecycle-iec62443-4-1-en.pdf
\6\	SIMATIC S7-1500 Redundantes System S7-1500R/H https://support.industry.siemens.com/cs/ww/de/view/109754833
\7\	Anbindung von WinCC Unified an die zentrale Benutzerverwaltung (UMC) https://support.industry.siemens.com/cs/ww/de/view/109780337
\8\	Siemens Industrial Cybersecurity Services https://www.siemens.com/global/en/products/services/digital-enterprise-services/industrial-security-services.html
\9\	Continuous endpoint protection against malware https://www.siemens.com/in/en/products/services/digital-enterprise-services/industrial-security-services/endpoint-protection.html
\10\	Checkliste für die Einrichtung von SCALANCE-Geräten https://support.industry.siemens.com/cs/ww/de/view/109745536
\11\	PAN-OS Administrator’s Guide https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/getting-started
\12\	Palo Alto – PAN-OS https://docs.paloaltonetworks.com/pan-os
\13\	Palo Alto – Best Practices for Securing Administrative Access section https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/getting-started/best-practices-for-securing-administrative-access
\14\	Benutzerverwaltung für SCALANCE-Geräte mit RADIUS-Protokoll https://support.industry.siemens.com/cs/ww/de/view/98210507
\15\	Rundum-Schutz mit Industrial Security – Systemintegrität https://support.industry.siemens.com/cs/ww/de/view/92605897
\16\	Rundum-Schutz mit Industrial Security – Netzwerksicherheit https://support.industry.siemens.com/cs/ww/de/view/92651441
\17\	Rundum-Schutz mit Industrial Security – Anlagensicherheit https://support.industry.siemens.com/cs/ww/de/view/50203404
\18\	Zentrales Benutzermanagement mit der „User Management Component (UMC)“ https://support.industry.siemens.com/cs/ww/de/view/109780337

Nr.	Thema
\19\	Siemens ProductCERT and Siemens CERT https://www.siemens.com/global/en/products/services/cert.html
\20\	Windows Autopatch https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/overview/windows-autopatch-overview
\21\	Microsoft Intune https://learn.microsoft.com/en-us/mem/intune-service/fundamentals/what-is-intune
\22\	Azure Update Manager https://azure.microsoft.com/en-us/products/azure-update-management-center
\23\	Trellix Endpoint Security https://www.trellix.com/products/endpoint-security
\24\	Datenblatt zu Trellix Endpoint Security https://www.trellix.com/assets/data-sheets/trellix-endpoint-security-datasheet.pdf
\25\	Trellix Application and Change Control https://www.trellix.com/products/trellix-application-control
\26\	Trellix ePolicy Orchestrator https://www.trellix.com/products/epo
\27\	SIMATIC RTU 3051C – 6NH3112-5BB00-0XX0 https://mall.industry.siemens.com/mall/en/ww/Catalog/Product/?mlfb=6NH3112-5BB00-0XX0&SiepCountryCode=WW
\28\	SIMATIC NET TeleControl - RTU SIMATIC RTU 3030C/RTU 30x1C https://support.industry.siemens.com/cs/ww/de/view/109986730
\29\	CP 1243-7 LTE EU – 6GK7243-7KX30-0XE0. Anbindung eines SIMATIC S7-1200 an das LTE-Netz im europäischen Frequenzbereich https://mall.industry.siemens.com/mall/en/ww/Catalog/Product/?mlfb=6GK7243-7KX30-0XE0&SiepCountryCode=WW
\30\	SIMATIC NET: S7-1200 - TeleControl CP 1243-7 LTE https://support.industry.siemens.com/cs/ww/de/view/109476704
\31\	CP 1542SP-1 IRC – 6GK7542-6VX00-0XE0. Anbindung eines SIMATIC S7-ET 200SP über Industrial Ethernet, SINAUT ST7, TeleControl Server Basic, IEC 60870-5-104 oder DNP3-Protokoll an eine Leitstelle https://mall.industry.siemens.com/mall/en/ww/Catalog/Product/?mlfb=6GK7542-6VX00-0XE0&SiepCountryCode=WW
\32\	SIMATIC NET: ET 200SP - Industrial Ethernet CP 1542SP-1, CP 1542SP-1 IRC, CP 1543SP-1 https://support.industry.siemens.com/cs/ww/de/view/109977935
\33\	SCALANCE MUM853-1 – 6GK5853-2EA00-2DA1. 5G-Router für die drahtlose Kommunikation über öffentliche 3/4/5G-Mobilfunk-Netze und private 5G-Netze https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6GK5853-2EA00-2DA1
\34\	SIMATIC NET Industrial Ethernet Security SINEC Security Monitor Operating Instructions https://support.industry.siemens.com/cs/ww/de/view/109982510
\35\	Netzwerkkonzepte für industrielle Automatisierungsnetzwerke https://support.industry.siemens.com/cs/ww/de/view/109802750
\36\	Palo Alto – DoS and Zone Protection Best Practices https://docs.paloaltonetworks.com/best-practices/dos-and-zone-protection-best-practices
\37\	SIMATIC WinCC Unified Online-Dokumentation: WinCC Audit (RT Unified) https://docs.tia.siemens.cloud/r/en-us/v20/wincc-audit-rt-unified

Nr.	Thema
\38\	Meldungen einer SIMATIC S7-1200/S7-1500 CPU per Syslog an SINEC INS senden https://support.industry.siemens.com/cs/ww/en/view/51929235
\39\	SIMATIC S7-1500/ET 200MP, S7-1500R/H, Drive Controller, S7-1500 Software Controller, ET 200SP, ET 200pro Syslog Messages https://support.industry.siemens.com/cs/ww/en/view/109823696
\40\	SIMATIC NET Netzwerkmanagement SINEC INS https://support.industry.siemens.com/cs/ww/en/view/109978415
\41\	SIMATIC NET Industrial Ethernet Security SCALANCE SC-600 https://support.industry.siemens.com/cs/ww/en/view/109954186
\42\	SIMATIC NET Industrial Ethernet Switches SCALANCE Layer 2 Switches https://support.industry.siemens.com/cs/ww/en/view/109977339
\43\	SIMATIC NET Netzwerkmanagement SINEC NMS https://support.industry.siemens.com/cs/ww/en/view/109973629
\44\	Getting Started: SINEC NMS verstehen und anwenden https://support.industry.siemens.com/cs/ww/en/view/109762792
\45\	SIMATIC NET Industrial Ethernet Security SINEC Security Inspector https://support.industry.siemens.com/cs/ww/en/view/109988448
\46\	SINEC Security Guard https://xcelerator.siemens.com/global/en/all-offerings/products/s/sinec-security-guard.html
\47\	Empfohlene Sicherheitseinstellungen für IPCs im Industrieumfeld (Windows) https://support.industry.siemens.com/cs/ww/en/view/109475014
\48\	SIMATIC IPC – Security Leitfaden für Linux-Systeme https://support.industry.siemens.com/cs/ww/en/view/109768383
\49\	PM-ANALYZE Systembeschreibung https://cache.industry.siemens.com/dl/files/856/109782856/att_1036486/v2/PM-ANALYZE_Systemdescription.pdf
\50\	SIMATIC Energy Manager V7.2 – Installation https://support.industry.siemens.com/cs/ww/en/view/109742441
\51\	SIMATIC Energy Manager PRO V7.5 – Operation https://support.industry.siemens.com/cs/ww/en/view/109963217
\52\	SIMATIC Energy Manager V7.5 – Acquisition https://support.industry.siemens.com/cs/ww/en/view/109963216
\53\	SIMATIC Energy Manager V7.5 – Systembeschreibung https://support.industry.siemens.com/cs/ww/en/view/109811736
\54\	SIMATIC WinCC Unified Online-Dokumentation: Benutzer und Rollen projektieren (RT Unified) https://docs.tia.siemens.cloud/r/en-us/v20/configuring-users-and-roles-rt-unified
\55\	Konfiguration der Sicherheitsfunktionen in TIA Portal V17 https://support.industry.siemens.com/cs/ww/en/view/109798583
\56\	Benutzerverwaltung & Zugriffssteuerung mit TIA Portal V19 https://support.industry.siemens.com/cs/ww/en/view/109973173

Nr.	Thema
\57\	Zertifikate mit TIA Portal verwenden https://support.industry.siemens.com/cs/ww/en/view/109769068
\58\	PROFINET Security https://profinet.co.uk/profinet-security/
\59\	Updates für SIMATIC WinCC Unified PC Runtime V20 https://support.industry.siemens.com/cs/ww/de/view/109963700
\60\	Image-Downloads für SIMATIC HMI Bediengeräte: Unified Comfort Panels https://support.industry.siemens.com/cs/ww/en/view/109825605
\61\	Firmware-Update S7-1500 CPUs inkl. Displays und ET 200 CPUs (ET 200SP, ET 200pro) https://support.industry.siemens.com/cs/ww/en/view/109478459
\62\	Firmware-Update für CPU 1214C, DC/DC/DC, 14DI/10DO/2AI https://support.industry.siemens.com/cs/ww/de/view/107539750

11.3. Änderungsdokumentation

Version	Datum	Änderung
V1.0	09/2025	Erste Ausgabe

