



WUPPERVERBAND

für Wasser, Mensch und Umwelt

**Projektierungsrichtlinie Leit- und
Automatisierungstechnik
für
Planung und Ausführung**

Wuppertal



Dokumenten-Administration

Version	Ausgabedatum	Editor(en)	Bemerkung
1.0	10.05.2021	Rinne	Vorabversion Entwicklungsphase
1.1	15.08.2023	Barttels	Kleine Ergänzungen im Bereich LWL und Netzwerk/ Bustechnik
1.2	13.09.2023	Rinne	Ergänzungen Bedienstationen, Sonderbauwerke
1.3		Rinne	Ergänzungen Alarmmanagement
1.4	26.02.2024	Franz	Sonderbauwerke
1.5	04.04.2024	Klasen	Restrukturierung der Richtlinie
1.5.1	16.05.2024	Barttels	Ergänzung zur Angriffserkennung (SzA), teilweise Strukturierung angepasst
1.5.2	31.05.2024	Wellershaus	Ergänzungen und Klarstellungen aus dem letzten Arbeitsterminen Ergänzung SIMATIC Shell Einstellung
1.5.3	31.05.2024	Rinne	Anpassung Skizze MRP-Ring Feldbus
1.5.4	01.08.2024	Wellershaus	div. Schärfungen und Klärungen

Inhaltsverzeichnis

1	Geltungsbereich.....	4
2	Allgemeine Bestimmungen.....	5
3	Grundlagen System-Peripherie	6
3.1	Verkabelung.....	6
3.1.1	Primärverkabelung	6
3.1.2	Sekundärverkabelung.....	6
3.1.3	Tertiärverkabelung.....	7
3.2	Netzwerk Topologie	7
3.2.1	Systembus.....	7
3.2.2	Terminalbus	8
3.2.3	Redundanzbus	8
3.2.4	Feldbus-Systeme.....	9
3.2.5	Weitere Netzwerke.....	10
3.3	Technische Räume	11
3.3.1	Serverschränke	11
3.3.2	Farbkodierung Netzkabel (Kupfer) in Serverschränken	13
3.4	Dokumentation.....	15
4	Automatisierungs-/Prozessleitsystem	16
4.1	Prinzipieller Aufbau der PCS 7 - Systeme	17
4.2	PCS7-Systembestandteile Server-Ebene.....	18
4.2.1	PC-Hardwareausbau	19
4.2.2	Zentrales System- und Asset-Management.....	20
4.3	IP-Adressen.....	20
4.4	Lizensierung und Mengengerüst	20
4.5	PCS7 Automatisierungsstationen	21
4.5.1	Hardware	21
4.6	Engineering.....	22
4.6.1	AS – Engineering.....	23
4.6.2	OS – Engineering.....	25



4.6.3	Kurzzeitarchivierung (Alarm- und TagLogging)	26
4.6.4	Langzeitarchivierung der Archive	26
4.6.5	PCS7 Berechtigungskonzept	26
4.7	Bedienstationen	27
4.7.1	Software Bedienstationen	27
4.7.2	Vor-Ort Bedienstationen..... Fehler! Textmarke nicht definiert.	
4.8	Prozessbilder.....	28
4.9	Alarmmanagement.....	30
4.9.1	Sonderbauwerke.....	30
4.10	System zur Angriffserkennung (SzA).....	31
4.10.1	Ausleitung Log	31
4.10.2	Ausleitung Datenverkehr.....	31
5	Abbildungsverzeichnis.....	33



1 Geltungsbereich

Diese Projektierungsrichtlinie gilt für alle Projekte der Leit- und Automatisierungstechnik im Zusammenhang mit dem Prozessleitsystem Siemens Simatic PCS 7 innerhalb von Anlagen des Wuppertal Wasser- und Umweltverbandes.

Ferner gilt dieses Dokument als Planungsrichtlinie für alle netzwerktechnisch-relevanten Baumaßnahmen.



2 Allgemeine Bestimmungen

Alle neu errichteten Anlagen müssen den zum Zeitpunkt der Errichtung gültigen Richtlinien und Vorschriften der DIN VDE, DIN sowie den IT-Sicherheitskonzepten entsprechen.

Darüber hinaus gelten folgende betriebsspezifische Vorgabedokumente:

- Brandschutzkonzept
- MSR-Kennzeichnung
- ...

In diesem Dokument werden die Grundlagen, verbindliche Festlegungen und Definitionen in Verbindung mit gültigen Normen und Ausführungsrichtlinien für die Einführung und Nutzung eines wuppertal-verbands-einheitlichen Prozessleitsystems auf Basis von Siemens Simatic PCS 7 beschrieben.

Die Vorgaben des Wuppertal-verbands sind einzuhalten und der Stand der Technik in Bezug auf IT-Sicherheit ist umzusetzen.

Das IT-Sicherheitskonzept des Wuppertal-verbands basiert auf dem branchenspezifischen Standard (B3S) für den KRITIS Sektor Wasser/Abwasser bzw. auf dem BSI-Grundschutzkatalog.

Umsetzungsabweichungen von dieser Richtlinie müssen von einem Fach-Verantwortlichen des Wuppertal-verbands genehmigt werden.

3 Grundlagen System-Peripherie

3.1 Verkabelung

In allen Fällen ist ein LWL Messprotokoll (ODTR) anzufertigen.

Die Verkabelung wird gem. EN50173 in folgende Abschnitte unterteilt:

3.1.1 Primärverkabelung

Die Primärverkabelung der Gebäudeanschlüsse ist generell mit gleichartigen Lichtwellenleiterkabeln (LWL) auszuführen. Die LWL-Außenkabel sind mit separater Trassenführung zu verlegen. Die zu verlegenden LWL-Kabel werden wie folgt spezifiziert:

- LWL-Standardkabel mit mindestens 24 Fasern 50/125µm im Multimodekabel (OM4)
- Längswasserdicht
- Als Multimode-Fasern sind laseroptimierte OM4-Fasern nach EN50173 (akt. Ausgabe) bzw. ISO/ICE11802 zu verwenden.
- Verbindungsart Spleißen, vorzugsweise Metz Connect OpDat 4HE (wenn weniger als 3HE erforderlich können 19“-Spleißbox mit 24 Duplex-LC-Buchsen auf 1HE verwendet werden)
- Im Primär-Bereich ist LWL-Außenkabel mit vorzugsweise metallischem Nagetierschutz (in Rücksprache mit dem Betrieb – nicht metallisch (Kevlar)) zu verlegen.

3.1.2 Sekundärverkabelung

Auch die Verkabelung im Gebäude-Steigebereich ist generell mit Lichtwellenleiterkabeln (LWL) auszuführen, es kann Außen- oder Innenkabel verwendet werden. Die zu verlegenden

LWL-Kabel werden wie folgt spezifiziert: [siehe oben](#)

- Nach Rücksprache können hier auch vorkonfektionierte LWL verwendet werden. (Messprotokoll muss vorliegen)

3.1.3 Tertiärverkabelung

Für die Verkabelung bis zu den Endgeräteanschlüssen ist eine gemeinsame strukturierte Verkabelung für alle Netzwerkdienste (z.B. Telefon und Daten) nach Anwendungsklasse F (600MHz) gem. DIN/EN 50173-1: 2018 auszuführen. Die maximal zulässige Länge der Zugangsverkabelung inkl. der Geräteanschlusskabel (Channel) darf 100m betragen.

Es sind Cat7 Leitungen gem. zuvor genannter Norm zu verwenden.

3.2 Netzwerk Topologie

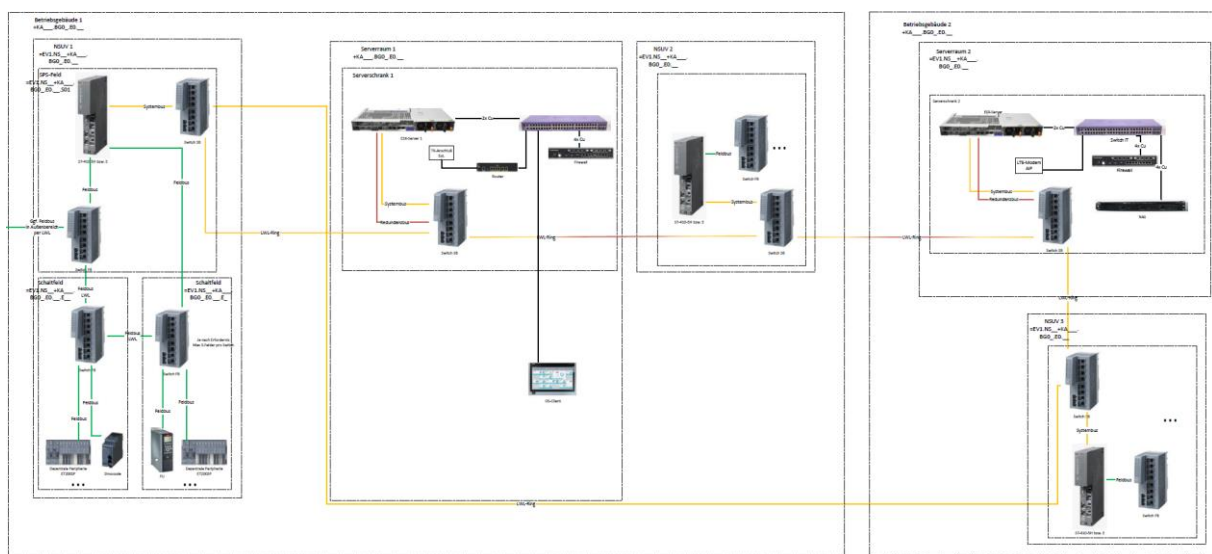


Abbildung: 3-1 Netzstruktur allgemein

3.2.1 Systembus

Der Systembus muss als Ringverkabelung ausgeführt werden, mit dem Media Redundancy Protocol (MRP).

An dem, mit Scalance Switchen auszuführenden MRP-Ring, sind die Server Netzwerkkarten (NIC Systembus) direkt zu verbinden.

Die AS ist ebenfalls mit dem ihr zugeordnetem Switch im Systembus zu verbinden.

Eine Einbindung der AS in den Systembus MRP-Ring kann nach gesonderter Absprache und Genehmigung realisiert werden.

3.2.2 Terminalbus

Der Terminalbus ist Anlagenspezifisch als Baumstruktur aufzubauen.

Es wird ein separates V-LAN in der Struktur der Wuppertal Water and Environmental Association IT genutzt.

Die Server werden mit der zum Terminalbus zugeordneten NIC an die Switches der IT angebunden.

Diese Switches sind zentral über den Bereich PV3 bereitgestellt und verwaltet.

3.2.3 Redundanzbus

Die Verbindung zwischen redundanten OS-Servern muss über Ethernet erfolgen.

Vorzugsweise wird eine Direktverbindung zwischen den Redundanzbus NIC der Server ohne aktive Komponenten gewählt.

Ist eine Direktverbindung ohne aktive Komponenten nicht möglich (räumliche Trennung,...) wird, aufgrund besserer Systemverfügbarkeit System- und Redundanzbus als V-LAN auf der gleichen physikalischen Netzwerkringstruktur verwendet.

An dem, mit Scalance Switches auszuführenden Systembus MRP-Ring, sind die Server Netzwerkkarten (NIC Redundanzbus) direkt zu verbinden. Hier sind die Scalance Switches entsprechend zu konfigurieren.

3.2.4 Feldbus-Systeme

Die Feldbussysteme sind in Profinet auszuführen.
(Ausnahmen sind nur nach betrieblicher Rücksprache zulässig)

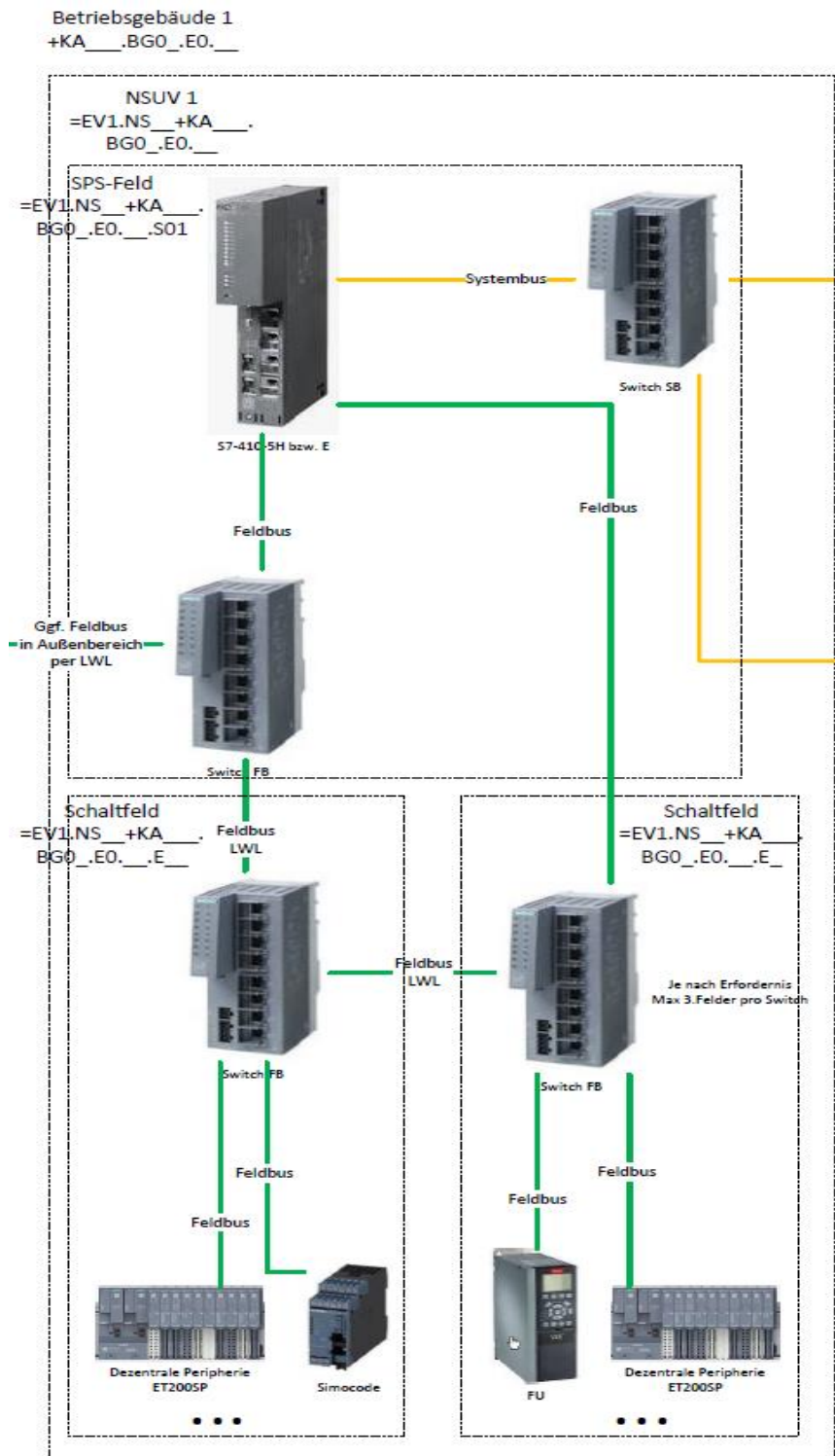


Abbildung: 3-2 Netzstruktur Feldbus

3.2.4.1 Profinet

Die Teilnehmer auf Feldebene werden in der Niederspannungsverteilung je nach Antriebs- bzw. Messtellendichte pro Schaltfeld sternförmig an im jeweiligen Schaltfeld installierte Feldbus-Switches angeschlossen. Bei geringer Teilnehmerzahl können die Feldbus-Switches in maximal jedem dritten Feld installiert werden und von jeweils benachbarten Felder Teilnehmer aufnehmen. Die Feldbus-Switches ihrerseits werden per LWL im Feldbus MRP Ring-verbunden.

Die Anbindung an die zugehörige AS wird im SPS Feld per Cu-Patch auf den Feldbus-Scalance-Switch hergestellt, um die Ringstruktur unter Einbindung der CPU zu erreichen, wird vom nächstgelegenen Feldbus-Scalance-Switch eine weitere Cu-Verbindung zur CPU hergestellt (siehe Skizze).

Es sind die aktuellen Fassungen der IEC 61158 und IEC 61784 zu berücksichtigen.

Es dürfen nur Geräte mit Security Class 1 oder höher verwendet werden.

3.2.4.2 Profibus

Auf die Nutzung von Profibus soll verzichtet werden.

Profibus kann nur nach gesonderter Absprache und Genehmigung realisiert werden.

PROFIBUS DP ist nach Norm IEC 61158 zu projektieren.

3.2.4.3 Feldbus in explosionsgeschützten Bereichen

Hier sind die Feldgeräte nach Norm IEC 61158 mithilfe des HART Protokoll anzubinden.

Die Verfügbarkeit von Profinet mit Ethernet – APL ist zu prüfen.

Bei Verfügbarkeit ist der Einsatz von Ethernet – APL zu fokussieren.

3.2.5 Weitere Netzwerke

Neben den Netzwerken der Leit- und Automatisierungstechnik existieren weitere Netzwerke. Diese Netzwerke sind logisch über VLAN segmentiert. Die VLAN-Segmentierung wird zentral über den Bereich PV3 bereitgestellt und verwaltet.



3.3 Technische Räume

Hier sind die geltenden Anforderungen aus den KRITIS Beurteilungen zu berücksichtigen und mit dem KRITIS Kern-Team des WV abzustimmen. (B3SWA)

3.3.1 Serverschränke

Bei Neueinrichtung der Serverschränke soll i.d.R. ein separater Technikraum, Datenverteilteraum vorgezogen werden. Die notwendige Verkehrsfläche: mind. 10 m², bei möglichst zentralem Standort. Zugangsmöglichkeiten zum Schrank von 2 Seiten, bei 2 oder mehr zusammenhängenden Schränken von Vorder- und Rückseite.

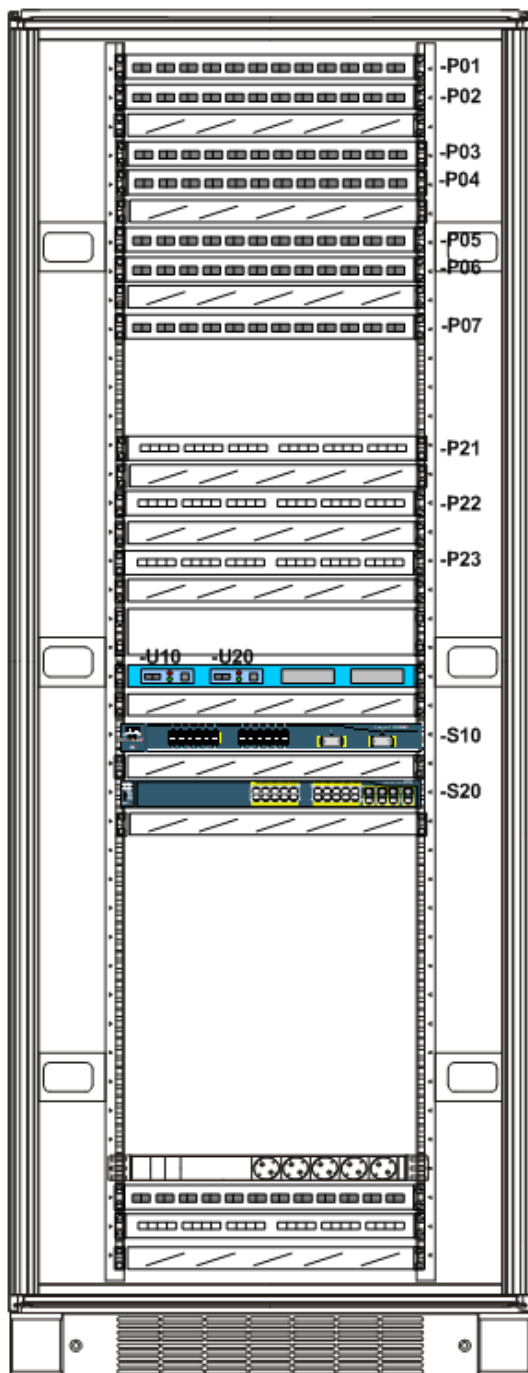


Abbildung 3-3 Beispiel Aufbau Server- /Netzwerkschrank

Aufbaureihenfolge der Komponenten in einem Netzwerkschrank:

1. Spleißbox (OpDat bzw. 19" Einbau)
2. Patchfelder
3. Reserve
4. Temperaturüberwachung
5. Aktive Komponenten
6. Lokale USV (Abstimmung mit Auftraggeber + Netzwerkfähig und managebar) (sep. VLAN)
7. Steckdosen über 2 getrennte Einspeisungen + Netzwerkfähig

3.3.2 Farbkodierung Netzkabel (Kupfer) in Serverschränken

Grau

Torkamera

Zeiterfassung

Drucker, PC, TC

Weiß

Management (USV / PDU ...)

Rot

Zutrittskontrolle

Magenta

Telekom Verbindung

Gelb

Firewall

Blau

Telefonanlage

Hellgrün

Automatisierungstechnik

Redundanzbus PCS7

Terminalbus (bspw. Warten PC / IPC)



3.3.3 Aktive Komponenten

Ausstattung, Mengengerüst, Hersteller, Fabrikat und Typ der aktiven Netzwerkkomponenten sind wegen der Forderung der Integration angebundener Dienste in die vorhandene Systemlandschaft vorgegeben und sind jeweils aktuell mit dem Betreiber abzustimmen.

- Ethernet-Switches mit 10/100/1000TX Autosense-Ports, Uplink-Ports mit 1GE- oder 10GE (LWL, SFP/SFP+), WLAN-Accesspoints, Multiprotocol-Router, Gateways, Firewall, Medienkonverter, usw.
- Zur Pufferung aller Aktivkomponenten ist ein USV-Anschluss vorzusehen, vorzugsweise an zentral vorhandene USV-Anlagen.

3.3.4 Passive Komponenten

- Geschirmte RJ45-Patchfelder Link-Klasse F oder höher (je 24xRJ45 auf 1HE) zum Anschluss der Gebäudekabel
- Verschluss freier Bereiche mit Blindplatten
- LWL Patchfelder ([siehe oben](#))

3.4 Dokumentation

Beschriftung der Netzwerkverteiler gem. OKZ

Dienstneutrale Dokumentation der Leitungen

Messprotokolle:

- OTDR-Messung bei LWL-Leitungen
- Kupfer: Verdrahtungstest, TDR-Längenmessung, Nachweis der Klasse-F-Fähigkeit aller Kabel inkl. Dosen und Patchfelder entsprechend Standard: Return Loss (RL), Impedanz, Dämpfung, Nahnebensprechdämpfung, Attenuation-Crosstalk-Ratio (ACR), Equal level far-end crosstalk loss (ELFEXT), Far-end Crosstalk loss (FEXT), Power sum attenuation to crosstalk loss ratio (PSACR), Power sum equal level far-end crosstalk loss (PSELFEXT), Power sum near-end crosstalk loss (PSNEXT).

Zeichnungen:

- Erstellung bzw. Ergänzung der vorhandenen Netzwerk Konfiguratoren
- Etagenpläne (Grundrisszeichnungen mit allen Anschlusspunkten, Kabeltrassen und Deckendurchbrüchen)
- Schrankzeichnung mit allen Einbauten
- Statuslisten mit den Kurzergebnissen der Kabelmessung (Pass/Fail)
- Verkabelungsübersichten (Tabelle mit Raum-Nr., Dosen-Nr., Kabellänge vom Sternpunkt, sKabelbezeichnung, ...)
- Messprotokolle (s.o.) Systemintegration

Es ist explizit darauf zu achten, dass bei Neubau, Umbau und Erweiterung von Teilbereichen der Netzwerkinfrastruktur die vollständige Interoperabilität und Kompatibilität zwischen der neuen Hard- und Software zu bestehenden Systemen vorschriftenkonform gegeben ist.

Zur Dokumentation wird beim Wuppertalverband derzeit das Netzwerkmanagement-Tool „Pathfinder“ verwendet.

Neue Netzwerkinfrastrukturen sind nach der Fertigstellung zum Import in einer Excel-Tabelle zu dokumentieren. Die entsprechende Vorlagedatei wird bei Bedarf zur Verfügung gestellt. Um eine ordnungsgemäße Importfunktion zur gewährleisten, darf die Vorlagedatei in ihrer Spaltenanordnung und –Beschriftung nicht verändert werden.



4 Automatisierungs-/Prozessleitsystem

Der Wuppertal Wasser- und Umweltverband hat die strategische Entscheidung getroffen, seine Anlagen zukünftig nach einem einheitlichen System aufzubauen.

Im Kern kommt hierbei das Prozessleitsystem SIMATIC PCS7 von der Fa. Siemens zum Einsatz.

Um den zukünftig immer weiter steigenden Anforderungen der IT-Sicherheit wirtschaftlich Rechnung tragen zu können, wurde festgelegt, die Prozessleitsystem-Landschaften nicht als Inseln zu betreiben, sondern sinnvoll in die IT-Infrastruktur des Wuppertal Wasser- und Umweltverbandes zu integrieren.

Aktuell befindet sich das System noch in der Aufbau- und Erprobungsphase. Daher sind noch nicht alle Bestandteile final abgestimmt. Für Abschnitte mit fehlenden Festlegungen bzw. Vorgaben sind bis auf Weiteres Einzelfallentscheidungen herbeizuführen.

4.1 Prinzipieller Aufbau der PCS 7- Systeme

Der Wupperverband betreibt in seinem Verbandsgebiet 11 Kläranlagen, 14 Talsperren und über 60 Sonderbauwerke. Alle Anlagen besitzen über verschiedene Wege eine informationstechnische Anbindung an den Hauptverwaltungssitz in Wuppertal. Alle Kläranlagenstandorte besitzen jeweils eine eigenständige örtliche Serverumgebung, die Talsperren sind teilweise zu Anlagenverbünden zusammengeschlossen und die Sonderbauwerke besitzen eine Leitsystemzentrale in der Hauptverwaltung.

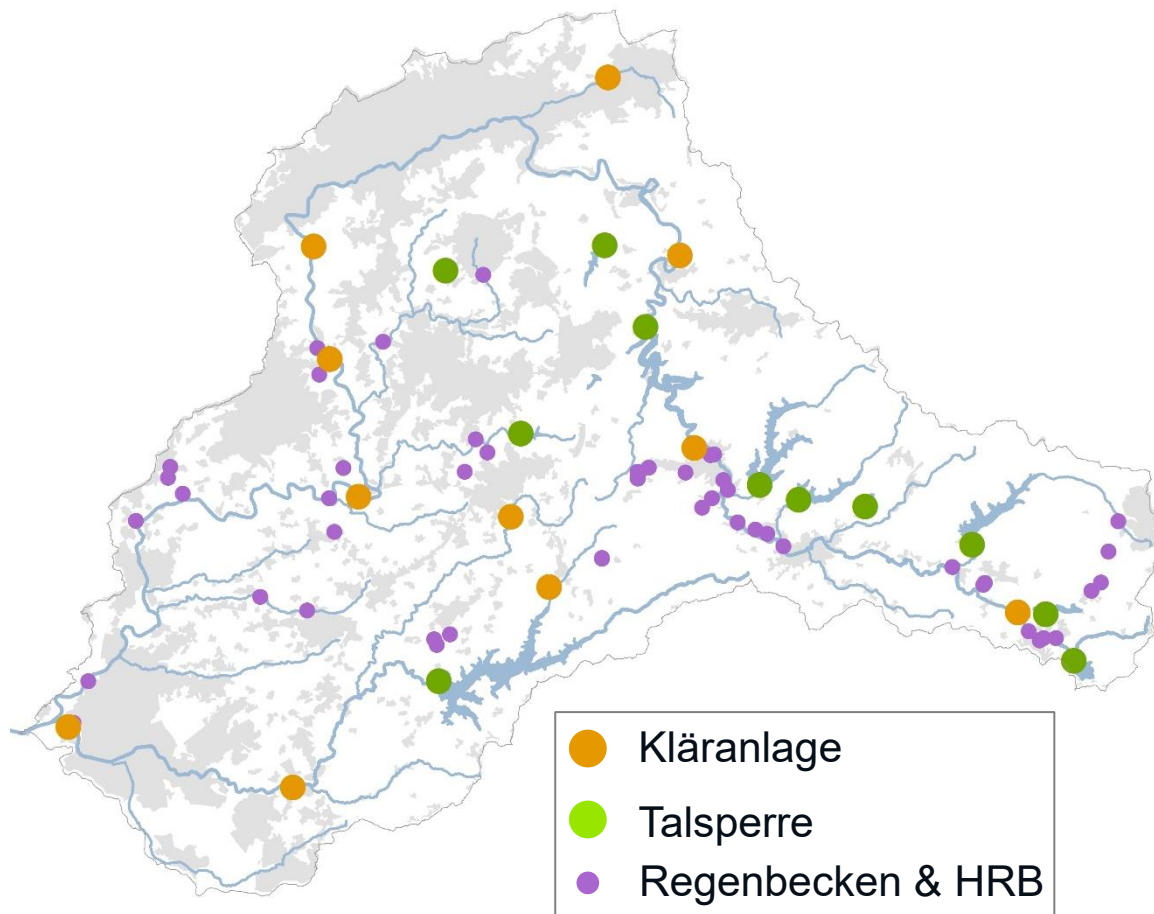
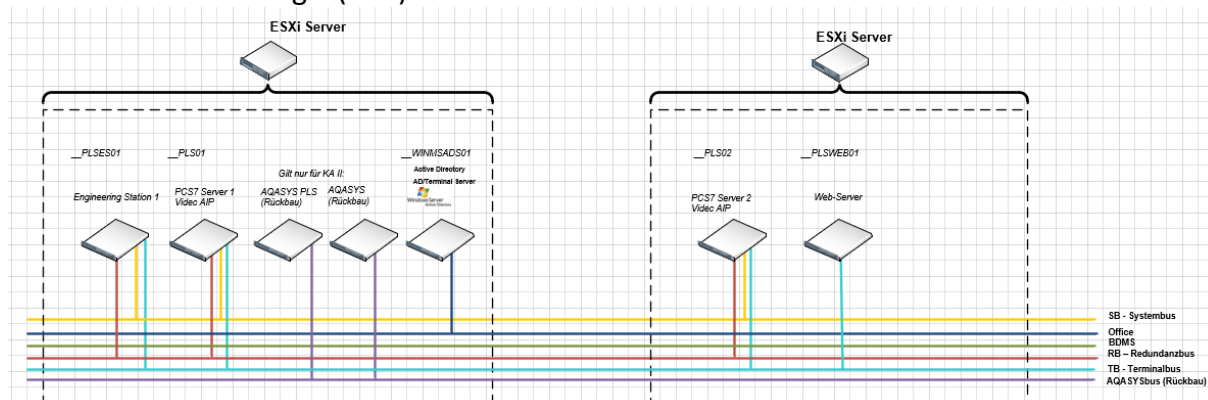


Abbildung 4-1 Anlagen Verbandsgebiet Wuppertal

Standorte mit einem PCS-7-Leitsystem besitzen jeweils 2 physikalische Server, die in unterschiedlichen Räumen (Ausführungshinweise s.o.) installiert sind. Das Prozessleitsystem SIMATIC PCS7 ist in einer serverbasierten virtuellen Umgebung realisiert. Virtualisierung bezeichnet die Abstraktion der physikalischen Hardware vom Betriebssystem. Auf einem realen Rechner ist dazu eine spezielle Virtualisierungsschicht implementiert, der sogenannte Hypervisor. Dadurch sind auf einem realen, physischen Computer (Hostsystem) mehrere voneinander isolierte virtuelle Maschinen (VM) realisierbar, die über eigene virtuelle Hardwarekomponenten verfügen. Diese verhalten sich wie reale Computer und können jeweils selbst Anwendungen ausführen. Die Serverstruktur wird durch den Bereich PV3 zur Verfügung gestellt. Installationen von Leitsystemkomponenten sind nur in Absprache mit den zuständigen ICS-Administratoren zulässig.

4.2 PCS7-Systembestandteile Server-Ebene

Zur Erhöhung der Anlagenverfügbarkeit und Sicherheit des Betriebes ist das Prozessleitsystem redundant aufgebaut. Zur Erreichung der gewünschten IT-Sicherheit werden die verschiedenen Bestandteile des PCS7-Systems (OS-Server, OS-Client, Webserver, Engineering, OPC-Server,) auf verschiedenen virtuellen Maschinen installiert. Zusätzlich wird auf den Standorten ein Physikalischer Warten PC errichtet. Die Kommunikation der Komponenten wird durch Firewall-Cluster überwacht und reglementiert. Die Bereitstellung der erforderlichen Firewall-Technologie erfolgt durch die beim Wupperverband zuständigen Bereich für Informationstechnologie (PV3).



Die generelle Systemstruktur des PCS7 mit der verteilten Anordnung der verschiedenen Systembestandteile ist im vereinfachten Netzstrukturplan dargestellt.

4.2.1 PC-Hardwareausbau

Es gelten die aktuellen Hardwarevoraussetzungen aus der PCS 7 Liesmich Dokument (in der aktuellen Fassung) hier ein Auszug für V9.1 SP2 UC04.

Engineering Station		
Name:	__PLSES01	
Prozessor:	>= i5-4570TE	
RAM:	>= 16GB	
Festplatte 1	C:\ 125GB	System
Festplatte 2	D:\ 200GB	Daten
Festplatte 3	L:\ 1GB	License
Netzwerk-adapter 1	Systembus	
Netzwerk-adapter 2	Terminalbus	
Browser	Microsoft Edge	

OS Server		
Name:	__PLS01	
Prozessor:	>= i5-4570TE	
RAM:	>= 16GB	
Festplatte 1	C:\ 125GB	System
Festplatte 2	D:\ 100GB	Daten
Festplatte 3	L:\ 1GB	License
Netzwerk-adapter 1	Systembus	
Netzwerk-adapter 2	Terminalbus	
Netzwerk-adapter 3	Redundanzbus	

redundanter OS Server		
Name:	__PLS02	
Prozessor:	>= i5-4570TE	
RAM:	>= 16GB	
Festplatte 1	C:\ 125GB	System
Festplatte 2	D:\ 100GB	Daten
Festplatte 3	L:\ 1GB	License
Netzwerk-adapter 1	Systembus	
Netzwerk-adapter 2	Terminalbus	
Netzwerk-adapter 3	Redundanzbus	

OS Client (auch Warten PC)		
Name:	__PLSCL01	
Prozessor:	>= i3-4330TE	
RAM:	>= 4GB	
Festplatte 1	C:\ 125GB	System
Festplatte 2	D:\ 100GB	Daten
Festplatte 3	L:\ 1GB	License
Netzwerk-adapter 1	Terminalbus	

WEB Server		
Name:	__PLSWEB01	
Prozessor:	>= i5-4570TE	
RAM:	>= 16GB	
Festplatte 1	C:\ 125GB	System
Festplatte 2	D:\ 100GB	Daten
Festplatte 3	L:\ 1GB	License
Netzwerk-adapter 1	Terminalbus	

4.2.2 Zentrales System- und Asset-Management

Befindet sich aktuell im Aufbau.

4.2.2.1 Management Console (in Bearbeitung)

4.2.2.2 SINEC NMS (in Bearbeitung)

4.3 IP-Adressen

Für die verschiedenen Netze (Feld-, System-, Terminalbus und sonstige IT-Netze) sind für jeden Standort die erforderlichen IP-Adressräume definiert. Diese werden von den IT- und ICS-Administratoren verwaltet. Vorgaben bez. der zu verwendenden bzw. zur Verfügung stehenden IP-Adressräume werden bei Projektstart übergeben.

4.4 Lizenzierung und Mengengerüst

Bezüglich der Lizenzierung unterscheidet sich die Installation auf einer virtuellen Maschine nicht von der Installation auf einer realen Hardware (SIMATIC PCS 7 Industrial Workstation). Das Betriebssystem und jede SIMATIC Software-Installation auf einer virtuellen Maschine, z. B. SIMATIC PCS 7 müssen lizenziert werden.

Da die Kommunikation für PCS 7 in virtueller Umgebung über BCE / Softnet - IE erfolgt, müssen für die entsprechende Lizenzen verwendet werden.

Bei Mengengerüsten müssen die aktuellen Vorgaben von Siemens in Abstimmung mit dem Auftraggeber berücksichtigt werden.

4.5 PCS7 Automatisierungsstationen

Die Automatisierungsstation (AS) ist die wichtigste Komponente im Prozessleitsystem PCS7. Die AS gewährleistet den sicheren Betrieb und Umsetzung der verfahrenstechnischen Vorgaben in einer Betriebsanlage. Das AS-System muss unabhängig vom übergeordneten Prozessleitsystem vollkommen autark arbeiten.

Somit sind die wichtigsten Anforderungen an Sicherheit, Verfügbarkeit und Ausführung der verfahrenstechnischen Funktionen der Betriebsanlage erfüllt.

4.5.1 Hardware

4.5.1.1 CPU

Eine zentrale AS-400 Station bildet im PCS7-System die Basis der Automatisierung in einer Anlage; größere Betriebsanlagen, z.B. Kläranlagen, werden entsprechend mit mehreren AS-400 Stationen ausgerüstet. Hierbei ist eine AS pro Verfahren Stufe zu planen (z.B. Mechanische-Reinigung, Biologie-Reinigung, ...) die Abstimmungen erfolgt mit dem ICS - Administrator und ICS – Betreiber.

Sind besondere Verfügbarkeiten oder Sicherheiten gefordert, wird die AS-400 Station redundant ausgeführt. Im Prozessleitsystem wird die redundante Station, durch Verwendung spezieller Systemsoftware, als ein Netzwerkteilnehmer abgebildet.

Auslegung erfolgt in Absprache mit dem ICS - Administrator und ICS – Betreiber.

Im Prozessleitsystem PCS7 erfolgt die Abbildung der Automatisierungsebene über den Controller AS 410.

Für Anwendungen mit kleinem Mengengerüst ist die CPU 410E, basierend auf der Hardware der CPU 410-5H einzusetzen. Die CPU 410E bietet die gleichen Vorteile für Anwendungen mit bis zu 200 PO. Programm- und systemtechnisch verhält sich die CPU 410E wie eine CPU 410-5H mit eingeschränkten Mengengerüsten.

Für alle weiteren Anwendungen ist die CPU 410-5H einzusetzen. Die Skalierung der Automatisierungsleistung der CPU 410-5H erfolgt dabei ohne CPU-Tausch und wird über die Anzahl der SIMATIC PCS 7 Prozessobjekte durchgeführt.

Die Auswahl der Zentralprozessoreinheit und die Abstimmung bzgl. der Anzahl der PO's ist auf jeden Fall mit der zuständigen Fachabteilung abzustimmen, da die Anzahl der Prozessobjekte u.a. auch Auswirkungen auf die Lizenzierung und Auslegung der zentralen virtualisierten PCS7 Prozessserver haben.

4.5.1.2 Baugruppen-/ und Rackzusammenstellung

4.5.1.3 Dezentrale Peripherie

Als Dezentrale Peripherie wird die ET 200-SP eingesetzt. Als Mindestanforderung werden Komponenten als High Feature (HF) eingesetzt. Analoge Baugruppen werden darüber hinaus mit HART-Funktionalität eingesetzt.

4.5.1.4 Feldgeräte

Anbindung vorzugsweise über Profinet

- Danfoss Frequenzumrichter
- Schieber Aumamatic
- Kommunikation zu „fremden“ Automatisierungskomponenten / Package Units
- Komplexe / Multi- Messtechnik (Hach Lange, MID,...).
- Standard Messtechnik (Höhenstand, Druck, Temperatur,...).
 - Die Verfügbarkeit von Profinet mit Ethernet – APL ist zu prüfen.
Bei Verfügbarkeit ist der Einsatz von Ethernet – APL zu fokussieren.
Als Alternative für diese Messtechnik ist das HART – Protokoll zu nutzen.

Für einzubindende Anlagenteile der Bestandsanlage, die nicht in der AS programmiert werden (Package Units wie z.B. BHKW-Anlagen, Zentrifugen, ...) muss eine Übergabeschnittstelle vereinbart und geplant werden. (vorzugsweise Profinet)

(IEC – Kommunikation ?)

4.6 Engineering

Für die Arbeiten am Prozessleitsystem wird beauftragten Dienstleistern durch den Bereich PV3 ein Zugang zur PCS7-Engineering-Umgebung bereitgestellt.

Um Zugriff auf die Systeme des Wupperverbandes zu erhalten, ist eine digitale Identität erforderlich. Zur Erzeugung einer digitalen Identität sind durch den Dienstleister im Vorfeld der Maßnahme ein Benutzerantrag und die Vertraulichkeitsvereinbarung zur Informationssicherheit für externe Geschäftspartner (Non-Disclosure-Agreements) zu unterzeichnen. Die genannten Dokumente werden durch den jeweiligen Projektverantwortlichen des Wupperverbandes zur Verfügung gestellt.

Durch die Bereitstellung eines VPN-Zugangs können externe Dienstleister auch von außerhalb des Wupperverbands-Netzwerkes auf die Projektierungsumgebung und sonstige freigegebene Systeme zugegriffen werden. Sofern ein externer Zugriff erforderlich ist, kann dieser durch Beantragung eines VPN-Zugangs durch den jeweiligen Projektverantwortlichen zur Verfügung gestellt werden.

Die Bearbeitung von PCS7-Projekten ist nur über den bereitgestellten Zugang zugelassen, die Verwendung von fremder Hardware innerhalb des Wupperverbands-Netzwerkes ist nicht freigegeben.

Bei Start der Implementierung auf den Systemen des Wuppertal Water and Environmental Association kann in Abstimmung mit den ICS-Administratoren einmalig eine Grundkonfiguration auf das System übertragen werden.

Veränderungen von aktiven Automatisierungsprogrammen sind nur innerhalb der regulären Arbeitszeiten zugelassen. (In Rücksprache mit Betrieb/ICS-Administratoren).

4.6.1 AS – Engineering

4.6.1.1 Aufbau der Programmstruktur in der Komponentensicht

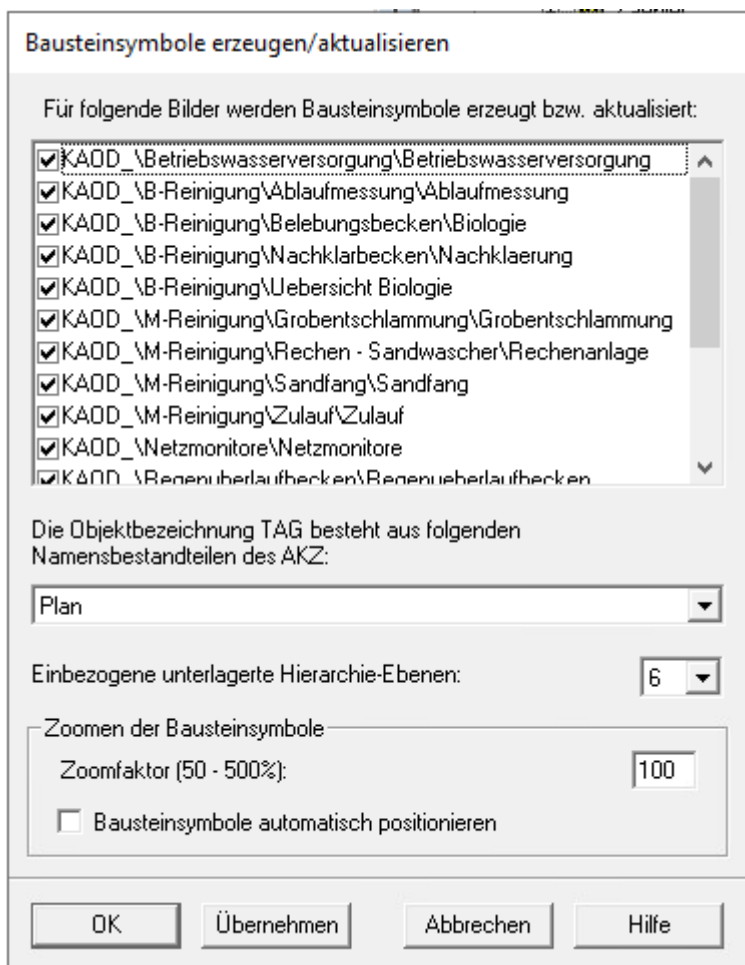
Multiprojektierung wird genutzt mit folgender Unterteilung:

- OS-Server, Client, Web-Server, ES und OPC-Server werden in einem Projekt konfiguriert
- Jede AS bekommt ein eigenes Projekt

4.6.1.2 Aufbau der Programmstruktur in der Technologischen Sicht

Die Technologische Hierarchie wird in dem Projekt der OS vorgegeben. Alle anderen Projekte (der Automatisierung Stationen (AS)) referenzieren auf diese Technologische Hierarchie.

Die Technologische Hierarchie ist **nicht** AKZ bildend.



Bausteinsymbole erzeugen/aktualisieren

Für folgende Bilder werden Bausteinsymbole erzeugt bzw. aktualisiert:

- ☒ KAOD_ \Betriebswasserversorgung\Betriebswasserversorgung
- ☒ KAOD_ \B-Reinigung\Ablaufmessung\Ablaufmessung
- ☒ KAOD_ \B-Reinigung\Belebungsbecken\Biologie
- ☒ KAOD_ \B-Reinigung\Nachklärbecken\Nachklärung
- ☒ KAOD_ \B-Reinigung\Übersicht Biologie
- ☒ KAOD_ \M-Reinigung\Grobentschlammung\Grobentschlammung
- ☒ KAOD_ \M-Reinigung\Rechen - Sandwascher\Rechenanlage
- ☒ KAOD_ \M-Reinigung\Sandfang\Sandfang
- ☒ KAOD_ \M-Reinigung\Zulauf\Zulauf
- ☒ KAOD_ \Netzmonitore\Netzmonitore
- ☒ KAOD_ \Regenüberlaufbecken\Regenüberlaufbecken

Die Objektbezeichnung TAG besteht aus folgenden Namensbestandteilen des AKZ:

Plan

Einbezogene unterlagerte Hierarchie-Ebenen: 6

Zoomen der Bausteinsymbole

Zoomfaktor (50 - 500%): 100

☐ Bausteinsymbole automatisch positionieren

OK Übernehmen Abbrechen Hilfe



Jedes Aggregat mit eigenem AKZ bekommt seinen eigenen Plan. Punkte werden im Plannamen durch Unterstriche ersetzt. Im Plan bekommt der Primäre Technologische Baustein das BMK als Namen.

Die Kommentare ergeben sich ebenfalls aus dem AKZ. Die Kommentare sollten so weit ausgeschrieben werden um das Aggregat eindeutig zu beschreiben.

Profinet Geräte erhalten ebenfalls Ihr AKZ als Namen. Die Sonderzeichen werden hier Durch "X" ersetzt.

Beispiel:

AKZ: RoSa_.RUB.DA01.2R01

Plannamen: RoSa__RUB_DA01_2R01

Name des integrierten Technologischen Bausteins: Bspw. „M01“

Kommentar: Rönsahl Regenüberlaufbecken Drosselanlage 01 Drosselschieber 01

Profinet Namen: RoSaXXRUBXDA01X2R01

Ausnahmefall: GFS (Global Function Service):

Jeder Anlagenteil bekommt seinen eigenen GFS. Bei Sonderbauwerken bekommt jede Anlage einen GFS.

Die Benennung erfolgt ebenfalls über das AKZ. Anlage und Anlagenteil, bzw. Anlage, mit dem Nachtrag "GFS".

Bsp.: KAOB__RUB_GFS oder RoSa__GFS

4.6.1.3 Verwendung von Standard-Bibliotheken

Die Erstellung der Automatisierungsprogramme soll auf Basis von einheitlichen Strukturen erfolgen. Kern der Strukturen sind die Prozessobjekte, die in der Systemwelt des PCS7 über die Bausteine der Industry Library (IL), Advanced Process Library (APL), sowie die auf diesen aufbauenden Water Control Module Types (WCMT) abgebildet werden.

Für die informationstechnische Verarbeitung von Antrieben, Messstellen und sonstigen Meldungen sind in erster Linie die genannten Bibliotheken zu verwenden. Abweichungen hiervon sind mit der Stabsstelle Automatisierungstechnik abzustimmen.

Es sind nur die, auf den Engineering-Stationen durch den WV zur Verfügung gestellten Versionen, der entsprechenden Bibliotheken zu nutzen.

4.6.1.4 AS-Programmschutz

Zum Schutz vor unbefugter Änderung ist das AS-Programm durch ein Passwort zu schützen. Dieses wird zu Projektbeginn durch die Abteilung T01 vorgegeben und im Passwort-Management System eingepflegt.

4.6.2 OS – Engineering

4.6.2.1 Ordnerstruktur

Auf allen Servern werden auf der Festplatte "Data" (D:) Folgende Ordner angelegt:

- i. 01-Projekt
- ii. 02-Install

Der Ordner „01-Projekt“ dient als Ablage des Projektes. Auf der ES werden hier das Multiprojekt und dem untergeordnet alle Teilprojekte gespeichert. Auf den OS Servern und den Clients wird der Ordner als Zielpfad für die Projekte projektiert.

Der Ordner „02-Install“ ist vorgesehen für Software, welche auf den Maschinen lokal gebraucht wird

4.6.2.2 Netzwerkverbindung zum Terminalbus

"SIMATIC Shell" ist Bestandteil von PCS 7 und dient zur zentralen Wartung und Diagnose aller im Client-Server-System eingebundenen PC-Stationen.

- Die Kommunikation ist grundsätzlich verschlüsselt zu konfigurieren.
- Der einzustellende PSK- Schlüssel wird durch den WV vorgegeben.

4.6.3 Kurzzeitarchivierung (Alarm- und TagLogging)

Die Kurzzeitarchivierung erfolgt auf den OS – Servern

Tag Logging 31 Tage (geteilt in 31 Segmente a 24h)

Alarm Logging 1 Jahr (geteilt in 12 Segmente a 1 Monat)

4.6.4 Langzeitarchivierung der Archive

Für die Langzeitarchivierung wird vom WV das zentrale Betriebsdatenmanagement WISKI genutzt. Die Kommunikation erfolgt über die OPC-UA-Schnittstelle (hierüber werden alle Datenpunkte weitergereicht). Ein separater Process- Historian wird nicht eingesetzt.

4.6.5 PCS7 Berechtigungskonzept

4.6.5.1 Informationssicherheit

Die Gewährleistung einer angemessenen Informationssicherheit gemäß dem Stand der Technik wird schon im Rahmen von Planung und Projektierung (Security-by-design) berücksichtigt.

Die Anlage wird als Kritische Infrastruktur (KRITIS) betrachtet. Daher ist eine angemessene Informationssicherheit mit Hilfe des branchenspezifischen Sicherheitsstandards B3S-WA (Wasser/Schmutzwasser) von DWA und DVGW umzusetzen.

4.6.5.2 Zugang zu den Engineering-Systemen (siehe: 4.6 #Engineering)

-ICS-Administratoren des WV erhalten die Berechtigungsstufe „Administrator“.

-Externe Projektoren erhalten **höchstens** die Berechtigungsstufe „Engineering“.

Als Screen-Lock Zeit nach Inaktivität ist für alle Benutzergruppen 15 Minuten einzustellen.

4.6.5.3 OS-Berechtigungen (in Bearbeitung)

Die Berechtigungsstufen werden über den SIMATIC-LOGON Manager an das Active-Directory des Wuppertal Wasserwerkes angebunden. Die Verwaltung der Gruppen erfolgt zentral über die Administratoren des Wuppertal Wasserwerkes. Der Wuppertal Wasserwerk legt fest welche Berechtigungen einem Bediener auf einer bestimmten Bedienstation zur Verfügung stehen. Für jeden Bereich muss ein Berechtigungskonzept erstellt werden.

XX definiert den Standort. (als Beispiel gilt: BU = Buchenhofen, OD = Odenthal, KE = Kerspe Talsperre)

XX-PCS7-ADMIN

XX-PCS7-ENGINEERING

XX-PCS7-BETRACHTER

XX-PCS7-OPERATOR

XX-PCS7-OPERATOR-PLUS

Als Auto-Logout Zeit ist für alle Benutzergruppen 5 Minuten Inaktiv einzustellen.

4.7 Bedienstationen

4.7.1 Software Bedienstationen

Die Bedienung des PCS7-Systems kann sowohl über OS-Client-Stationen als auch Web- Clients erfolgen.

Der Ausstattungsgrad eines PCS7-Systems mit OS-Clients ist anwendungsfallbezogen festzulegen und u.a. abhängig von der Standortgröße. Auf Klärwerksstandorten kommt ein weiterer OS-Client (Warten – Client), installiert auf einem Windows-basierten 19“ Rechner im Server Rack des jeweiligen Standortes hinzu.

Als ergänzende Bedienmöglichkeit stehen Web-Clients zur Verfügung. Zur Nutzung des Web-basierten Zugriffs ist für jedes PCS7- System auf Klärwerken, Talsperren und der Hauptverwaltung ein entsprechender Web-Server vorgesehen.

Der Zugriff auf einen Web-Client wird anwenderbezogen zentral seitens der IT über die Citrix-Oberfläche zur Verfügung gestellt.

Durch den Web-basierten Zugriff wird auch eine Nutzung über mobile Endgeräte ermöglicht.

Diese greifen entweder über ein standortbezogenes WLAN oder über Mobilfunk und VPN auf den Web-Server zu.

4.7.1 Vor-Ort Bedienstationen

Die Bedienung der Aggregate wird zur erhöhten Ausfallsicherheit zusätzlich über eine Vor-Ort Bedienstelle erfolgen. Hier ist die Schlüsselschalterstellung (Vor-Ort, Service, Fern) zu berücksichtigen. Im „Vor-Ort“ Betrieb werden die Aggregate (Motoren, Schieber, Frequenzumrichter) Hardwaretechnisch angesteuert. In „Service“ Stellung ist jegliche Funktion, elektrisch sowie steuerungstechnisch, zu verriegeln. In der „Fern“ Stellung wird die Bedienung/Steuerung an das Leitsystem übergeben.

4.8 Prozessbilder

Die Prozessbilder der verfahrenstechnischen Anlagen sind in Anlehnung an die R&I Verfahrensfließbilder zu erstellen (2 Dimensionale Darstellung). Die Farbgebung der unterschiedlichen Medienströme ist dabei zu übernehmen.

Medienarten				
Gruppe	Medium	Linienart	RGB-Farbe	RAL-Farbe
Gruppe 1	Wasser			RAL 6032
	Abwasser	Continuous	26,122,99	RAL 5021
	Betriebswasser	VERDECKT	35,127,82	RAL 6032
	Fettwassergemisch	ACAD_ISO12W100	35,127,82	RAL 6032
	Kondensat	ACAD_ISO09W100	35,127,82	RAL 6032
	Prozesswasser	ACAD_ISO08W100	35,127,82	RAL 6032
	Sandwassergemisch	ACAD_ISO06W100	35,127,82	RAL 6032
	Spülwasser	RAND	35,127,82	RAL 6032
	Stadtwasser	ACAD_ISO10W100	97,153,59	RAL 6018
	Trinkwasser	ACAD_ISO07W100	133,166,122	RAL 6021
Gruppe 2	Wasserdampf			RAL 3001
	Wasserdampf	Continuous	155,36,35	RAL 3001
Gruppe 3	Luft			RAL 7004
	Prozessluft	Continuous	155,155,155	RAL 7004
	Steuerluft	ACAD_ISO10W100	155,155,155	RAL 7004
Gruppe 4	Brennbare Gase			RAL 1003
	Erdgas, Flüssiggas	Continuous	255,214,77	RAL 1018
	Faulgas	ACAD_ISO10W100	227,184,56	RAL 1012
Gruppe 5	Nichtbrennbare Gase			RAL 1003
	Stickstoff, N ₂ -haltige Gase	ACAD_ISO09W100	249,168,0	RAL 1003
	Rauchgas	RAND	228,158,0	RAL 1004
Gruppe 6	Säure			RAL 2010
	Fäll- / Flockungsmittel	Continuous	224,94,31	RAL 2000
	pH-Regulatoren	ACAD_ISO10W100	224,94,31	RAL 2000
	Polymeres Flockungsmittel	ACAD_ISO12W100	224,94,31	RAL 2000
Gruppe 7	Lauge			RAL 4008
	Fäll- / Flockungsmittel	Continuous	132,76,130	RAL 4008
	pH-Regulatoren	ACAD_ISO10W100	132,76,130	RAL 4008
Gruppe 8	Brennbare Flüssigkeiten			RAL 8002
	Heizöl	Continuous	121,77,62	RAL 8002
	Fette / Öle	ACAD_ISO07W100	137,105,62	RAL 8000
	Externe C-Quelle / Co-Substrate	VERDECKT	127,64,49	RAL 8029
Gruppe 9	Nicht Brennbare Flüssigkeiten / Schlamm			RAL 8002
	Fäkalschlamm	ACAD_ISO10W100	121,77,62	RAL 8002
	Primär-, Rücklauf-, Überschussschlamm	ACAD_ISO12W100	141,73,49	RAL 8004
	Schwimmschlamm	ACAD_ISO06W100	114,74,37	RAL 8008
	Faulschlamm	ACAD_ISO08W100	117,88,71	RAL 8025
Gruppe 10	Sonstige Medien			
	Rechengut	ACAD_ISO09W100	121,77,62	RAL 8002
	Sandfanggut	RAND	121,77,62	RAL 8002
Gruppe 0	Sauerstoff			RAL 5005
	Ozon	Continuous	0,83,135	RAL 5005
Gebäudetechnik				
	Heizungsvorlauf	ACAD_ISO08W100	171,31,28	RAL 3000
	Heizungsrücklauf	ACAD_ISO08W100	0,43,112	RAL 5010
	Zuluft	ACAD_ISO10W100	0,137,182	RAL 5012
	Abluft	ACAD_ISO12W100	77,105,153	RAL 5014



MS- und NS-Verteilungen werden gemäß den Einstrich-Diagrammen erstellt und es wird dafür eine dynamische Einfärbung von Stromschienen und Schaltgeräten vorgesehen.

Zur effizienteren Bedienung soll der Bediener durch drücken des WV Logos auf die Übergeordnete Anlagensicht weitergeleitet werden.

4.9 Alarmmanagement

Als Alarmierungstool wird die Software Alarm Informations Portal (AIP) der Fa. Videc eingesetzt. Das Alarmierungssystem ist, analog zum PCS7-System, redundant aufgebaut. Auf jedem der beiden PCS7-OS-Server wird zusätzlich eine AIP-Serverinstanz sowie jeweils ein Meldeagent installiert.

Zum Absetzen von Alarmen aus dem AIP werden ein festnetzgebundener Telefonanschluss und eine LTE-basierte Modemkommunikation zum Versenden von SMS Benachrichtigungen über Mobilfunk vorgesehen.

Die physikalische Anschaltung für beide Kommunikationswege erfolgt örtlich getrennt in den beiden Serverräumen, d.h. in einem Serverschrank erfolgt die Anbindung des LTE-Modems im anderen Schrank wird die Telefonanlage gekoppelt.

Beim Telefonanlagen-Anschluss handelt es sich hierbei um zum jeweiligen Standort gerouteten VoIP-Nebenstellen der Telefonanlage der Hauptverwaltung des WV.

An einigen Standorten existieren derzeit, parallel zum WV-internen Datenanschluss, der stets gesichert über eine VPN-Verbindung über die Hauptverwaltung des WV läuft, noch separate TK-Anschlüsse mit direkter Verbindung ins öffentliche Netz. An diesen Standorten wird als zusätzliche Rückfall-Ebene ein automatisches Wählgerät (Telenot) eingesetzt, welches als Meldungstrigger einen digitalen Kontakt einer nahegelegenen SPS erhält.

Die Alarmierung erfolgt stets an das Mobilfunktelefon des Standort-bezogenen Bereitschaftsdienstes.

Meldungen, welche den Status der AIP Server oder Agenten betreffen werden lediglich per Email an die Stabsstelle T01 übermittelt.

4.9.1 Sonderbauwerke

Anlagen im Sonderbauwerksbereich besitzen häufig eine geringe räumliche Ausdehnung mit einer geringen Anzahl von zu verarbeitenden Antrieben und Messstellen. Gleichzeitig erzeugt ihre dezentrale Anordnung eine erhöhte Anforderung an autarke Betriebs- und Bedienfähigkeit bei Verbindungsunterbrechung zur PCS7-Zentrale.

Daher unterscheidet sich die Systemarchitektur an einigen Stellen von der Struktur des Klärwerkssektors.

Die PCS7-Zentrale für den Betrieb T2/Becken& Netze befindet sich in der Hauptverwaltung des WV. An diese werden alle Sonderbauwerke kommunikationstechnisch angebunden. Die Kommunikation erfolgt, je nach örtlicher Verfügbarkeit, sowohl über eine kabelgebundene DSL-Verbindung als auch über eine redundante Kommunikationsstrecke per Mobilfunk. In Einzelfällen kann jedoch auch nur eine Kommunikationsstrecke bereitgestellt werden. Die Kommunikationsverbindung von der Hauptverwaltung zum Standort wird durch den Bereich PV3 zur Verfügung gestellt und verwaltet. Die Schnittstelle für den Systemdienstleister stellt hierbei der Port des dezentralen Routers im Sonderbauwerk dar.

Sonderbauwerke nutzen für die Kommunikation zur PCS7-Zentrale in der Hauptverwaltung das Fernwirkprotokoll IEC 60870-5-104.

Es gibt 2 Automatisierungslösungen, eine „Große“ S7-400 und eine „kleine“ ET200SP. Die Einordnung welche Automatisierungslösung gebraucht wird trifft der Betrieb, nach den Kriterien:

- Größe der Anlage
- Wichtigkeit der Anlage
- Anzahl an existenziellen Funktionen.

Die große Lösung besteht aus einer S7-410-5H. Sie wird per Routing an den Systembus des PCS-7 angeschlossen. Von der AS aus läuft ein Feldbus Ring über die OT-Switche im Schaltschrank, Feldbusgeräte werden an Ihnen im Stern angeschlossen.

Die kleine Lösung ist eine ET200 SP. Sie wird in den Feldbus der sich in der HV befindenden S7-410 eingebunden. Sie ist der erste Teilnehmer in der Feldbuslinie nach dem IT-Router. Bei Verbindungsausfall werden existenzielle Funktionen von den Busteilnehmern selbst übernommen. Pumpen werden von Simocodes und Regelungen von Aumaticen gesteuert.

Als Automatisierungsgerät kommt in Sonderbauwerken stets die S7-410-5H zum Einsatz, da in dieser, zusätzlich zur eigentlichen Automatisierungsfunktion, die temporäre Zwischenspeicherung von Daten bei Kommunikationsunterbrechungen erfolgt.

4.10 System zur Angriffserkennung (SzA)

Es sind Vorrichtungen (Software/ Hardware) einzuplanen, um die Anlage an eine vorhandene Angriffserkennung anzubinden. Die Gesetzlichen Rahmenbedingungen sind in dem IT-Sicherheitsgesetz 2.0 festgeschrieben.

[Grafische Darstellung]

4.10.1 Ausleitung Log

[Zu ergänzen]

4.10.2 Ausleitung Datenverkehr



[Zu ergänzen]



5 Abbildungsverzeichnis

Abbildung: 3-1 Netzstruktur allgemein	7
Abbildung: 3-2 Netzstruktur Feldbus	9
Abbildung 3-3 Beispiel Aufbau Server- /Netzwerkschrank	12
Abbildung 4-1 Anlagen Verbandsgebiet Wuppertal	17
Abbildung 4-2: Prinzipielle Netzstruktur PCS7	Fehler! Textmarke nicht definiert.