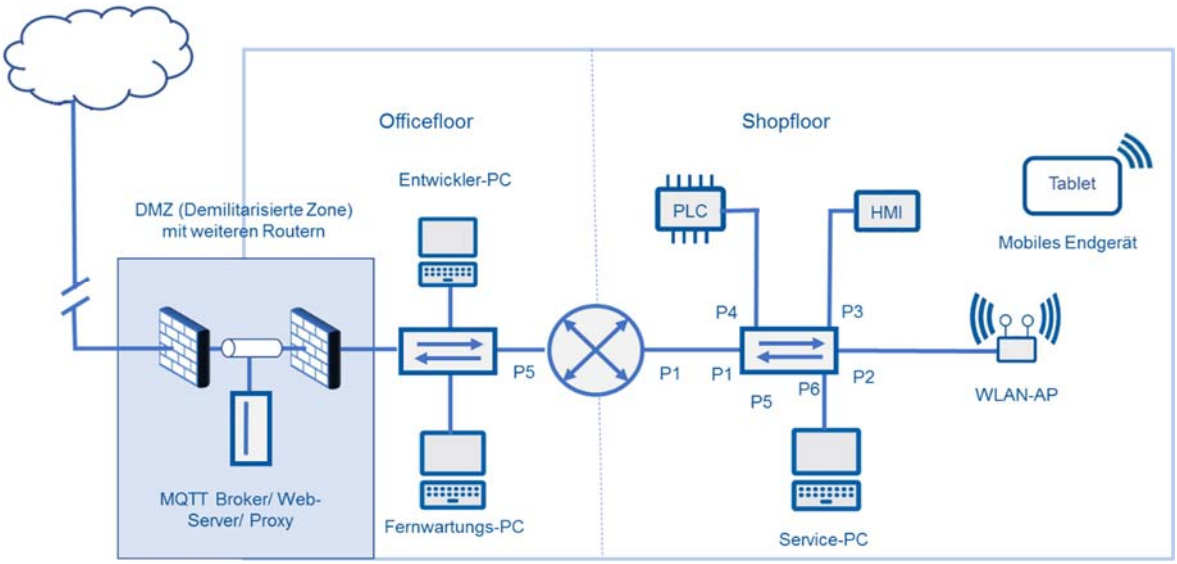
Akademie für Lehrerfortbildung

Digitale Transformation

Cyber-Sicherheit in Produktionsnetzen

M1.4



Interdisziplinäre Qualifizierung von Lehrkräften in den Berufsfeldern Elektrotechnik, Metalltechnik und Informationstechnologie

Inhalt

IMPRESSUM

Herausgeber:	Akademie für Lehrerfortbildung und Personalführung Kardinal von Waldburg-Str. 6-7 89407 Dillingen/Donau
Redaktionsgruppe:	Michael Ziegler, Berufsschule Schulen Altötting Günther Seitz, Berufliches Schulzentrum Hof, Stadt und Land Alexander Ippisch, Berufliches Schulzentrum Amberg Michael Feike, Staatliche Berufsschule III Fürth Dominik Kopp, Alexander Wald, Berufsschule I und Berufsfachschule für Informationstechnik Landshut
Redaktionsleitung:	Michael Lotter, Akademie Dillingen
URL:	http://alp.dillingen.de
Mail:	m.lotter@alp.dillingen.de
Stand:	Juni 2020

DIDAKTISCHE ÜBERLEGUNGEN

Eine hohe Affinität zu den Handlungsfeldern von Industrie 4.0 besitzen unter anderem die Berufsbilder des Elektronikers für Automatisierungstechnik, des Fachinformatikers und des Mechatronikers sowie die technischen Assistenten für Informatik. Die zunehmende Digitalisierung in diesen Berufsbildern bedeutet eine zunehmende Vernetzung und Implementierung cyber-physischer Systeme (CPS). Die Berufsbilder bleiben mit hoher Wahrscheinlichkeit bestehen. Jedoch müssen sie sich aufgrund der Industrie 4.0-Entwicklungen neu ausrichten, um den veränderten Anforderungen gerecht zu werden.

Das Fortbildungsmodul „M1.5 Cyber-Sicherheit in Produktionsnetzen“ fördert Kompetenzen und Fertigkeiten, die für Lehrkräfte in den Berufsfeldern Informationstechnologie, Elektrotechnik und Metalltechnik gleichermaßen erforderlich sind, um die Anforderungen der Industrie 4.0-Entwicklung im Unterricht beruflicher Schulen zu berücksichtigen. Die einzelnen Laborübungen fördern dabei Schritt für Schritt die Handlungskompetenz und Handlungssicherheit der Lehrkräfte in einem integrierten Fachunterrichtsraum[1], der vernetzte Komponenten eines cyber-physischen Systems bereitstellt.

Der Schwerpunkt des Moduls liegt auf der Implementierung technologischer Schutzmaßnahmen auf Grundlage eines definierten Schutzbedarfs und einer Risikolage, welche für das gewählte Szenario typisch ist.

Folgende Lernsituationsbeschreibung veranschaulicht die Gemengelage bestimmter Kompetenzbereiche, die sich auf Grund der Arbeitsteilung in einem exemplarisch beschriebenen, produzierenden Gewerbe ergeben kann. Die Lernsituation ist für den Fachinformatiker mit der Fachrichtung Digitale Vernetzung ausgelegt. Entsprechend der Neuordnung der IT-Berufe ist das der Beruf, der die Schnittstelle zwischen OT und IT bedient. Eine Anpassung der Lernsituation auf weitere Berufe, die in diesem Umfeld tätig sind ist durch eine veränderte Aufgabenstellung und Ausrichtung auf berufstypische Tätigkeit sehr gut möglich, zumal auch Industriemechaniker, Mechatroniker, Elektroniker für Automatisierungstechnik usw. vor der Herausforderung stehen, IT-Sicherheitsrichtlinien Ihres Unternehmens, umzusetzen und anzuwenden.

[1] Einführung in die Berufspädagogik, Andreas Schelten, ISBN 3-515-08440-1

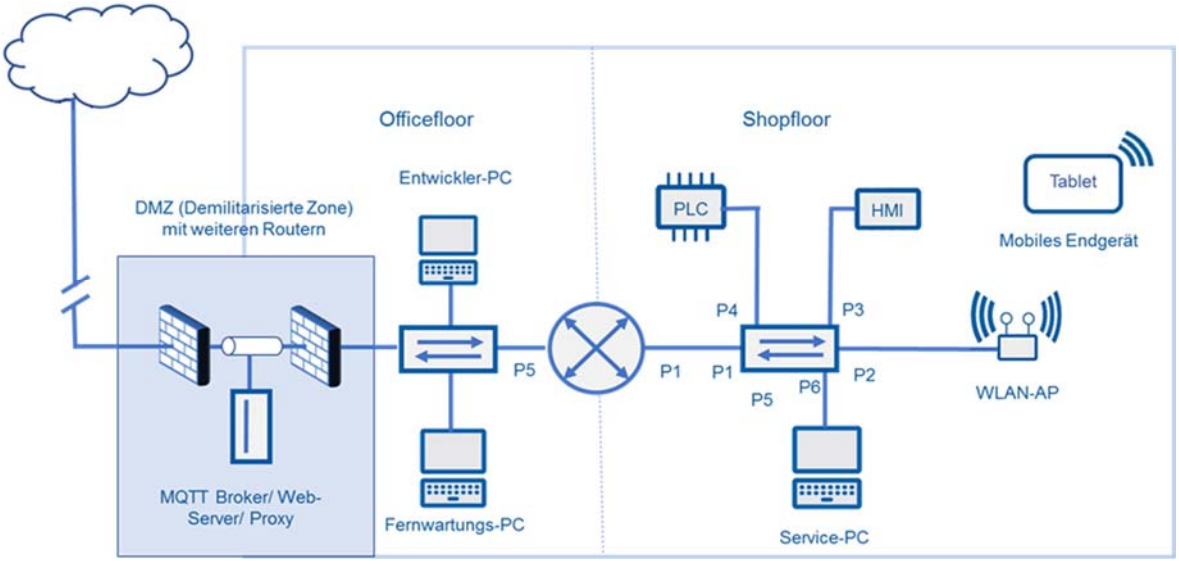
EXEMPLARISCHE LERNSITUATIONSBESCHREIBUNG

Grundlegende Informationen
Beruf: Fachinformatiker/in - Digitale Vernetzung
Jahrgangsstufe: 12
Lernfeld 10d:
Betrieb und Sicherheit vernetzter Systeme gewährleisten
Kernkompetenz des Lernfeldes: Die Schülerinnen und Schüler verfügen über die Kompetenz, mit Hilfe einer Risikoanalyse den Schutzbedarf eines vernetzten Systems zu ermitteln und Schutzmaßnahmen zu planen, umzusetzen und zu dokumentieren.
Ausgewählte Teilkompetenzen der Lernsituation *Die Schülerinnen und Schüler sollen…* ➢ den Schutzbedarf für einen vorgegebenen Informationsverbund und mit Hilfe von vorgegebene Schutzkategorien eines Sicherheitskonzepts ermitteln ➢ auf den Informationsverbund den BSI-Systembaustein „IND.2.1 Allgemeine ICS-Komponenten“ angewendet und passende Schutzmaßnahmen planen. ➢ die ausgewählten Schutzmaßnahmen, unter Berücksichtigung technischer und arbeitsorganisatorischer Rahmenbedingungen, implementieren. ➢ die Sicherheit des vorgegebenen Informationsverbunds prüfen. ➢ die Sicherheit des vorgegebenen Informationsverbunds bewerten, d. h. sie setzen das erreichte Sicherheitsniveau in Bezug zu den definierten Anforderungen auf Grundlagen einer Risikoanalyse (Welche Schäden können eintreten und wie hoch ist die Wahrscheinlichkeit des jeweiligen Schadenseintritts?)
Geschätzter Zeitumfang: 9 x 45 Minuten

Lernsituation

Am Standort eines Herstellers für Sportschuhe wird der Fertigungsprozess automatisiert gesteuert. Mitarbeiter der Produktion überwachen den Prozess lokal oder per Fernwartung mit mobilen und stationären Endgeräten, um Wartungs- und Instandsetzungsaufgaben nachzukommen. Die IT-Abteilung sorgt für den störungsfreien Betrieb der IT-Infrastruktur der Server, Clients und Netze. Beim Betrieb der Produktions-IT werden sie von Mitarbeitern der Produktionsabteilung unterstützt. Die Entwicklungsabteilung stellt für den flexiblen Produktionsprozess Betriebsmittel bereit, d. h. Konfigurationen und Programme werden hier entwickelt. Je nach Relevanz werden Prozessdaten aus der Produktion des Standorts für die Managementebene oder auch für Zulieferer und Kunden bereitgestellt. Der Informationssicherheitsbeauftragte (ISB) der Firma gibt vor, die Standardanforderungen der relevanten BSI-System-Bausteine, z. B. IND.2.1 Allgemeine ICS-Komponenten umzusetzen, damit nicht nur die klassische IT-Infrastruktur, sondern auch die Infrastruktur der Produktions-IT die Kriterien für eine ISO 27001 Zertifizierung erfüllen. Damit weist der Hersteller für Sportschuhe gegenüber Externen, z. B. seinen Kunden nach, dass die Anforderungen der Informationssicherheit (Vertraulichkeit, Verfügbarkeit und Integrität) in seinem Wirkungsbereich erfüllen sind.

Ale Mitarbeiter der IT-Abteilung sorgen Sie dafür, dass die vorgegebenen Anforderungen zur Informationssicherheit im Shop- und Officefloor des Werks- und Fabrikbereich des Turnschuhherstellers umgesetzt werden und ergreifen Sie die vorgegebenen Schutzmaßnahmen.



TECHNISCHE ÜBERLEGUNGEN

Shopfloor und Officefloor müssen zusammenwachsen. Unter dieser Prämisse sind die nachfolgenden Übungen, die für Lehrkräfte aus den Berufsfeldern Metall, Elektro und Informatik entwickelt wurden, zu verstehen. Während bisher der Office-Bereich weitgehend von den IT-Fachkräften abgedeckt wurde, war und ist der Produktionsbereich eine Domäne der Metall- und Elektrofachkräfte. Die zunehmende Digitalisierung der gesamten Wertschöpfungskette erfordert allerdings zunehmend interdisziplinäre Kompetenzen. Standardisierungstendenzen in der Vernetzung (z. B. Ethernet, Industrial-Ethernet oder TSN) erfordern auch von den informationstechnischen Berufen Kenntnisse die im Produktionsumfeld zu finden sind. Gleichermaßen müssen sich klassische Industrieberufe auf allgemeine IT-Kenntnisse einlassen. Die Vernetzung der Systeme, vom Sensor bis zum Webshop, oder auch sogenannte Entitäten müssen von den spezifischen Berufen verstanden, erstellt, gewartet und instandgesetzt werden. Der Zusammenhang wird im Referenzarchitekturmodel Industrie 4.0 (RAMI) dargestellt.

Die einzelnen Übungen bauen aufeinander auf und sollen verschiedene Komponenten aus den unterschiedlichen Bereichen der Wertschöpfungskette verwenden. In der Ausstattungsempfehlung wird dies berücksichtigt, eine Anpassung bzw. Ergänzung ist jederzeit möglich.

Um Prozessdaten herstellerunabhängig weiterverarbeiten zu können, ist ein offenes, standardisiertes aber auch sicheres Protokoll notwendig. In den Übungen wird daher mit dem OPC UA-Protokoll gearbeitet. OPC UA wird von den meisten Herstellern unterschiedlichster Anlagen, Maschinen aber auch Softwareprodukten unterstützt.

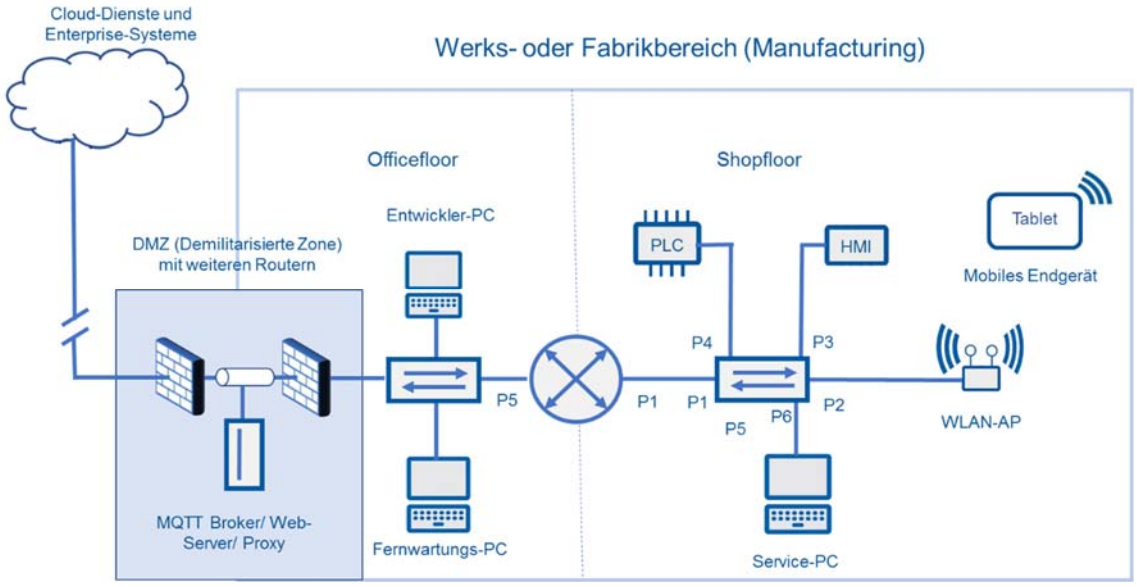
Die Laborübungen wurden mit dem internen OPC UA-Server der PLC S7 1500 erarbeitet und getestet. Für die Konfiguration ist jedoch das TIA Portal der Fa. Siemens notwendig. (Hinweis: Alternativ kann natürlich auch der aus dem Modul M1.3 bekannte externe OPC UA-Server UA Link der Fa. IBHsoftec verwendet werden. Er bietet zur Konfiguration eine Web-Oberfläche und beinhaltet mehrere Ethernet-Schnittstellen inklusive einer Firewall.) Als OPC UA-Client wird der kostenlose und weitverbreitete Test-Client der Firma UA Expert verwendet. Zur einfachen Weiterverarbeitung der OPC UA-Daten wird hier die Software OPC UA-Router der Firma Inray verwendet. Die Software ist kostenfrei und zwei Stunden im Demo-Modus nutzbar.

Die Netzwerkkonfiguration von Industriekomponenten unterscheidet sich wesentlich von denen aus dem Office-Bereich bekannten Windowssystemen. Komponenten die eine komplexe Konfiguration benötigen müssen vom Lehrenden vorinstalliert werden. Entsprechende Konfigurationsdateien für den Accesspoint und Router liegen vor, können aber auch vom Multiplikator/Lehrenden erstellt werden. Eine Konfiguration des vorgeschlagenen Siemens-Routers und Accesspoint durch Teilnehmer/Lernende ist in dieser Phase nicht vorgesehen. Die erstellten Konfigurationsdateien beziehen sich auf das Adressschema der Laborübersicht und sollten daher verwendet werden.

LAB 01 – INBETRIEBNAHME EINER VERNETZTEN ANLAGE

Die Fertigungsumgebung wurde im Rahmen einer Modernisierung erweitert. Bei der Planung und Implementierung wurde eine serviceorientierte Architektur berücksichtigt. Kriterien wie Fernwartbarkeit, vorausschauende Instandhaltung, Monitoring und eine erhöhte Anlagenverfügbarkeit wurden dabei berücksichtigt und umgesetzt.

In dieser Laborübung soll das Produktionsnetzwerk (rechte Seite, siehe Grafik unten ↓) vernetzt, konfiguriert (IP-Adressen) und in Betrieb genommen werden.



Vorbereitung

- IP-Adressierungsschema
- Handbuch SCALANCE XC208 z. B. über die Smartphone App „Industry Online Support “
- Vorkonfigurierte Steuerung (PLC) mit Anwendungsprogramm
- Vorkonfigurierte Devices (HMI, Router, Switch, WLAN-AP)
- Funktionsfähiges Prozessmodell (z.B. Mischanlage, Temperaturerfassung, …)
- Ggf. Anwendung auf WLAN-Geräten für PLC-Zugriff (z.B. SIMATIC S7 App)
- Werkzeug zur Ermittlung und Konfiguration von IP-Adressen und Geräteinformationen (z.B. Primary Setup-Tool (PST), Proneta, cmd-Befehle)

Aufgaben

1. Identifizieren Sie mit Hilfe der App durch den jeweiligen QR-Code die einzelnen Komponenten
2. Verbinden Sie die einzelnen Komponenten „portgenau“ am Switch im Produktionsnetz. Nutzen Sie dazu die vorgegebene Topologie und das IP-Adressierungsschema (die Verbindung Router ↔ Switch wird erst in LAB04 benötigt)
3. Überprüfen Sie ggf. die elektrischen Verbindungen (Stromversorgung, Ein- und Ausgänge der Steuerung, Ethernet-Schnittstellen-LEDs)
4. Nehmen Sie an den Endgeräten (PC, Laptop, Tablet bzw. SmartPhone,) die IP-Konfiguration gemäß dem IP-Adressierungsschema vor
5. Überprüfen Sie an den anderen Geräten (HMI, PLC, Switch im Produktionsnetz, WLAN-AP) die IP-Konfiguration gemäß dem IP-Adressierungsschema
6. Überprüfen Sie die Verbindungen physikalisch und logisch
7. Überprüfen Sie den Webzugriff auf die Automatisierungsgeräte (PLC, Switch im Produktionsnetz, WLAN-AP) mit HTTP und HTTPS.

Hinweis

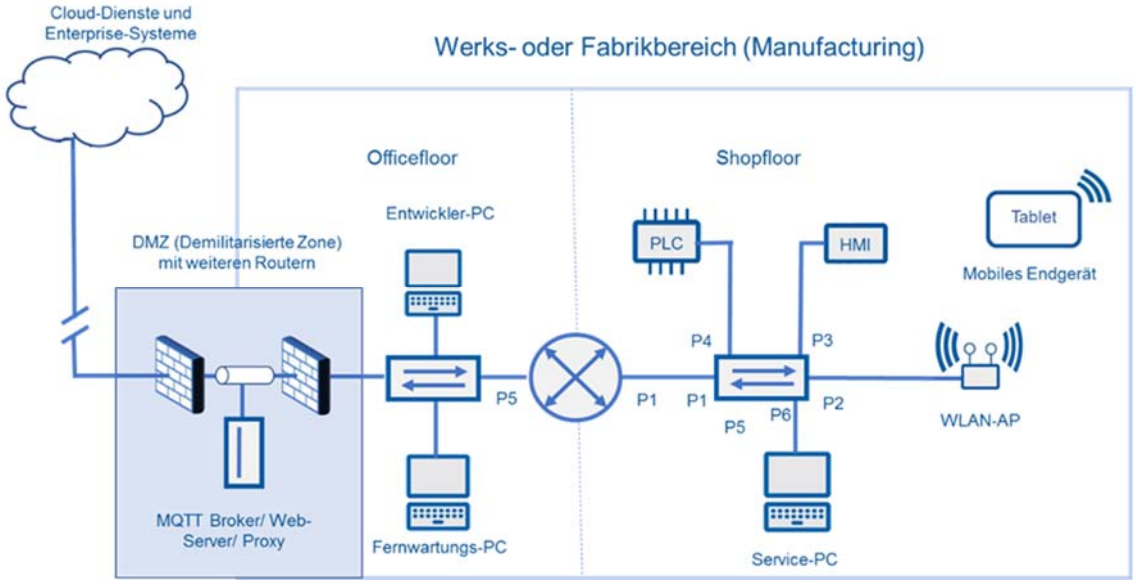
- Verwenden Sie ggf. herstellerspezifische und offene Tools wie das Primary Setup-Tool (PST), Proneta, cmd-Befehle

- SIMATIC S7 App
  - https://apps.apple.com/de/app/simatic-s7/id547218432)

Notizen

LAB 02 – SCHUTZBEDARF ERFASSEN UND SCHUTZMASSNAHMEN BEGRÜNDEN

Für eine spätere Risikobewertung im Rahmen des IT-Grundschutzes (BSI) durch externe Dienstleister muss im Vorfeld schon eine Analyse des Schutzbedarfes der vernetzten Anlage durchgeführt werden. Nach Festlegung der Sicherheitsanforderungen (z.B. normal, hoch, sehr hoch) sollen erste Maßnahmen realisiert werden.



Vorbereitung

- Funktionsfähige Laborübung 1

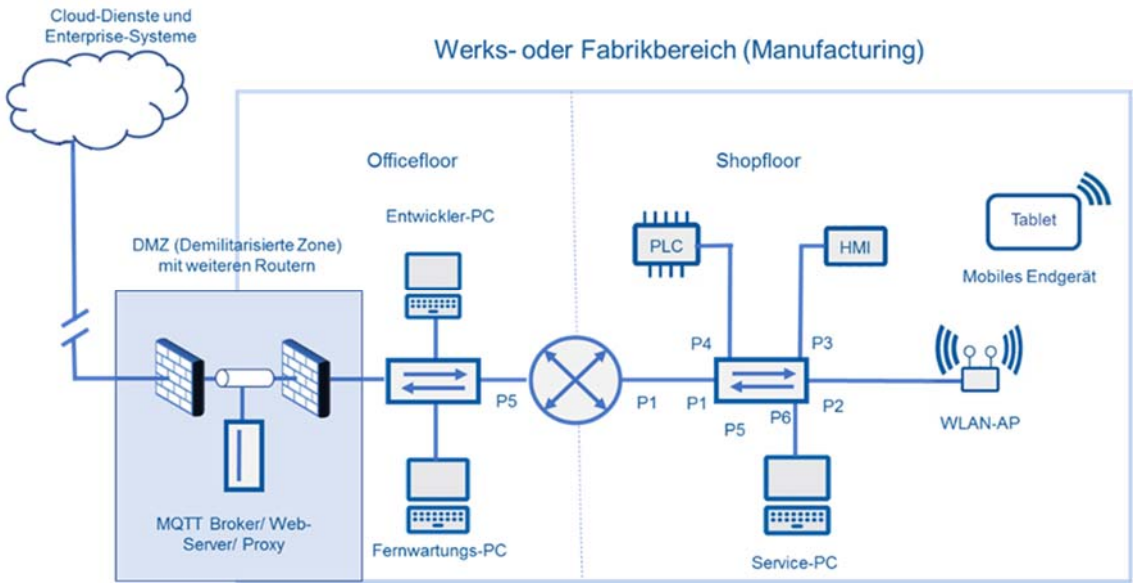
Aufgaben

1. Informieren Sie sich über die Struktur, den Schutzbedarf und die Sicherheitsanforderungen des vorliegenden CPS! Nutzen Sie dazu die vorliegenden Dokumentationen!
2. Der BSI – Grundschutz bietet als Entscheidungshilfe einen Baustein (Kürzel IND) für industrielle IT an. Informieren Sie sich genau über den Unterpunkt „IND.2.1 Allgemeine ICS-Komponente“!
3. Schlagen Sie nun Maßnahmen zur Umsetzung von „IND 2.1“ vor!

Notizen

LAB 03 – EINRICHTUNG EINES SICHEREN PLC-ZUGANGS

Die Anlagensicherheit im internen Netzwerk soll erhöht werden. Dazu wird eine sichere und dedizierte Verbindung zwischen der PLC, dem HMI und dem Service-PC auf dem Switch eingerichtet. Die WLAN-Geräte sollen von dieser Kommunikation ausgeschlossen werden. Nutzen Sie dazu die vom Switch unterstützte VLAN-Fähigkeit.



Vorbereitung

- Der Switch im Produktionsnetz hat die IP-Konfiguration und den Gerätenamen gemäß des IP-Adressenschemas
- Anpassung bzw. Deaktivierung der Windows-Firewall
- Webzugriff auf Switch sicherstellen bzw. testen
- Verfügbarkeit des Benutzernamens und des Passworts für Webzugriff auf den Switch im Produktionsnetz

Aufgaben

1. Verbinden Sie Ihren Service-PC mit dem Switch im Produktionsnetz an Switchport P8
2. Testen Sie die logische Verbindung vom Service-PC zu
    a. Switch
    b. WLAN-AP
    c. HMI
    d. PLC

3. Schalten Sie im Menüpunkt „Layer-2 → Ring-Redundanz“ die Ringredundanz ab (Häkchen entfernen), da Sie sonst nicht die Ports P1 und P2 für VLAN konfigurieren können.“
4. Konfigurieren Sie auf dem Switch im Produktionsnetz das portbasierte VLAN 1 „INT“ auf den Switchports P1, P7 und P8.
5. Konfigurieren Sie auf dem Switch im Produktionsnetz das portbasierte VLAN 10 „PRODUKTION_1“ auf den Switchports P1, P2 und P5
6. Konfigurieren Sie auf dem Switch im Produktionsnetz das portbasierte VLAN 20 „PRODUKTION_2“ auf den Switchports P3, P4 und P6
7. Testen Sie erneut die logische Verbindung vom Service-PC zu
    a. Switch im Produktionsnetz
    b. WLAN-AP
    c. HMI
    d. PLC
8. Stellen Sie sicher, dass das HMI aktuelle Prozessdaten mit der PLC austauscht
9. Verwenden Sie auf dem Service-PC Proneta zur Ermittlung von teilnehmenden Komponenten im Netz. Welche Komponenten finden Sie?

Hinweise

- Nutzen Sie für die VLAN-Konfiguration die bereitgestellten Hilfsmaterialien
- Das Web-Based-Management (WBM) des Switches ist nur über vlan1 erreichbar. Daher ist nach Teilaufgabe 4 eine Konfiguration nur noch über Port 1, 7 und 8 möglich.

Übersicht – Portbasierte VLAN-Konfiguration

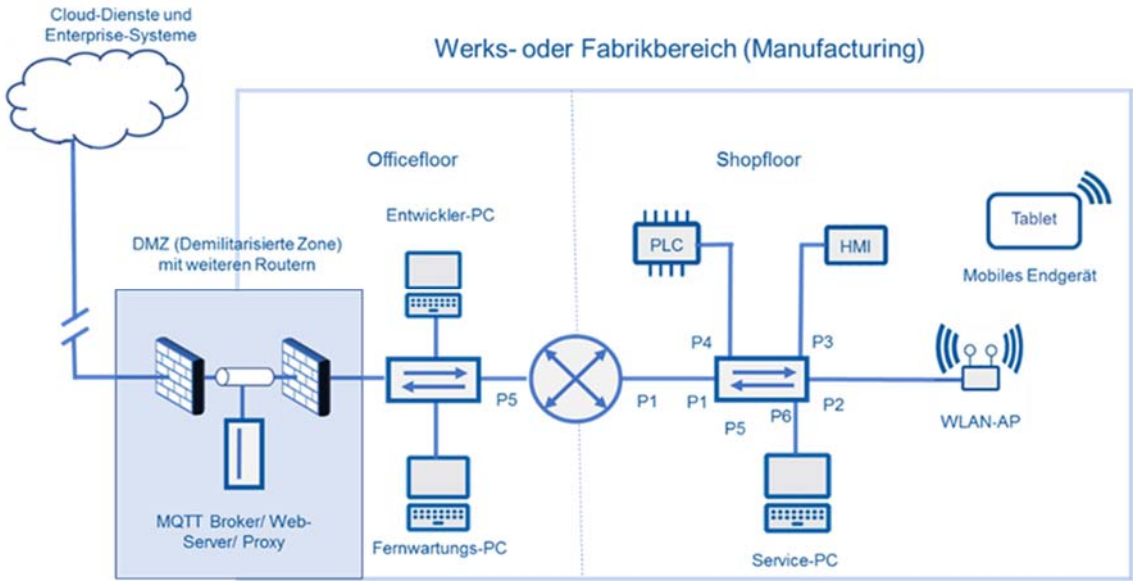
VLAN ID	Name	Ports
VLAN 1	INT	P1, P7, P8
VLAN 10	PRODUKTION_1	P2, P5
VLAN 20	PRODUKTION_2	P3, P4, P6

Notizen

LAB 04 – KOMMUNIKATION ZWISCHEN VLANS ERMÖGLICHEN

Der Techniker, der Wartungsaufgaben mit Hilfe des Service-PCs nachkommt, benötigt ein Firmware-Update für die PLC, das er von außerhalb des Produktionswerks bezieht.

Der Lösungsansatz soll an den zentralen Netzwerk-Komponenten umgesetzt werden und eine größtmögliche Flexibilität bieten.



Vorbereitung

- Konfigurationszustand aus LAB 03
- Vorbereitete Konfiguration inkl. Inter-VLAN-Routing und Trunk für den Router SCALANCE S615 (auf C-Plug oder als Konfigurations-Datei)

Aufgaben

1. Stellen Sie den Webzugriff auf den Switch im Produktionsnetz sicher
2. Voraussetzung für die die Kommunikation zwischen verschiedenen VLANs sind verschiedene IP-Netze für jedes VLAN. Passen Sie die IP-Konfiguration auf ALLEN Geräten des VLAN 10 und VLAN 20 gemäß des IP-Adressierungsschemas an. Denken Sie dabei auch an die Einstellung des jeweiligen Default-Gateways. Für das HMI und die PLC steht Ihnen das TIA-Portal, das PST und Proneta zur Verfügung. Den Switch im Produktionsnetz und den WLAN-AP können Sie nur mit dem PST oder Proneta konfigurieren (sind nicht in TIA projektiert).

3. Für die Verbindung zwischen dem Router (P1) und dem Switch (P1) ist eine „Trunk“-Verbindung erforderlich. P1 am Router ist bereits vorkonfiguriert. Passen Sie auch die Konfiguration am Port P1 des Switches an, damit die Trunkverbindung zustande kommt.
4. Verbinden Sie nun den Router (P1) mit dem Switch (P1) physikalisch mit einem geeigneten Medium.
5. Die Kommunikation zwischen allen relevanten Netzwerkkomponenten ist nun wieder möglich, Broadcasts sind jedoch weiterhin auf die jeweiligen VLANs begrenzt.
6. Testen Sie die Verbindung zwischen den beteiligten Komponenten mit einem geeigneten Werkzeug.
    a. Testen Sie mit dem Befehl *ping* und notieren Sie die Testergebnisse.
    b. Testen Sie mit dem Befehl *tracer*t und verwenden Sie die Ergebnisse, um damit die Verbindungspfade in die Topologie einzuzeichnen.

Hinweise

Befehl	**Beschreibung**
ping <IP-Adresse>	Verbindungstest auf IP-Ebene
tracert <IP-Adresse>	Darstellung der Routenverfolgung zum Ziel

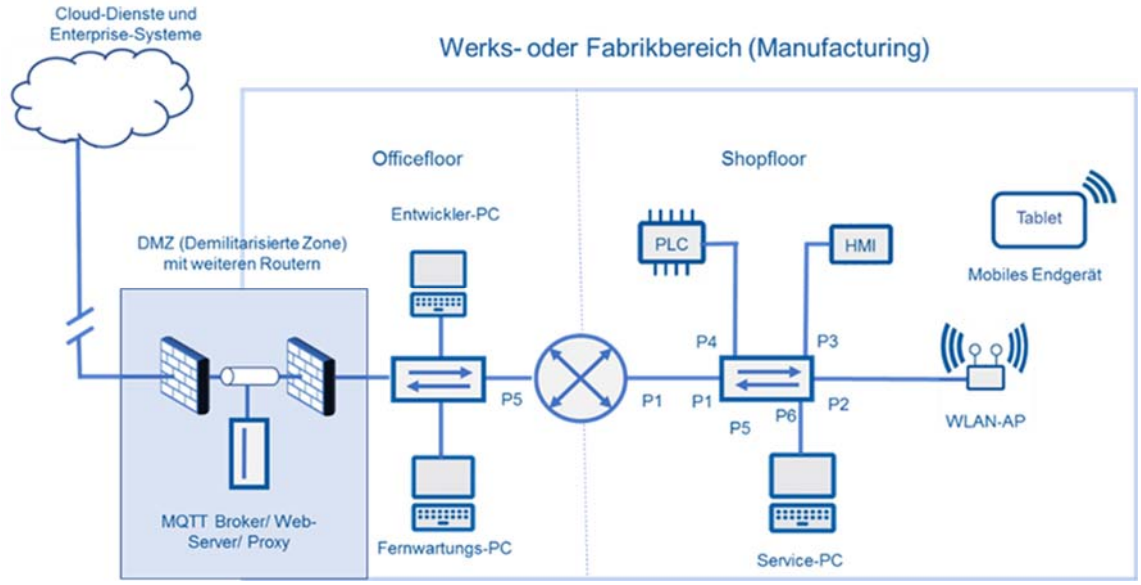
Notizen

LAB 05 – KOMMUNIKATION AM ROUTER EINSCHRÄNKEN

Anwender (z.B. Service-Techniker) sind gefordert, Sicherheitsrichtlinien nachzuvollziehen, damit sie Bedarfe (Funktion, Verfügbarkeit, Sicherheitsmängel, …) in ihrem Handlungsrahmen qualifiziert kommunizieren können.

Die Sicherheitsrichtlinien des Unternehmens fordern den gefilterten Datenverkehr z. B. je nach Dienst, Quelle und Ziel. Diese Sicherheitsrichtlinien werden u. a. am Router als Firewall-Regeln umgesetzt. Folgende Regeln sollen umgesetzt werden:

1. Dem Service-PC ist der Download (FTP) von Firmware aus dem Officefloor erlaubt.
2. Der Service-PC soll Zugriff über telnet (Port 23) auf den WLAN-AP haben.
3. Der Fernwartungs-PC soll Webzugriff (HTTP und HTTPS) auf den WLAN-AP haben.
4. Nur obige Regeln sind zulässig! Der restliche Datenverkehr zwischen den Netzen soll unterbunden sein.



Vorbereitung

- Konfigurationszustand aus Lab 04

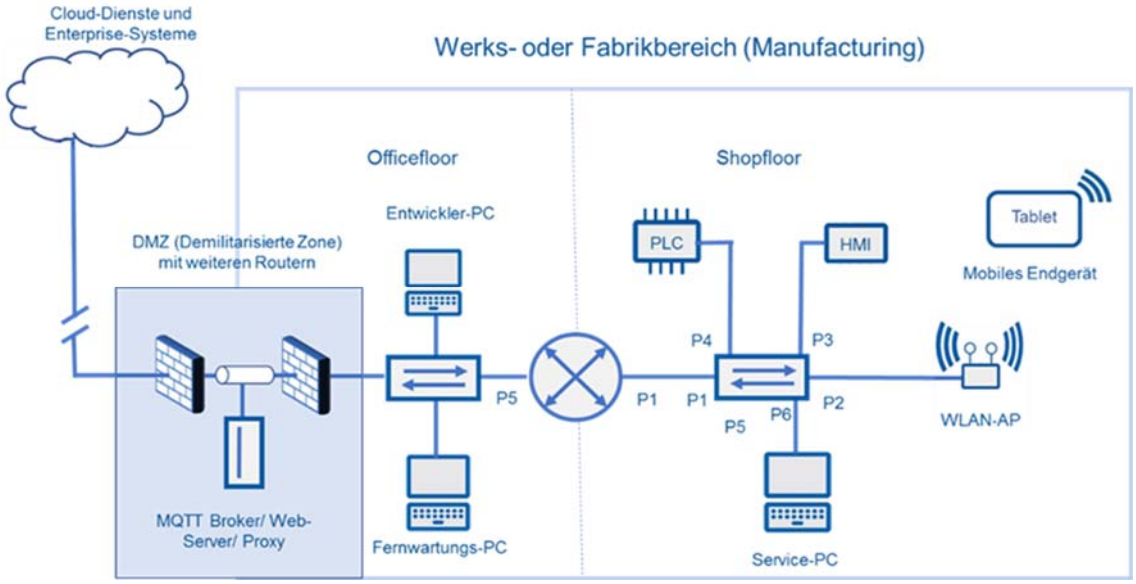
Aufgaben

1. Implementieren Sie die Firewall-Regeln mit Hilfe der bereitgestellten Anleitung
2. Testen Sie die Wirksamkeit jeder implementierten Firewall-Regel einzeln.
3. Untersuchen Sie die Kommunikation mit einem Traffic-Analyser (z. B. Wireshark)
4. Erhöhen Sie die Netzwerksicherheit in dem Sie den telnet-Zugriff vom Service-PC (VLAN 20) auf den WLAN-AP (VLAN10) unterbinden und nur das verschlüsselte Protokoll SSH zugelassen wird

Notizen

LAB 06 – SICHEREN WEBZUGRIFF EINRICHTEN

Für einen sicheren Webzugriff (https) ist eine Verbindung zum Switch einzurichten. Dies setzt eine Vertrauensstellung zwischen den Teilnehmern (Clients und Server) voraus, welche über ein Zertifikat nachgewiesen wird.



Voraussetzung

- Konfigurationszustand aus Lab 05
- XCA-Software zur Zertifikatserstellung
- Anleitung zur Erstellung einer zweistufigen Zertifikatshierarchie

Aufgaben

1. HTTPS nutzt Zertifizierungsstellen (CAs), welche die Gültigkeit von Zertifikaten garantieren. Im Zertifikat wird die tatsächliche Zugehörigkeit eines Domänennamens zur entsprechenden Organisation nachgewiesen. Webbrowser enthalten in ihrer Standardausstattung eine vorkonfigurierte Liste vertrauenswürdiger Zertifizierungsstellen, deren Zertifikate der Browser vertraut.
   Finden Sie die Zertifikate der CAs (Root-Zertifikate), denen Ihr Browser in seiner Grundausstattung vertraut.

2. Die Inhalte bzw. die Struktur eines digitalen Zertifikats sind im ITU-T-Standard X.509 festgelegt. Ein wichtiges Element eines Zertifikats ist ein digitaler Fingerabdruck. Dies ist ein eindeutiger Hash-Wert, der aus den Inhalten des Zertifikats und einem Schlüssel, der nur dem Ersteller bekannt ist (privat Key), erzeugt wird. Gehen Sie davon aus, dass die Fingerabdrücke in der Tabelle (siehe Hinweise) für die erwähnten Organisationen gültig sind. Rufen Sie mit Ihrem Browser die Webseiten auf und vergleichen Sie die Fingerprints der Tabelle (Stand 02.06.2020) mit den Fingerprints der entsprechenden Zertifikate.
3. Als Service-Techniker müssen Sie sicherstellen, dass Sie auf die Weboberfläche desjenigen Switches (oder einer beliebigen anderen Komponente) zugreifen, den Sie auch tatsächlich konfigurieren wollen. Beispielsweise könnten sonst das Zugangspasswort zur Weboberfläche oder andere sensible Konfigurationsdaten von Dritten ausgespäht werden. Erzeugen Sie zu diesem Zweck eine Zertifikats-Struktur, der Sie vertrauen. Gehen Sie dabei wie folgt vor:
    a. Erzeugen Sie ein Zertifikat Ihrer CA (Root-Zertifikat)
    b. Erzeugen Sie ein Serverzertifikat für den Switch
    c. Installieren Sie das Serverzertifikat auf dem Switch
    d. Machen Sie das Root-Zertifikat auf Ihrem Windowsrechner bekannt, damit der Internetexplorer dem Serverzertifikat vertraut.
    e. Machen Sie das Root-Zertifikat im Firefox bekannt, damit dem Serverzertifikat vertraut.

    Details zur Aufgabe 3 finden Sie in der Anleitung zur Erstellung einer zweistufigen Zertifikatshierarchie
4. Überprüfen Sie nach den Schritten c-e den Erfolg Ihrer Installation/Konfiguration

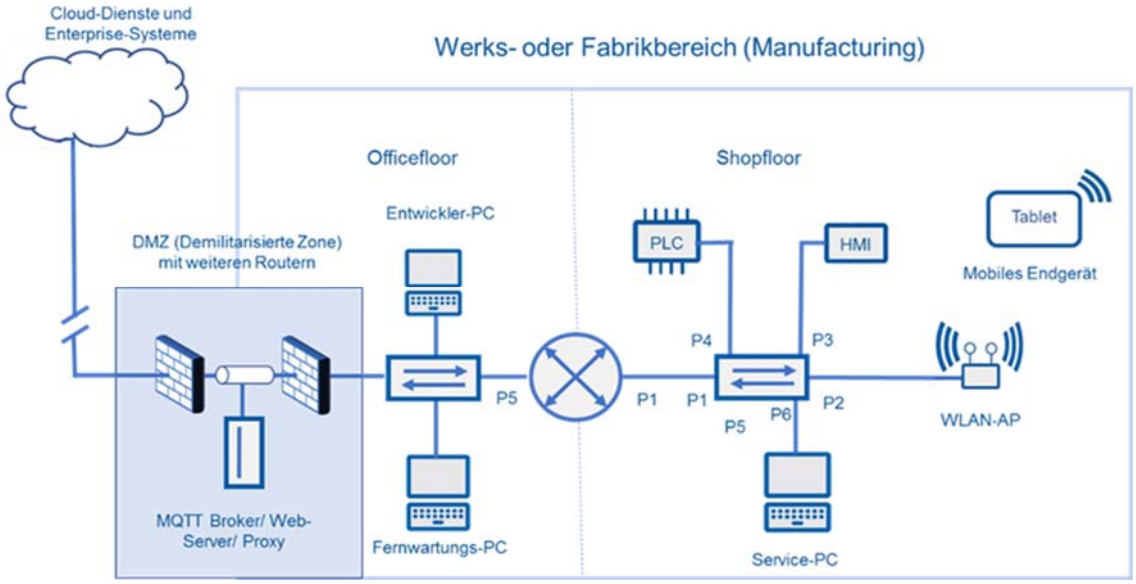
Hinweise

Organisation	Domänenname	SHA-1 Fingerprint auf dem Zertifikat (Stand: 02.06.2020)
wikipedia	*.wikipedia.org	82:BC:F2:74:FD:93:D2:AD:E7:60:EB:BA:D2:A3:63:60:16:1F:6C:62
ALP Dillingen	alp.dillingen.de	AB:8B:6D:60:1F:8A:A4:EA:66:75:9F:BA:49:50:26:5F:FF:F8:D3:42
SZ	www.sueddeutsche.de	95:FF:AE:56:9B:4F:DA:47:55:40:F4:F5:49:FA:15:CA:C6:68:BD:08

Notizen

LAB 07 – STEUERUNG DES PROZESSES AUS DER LEITEBENE

Auch aus der zentralen Leitstelle soll das Befüllen und Entleeren des Mischbehälters in der Produktion einer Zweigstelle gesteuert werden und der Status des Füllzustands angezeigt werden.



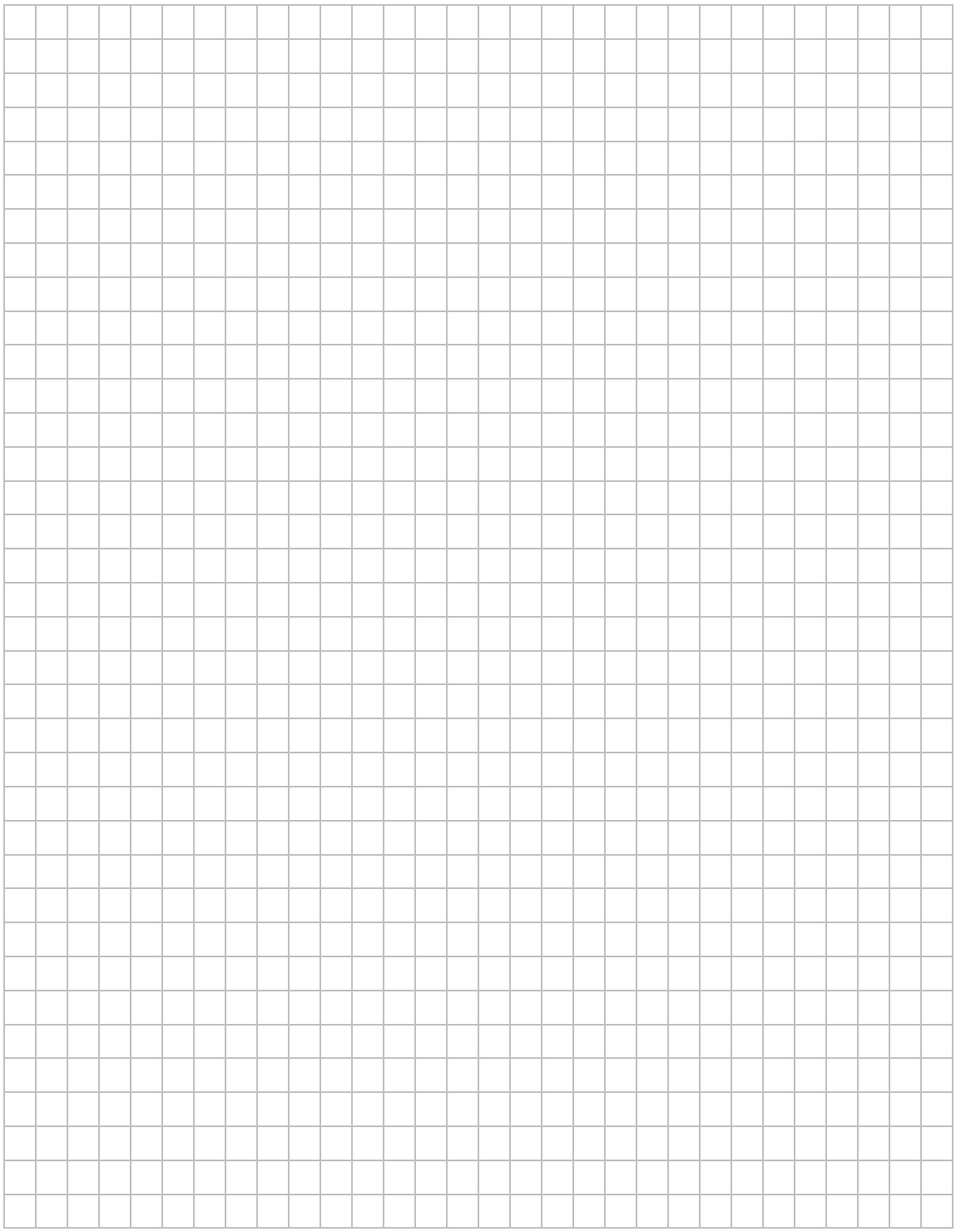
Vorbereitung

- Funktionszustand der vorausgehenden Laborübung

Aufgaben

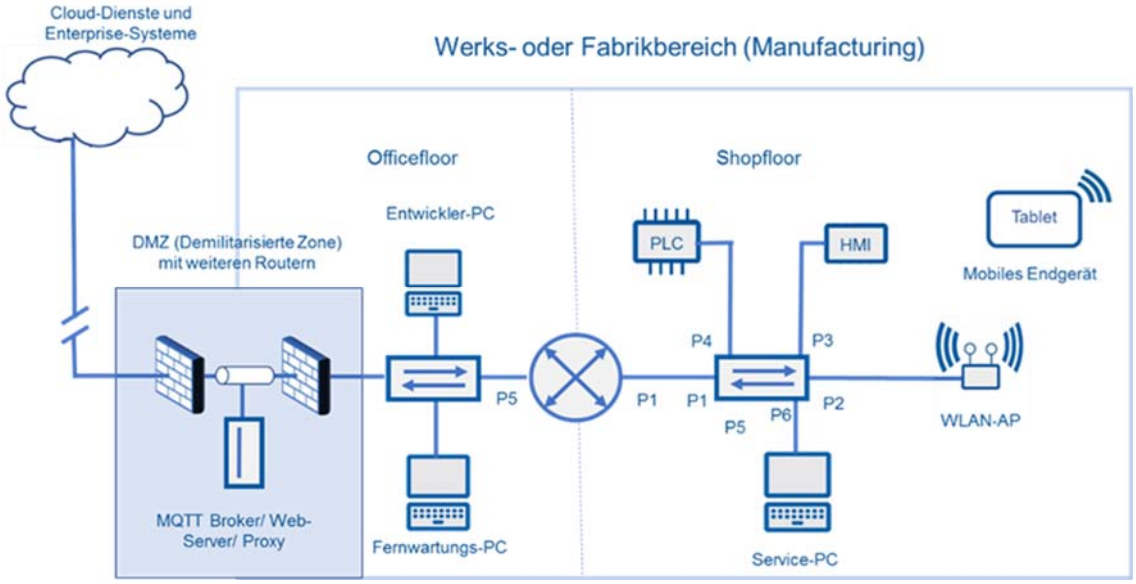
1. Konfigurieren Sie in der Projektierungsumgebung die Berechtigungen für den Zugriff auf die Prozesswerte aus der Managementebene.
   - Füllen ein/aus erhält Schreib-Lese-Zugriff
   - Füllstand nur Lesezugriff
   - Zustand der Ventile Lesezugriff
2. Testen Sie mit einem OPC UA-Client den Zugriff auf die Prozessdaten

Notizen



LAB 08 – OPC UA DATEN IN EINE TABELLE SCHREIBEN

Zur Archivierung und statistischen Auswertung sollen Prozessdaten mit Zeitstempel in eine Tabelle gespeichert werden.



Vorbereitung

- Funktionszustand der vorausgehenden Laborübung

Aufgaben

1. Stellen Sie eine Verbindung zum OPC UA-Server im Client her.
2. Erstellen Sie eine Excel-Tabelle „Füllstand.xlsx“ mit den Spalten „Zeit“ und „Füllstand“ im Tabellenblatt „Tabelle1“.
3. Konfigurieren Sie nach Anleitung die nötigen Verbindungen und Transferobjekte mit der Software Inray OPC-Router.
4. Stellen Sie in der Excel-Tabelle die Daten grafisch dar und prüfen Sie die Plausibilität.

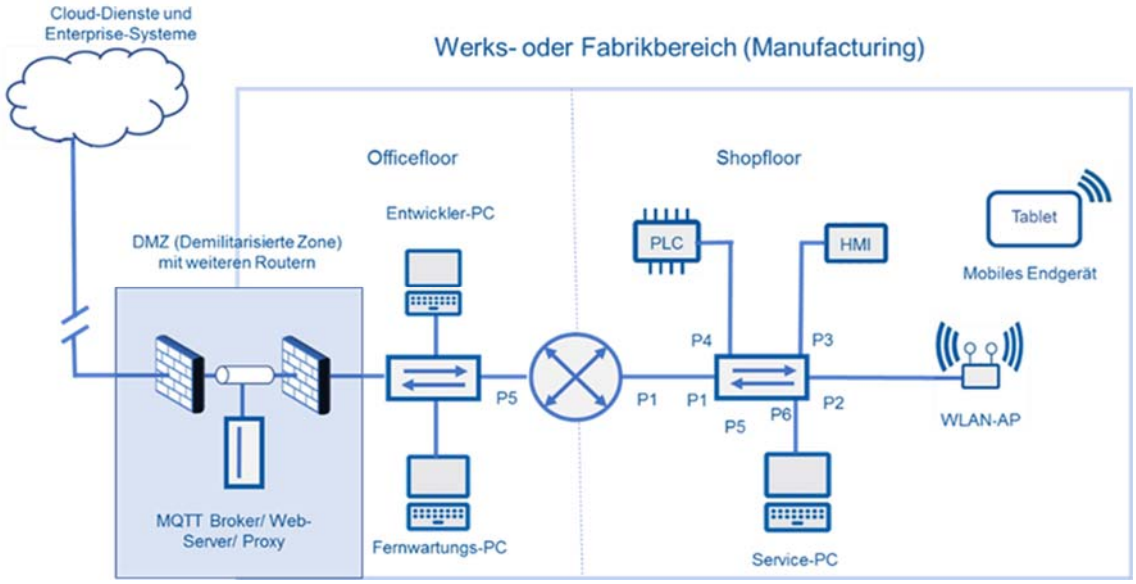
Hinweis

- Installierter OPC UA-Client (Inray-Router) und installiertes MS-Excel
- Detaillierte Konfigurationsschritte sind der Anleitung zu entnehmen

Notizen

LAB 09 – OPC UA DATEN IN EINE DATENBANK SCHREIBEN

Zur Archivierung und statistischen Auswertung sollen Prozessdaten mit Zeitstempel in eine Datenbank gespeichert werden. Im Gegensatz zu einer Tabelle bietet die Datenbank eine zentrale Datenablage und u. a. auch ein Rollen und Rechtekonzept.



Vorbereitung

- Funktionszustand der vorausgehenden Laborübung

Aufgaben

1. Stellen Sie eine Verbindung zum OPC UA-Server im Client her.
2. Testen Sie die Verbindung zur Datenbank vom OPC-Client mit den Zugriffsparametern.
3. Konfigurieren Sie nach Anleitung die nötigen Verbindungen und Transferobjekte mit der Software Inray OPC-Router.
4. Testen Sie über einen Datenbank-Client ob zeitaktuelle Daten eingetragen wurden und prüfen Sie die Plausibilität.

Hinweise

- Installierter OPC UA-Client (Inray-Router) und installierte und konfigurierte MySQL-Datenbank/MariaDB
- Detaillierte Konfigurationsschritte sind der Anleitung zu entnehmen

- Zur Visualisierung der Daten bietet sich eine erweiterte Übung im Umgang mit SQL und PHP an.

Notizen

AUSSTATTUNG FÜR LABORÜBUNGEN

Zur Durchführung der Laborübungen wird neben den Computern und Notebooks der Schulen folgende Ausstattung von der Fachgruppe „Datenkommunikation“ empfohlen. Damit ist u. a. die didaktische Eignung und Industrietauglichkeit gewährleistet. Bei Abweichungen von den Ausstattungsempfehlungen ist auf diese Kriterien zu achten, damit die beabsichtigten Intentionen der Laborübungen für Lehrerfortbildung und Unterricht erreicht werden.

Nr.	Bezeichnung	Menge	Lab
1	Router Siemens SCALANCE S615: 6GK5615-0AA00-2AA2	1	01-10
2	Switch (min. 6 Port) Siemens SCALANCE z.B XC208	2	01-10
3	PLC, z. B. LOGO 8 oder CPU S7 mit Profinet	1	01-10
4	HMI z. B. TP 700 Comfort oder LOGO TDE mit IE-Schnittstelle	2	01-10
5	Spannungsversorgung	1	01-10
6	Montagematerial	1	01-10
7	Programmiersoftware z. B. TIA V14, PST, Proneta	1	01-10
8	Simulationsboard zur Prozessimulation	1	01-10
9	Patchkabel pro Arbeitsplatz	9	01-10
10	ASi-Master z. B. Kommunikationsmodul ASi Master	1	01-10
11	ASi-Slave, Signallampe, Tastermodul	3	01-10
12	ASi-Netzteil	1	01-10
13	OPC UA Server z. B. IBH-Link OPC UA oder interne OPC UA Server von PLCs	1	02-10
14	OPC UA Client UA Expert, Inray OPC UA Router		03-10
15	Datenbank, z. B. mySQL, MS-Excel		08-09

DIGITALE TRANSFORMATION - FORTBILDUNGSMODULE