Retrofitprojekte aus der Praxis - Industrial Security
Zugangsberechtigung, Authentifizierung, Benutzermanagement

PILZ
THE SPIRIT OF SAFETY

AUTOMATION
ON TOUR
with Pilz

Agenda

01 Industrial Security

02 Systeme für Zugangs- und Zugriffsberechtigung

03 Retrofit Lösungen für Zugangsberechtigung und Authentifizierung

04 Retrofit Lösungen für Zugriffsberechtigungen auf Schnittstellen und Systeme

01

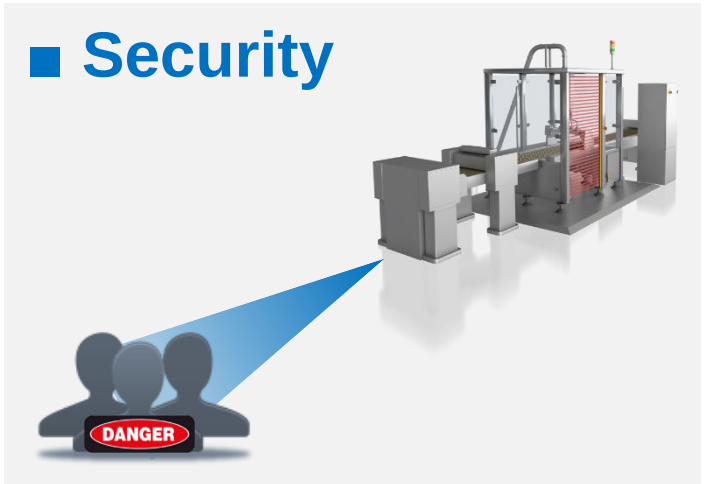
Industrial Security

Safety & Security

Zwei Seiten einer Medaille

Safety

- Maschinensicherheit ist die Grundlage für eine sichere Kooperation von Mensch und Maschine
- Schutz der Mitarbeiter vor den Gefahren, die von der Maschine ausgehen z.B. gefährliche Bewegungen
- Reibungsloser Betrieb und sichere Produktion



Security

- Schutz der Maschine vor Manipulation, Fehlbedienung oder gar Sabotage
- Zunehmende Vernetzung von Maschinen und Komponenten machen dies erforderlich → Industrie 4.0
- Schutz der Maschine vor unbefugten Zugriffen
- Sicherstellung der Maschinensicherheit + Produktion

Industrial Security

Zugangsschutz an Maschinen & Anlagen

■ „Physische“ **Security**

■ Physischer „Zugang“

■ „Informationstechnische“ **Security**

■ „Zugriff“ auf Systeme und Daten

Schutz der Maschine vor dem physischem Zugang durch Personal.
z:B. Schutz gegen unauthioriserten Zugang und Bedienfehler.

Schutz der industiellen Systeme und Daten vor Zugriffen.
z.B. Schutz gegen unauthorisierten Remote – Access

Industrial Security

Was versteht man unter Industrial Security?

Industrial Security → Schutz von Produktions- und Industrieanlagen vor absichtlich (Cyber-Angriff) oder unabsichtlich (Bedienfehler) herbeigeführten Fehlern.

Sicherheit von Steuerungsfunktionalitäten und -netzwerken von Produktion- und Industrieanlagen in den Bereichen Fabrikautomation und Prozesssteuerung.

- Anlagen sind heute zunehmend sehr stark mit Informationstechnologie sowie mit externen Netzwerken vernetzt → Gefahr von Cyber-Angriffen
- Manipulation von Maschinen und deren Funktionen ist möglich
- Gefährdung der Maschinensicherheit und es Bedienpersonals möglich
- Ungeregelter Zugang und Zugriff auf Maschinen und Funktionalitäten → Fehlbedienung + Fehlfunktion

IEC 62443 „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und System“ → beste Orientierungshilfe dar, um Industrial Security effektiv umzusetzen.

Office IT
Bewährte Security Mechanismen und Funktionalitäten

↓

Industrial Security

Industrial Security

Was ist das Ziel von Industrial Security?

Gewährleistung der Verfügbarkeit von Maschinen und Anlagen, sowie der Integrität und Vertraulichkeit von maschinellen Daten und Prozessen

Angreifer nutzen häufig bestehende Schwachstellen, um in Steuerungsnetzwerke einzudringen oder den Ablauf der Prozesse zu stören bis hin zum Anlagenstillstand oder Manipulation von Sicherheitsfunktionen.

- Verhinderung des unbefugten Zugriffs auf das Steuerungsnetzwerk
- Erkennung von Schwachstellen, extern aber auch intern
- Analyse der Schwachstellen
- Behebung der Schwachstellen
- Implementierung von Schutzmechanismen und Absicherung von Zugriffen
- Gewährleistung von Datensicherheit und Investitionsschutz
- Implementierung von Maßnahmen durch den Anlagenbetreiber

02

Systeme für Zugangs- und Zugriffsberechtigung

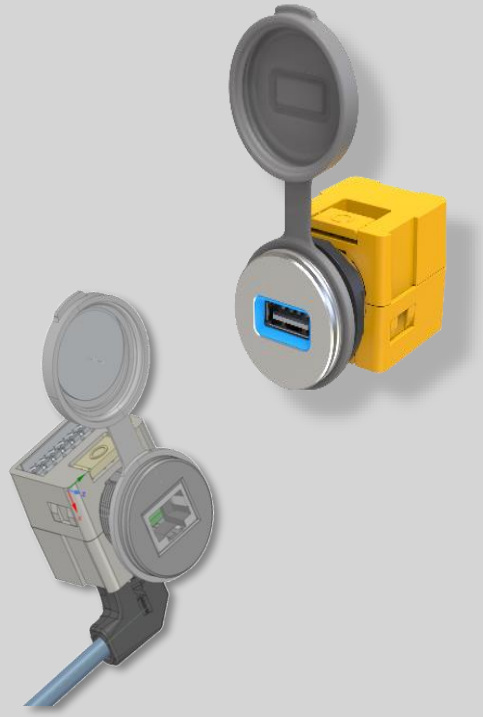
Systeme für Zugangs- und Zugriffsberechtigung

I.A.M → Identification & Access Management

Identifikation	Qualifikation & Ausbildungsgrad		Zugriff / Zugang
			
Wer bin ich?	***Was ist meine Qualifikation?***	***Was ist mein Ausbildungsniveau?***	***Was sind meine Berechtigungen?***
→ Person → **Hardware** → **Prozess**	→ Bediener → Einrichter → Service → …	→ Anfänger → Experte → …	→ Roboter Level = 2 → Zugang Tür 4 = Ja → Zugriff HMI Seite 14 → Sprache = deutsch → …

Systeme für Zugangs- und Zugriffsberechtigung

I.A.M → Identification & Access Management

Abfrage Berechtigung & Authentifizierung	Zugangskontrolle Freigabe / Sperre	Zugriffskontrolle Schnittstellen	Zugriffskontrolle Systeme + Daten
			

03

Retrofit Lösungen für Zugangsberechtigung und Authentifizierung

Retrofit Lösungen für Zugangsberechtigung und Authentifizierung

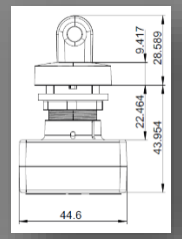
PITreader – Übersicht wichtigste Eigenschaften

Voll ansteuerbarer Multicolor LED Ring zur Anwenderinformation.

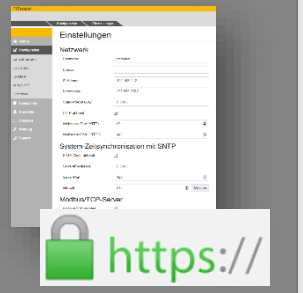
Authentifizierung über frei beschreibbare Transponder Schlüssel in RFID Technik.

Zertifizierter Security Chip integriert: MIFARE Plus EV1 von NXP.

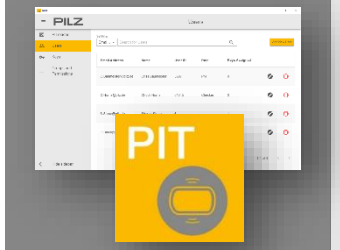
Ethernet Schnittstelle (OPC UA server, REST Api, 24V Ausgang, serielle Verbindung zu PIT m4 SEU, 24V Spannungsversorgung.



Standard Einbau-Maß von 22,5mm. Geringe Einbautiefe von nur 45mm.



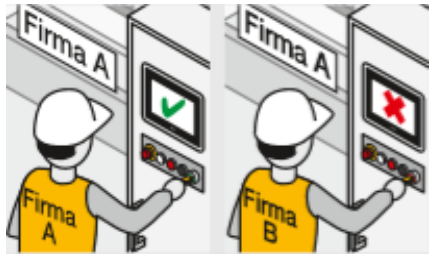
Konfiguration aller Funktionen über securen, integrierten Webserver. Programmieren der Transponder.



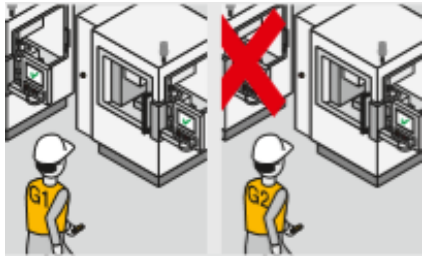
Datenbank Tool zum effizienten managen von Transpondern und Anwendern: PIT Transponder Manager.

Retrofit Lösungen für Zugangsberechtigung und Authentifizierung

PITreader – Umfassende Funktionen

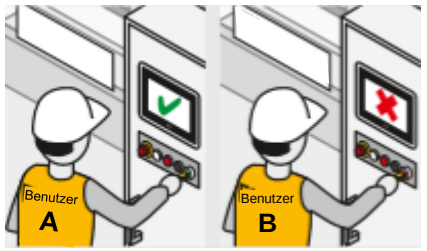


Basic / OEM Coding

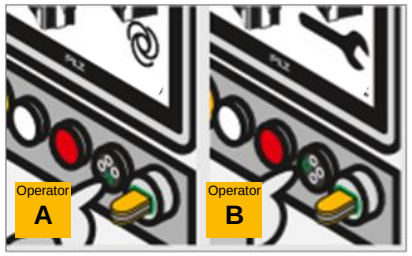


Gruppenbasiertes Rechtemanagement

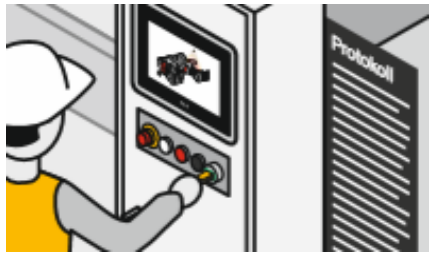
Zeitliche Berechtigung



Einzelauthentifizierung



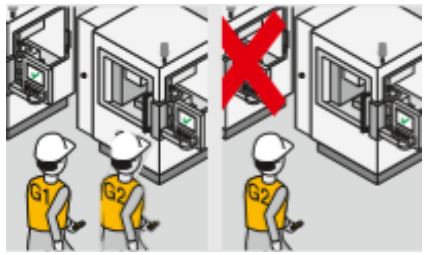
Sichere Betriebsartenwahl



Protokollierung der Aktionen

Blockierliste

Benutzerdefinierte Berechtigung



4 Augen Prinzip

Industrial **Security**

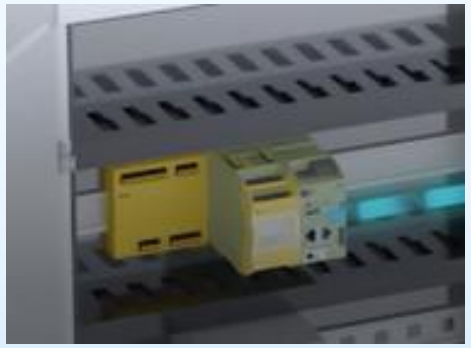
Safety

Retrofit Lösungen für Zugangsberechtigung und Authentifizierung

PITreader – Applikationsmöglichkeiten

HMI / IPC / Visualisierung

→ Personalisierte Anwender Identifikation (Passwort Ersatz)
→ Regelung von Editier-/ Leseberechtigungen
→ Anzeige von Seiten
→ Anwendersprache umschalten



Steuerung / SPS

→ Funktionen freischalten
→ Freigaben erteilen
→ Varianten umschalten
→ Rezepte umschalten

Tür Authentifizierung

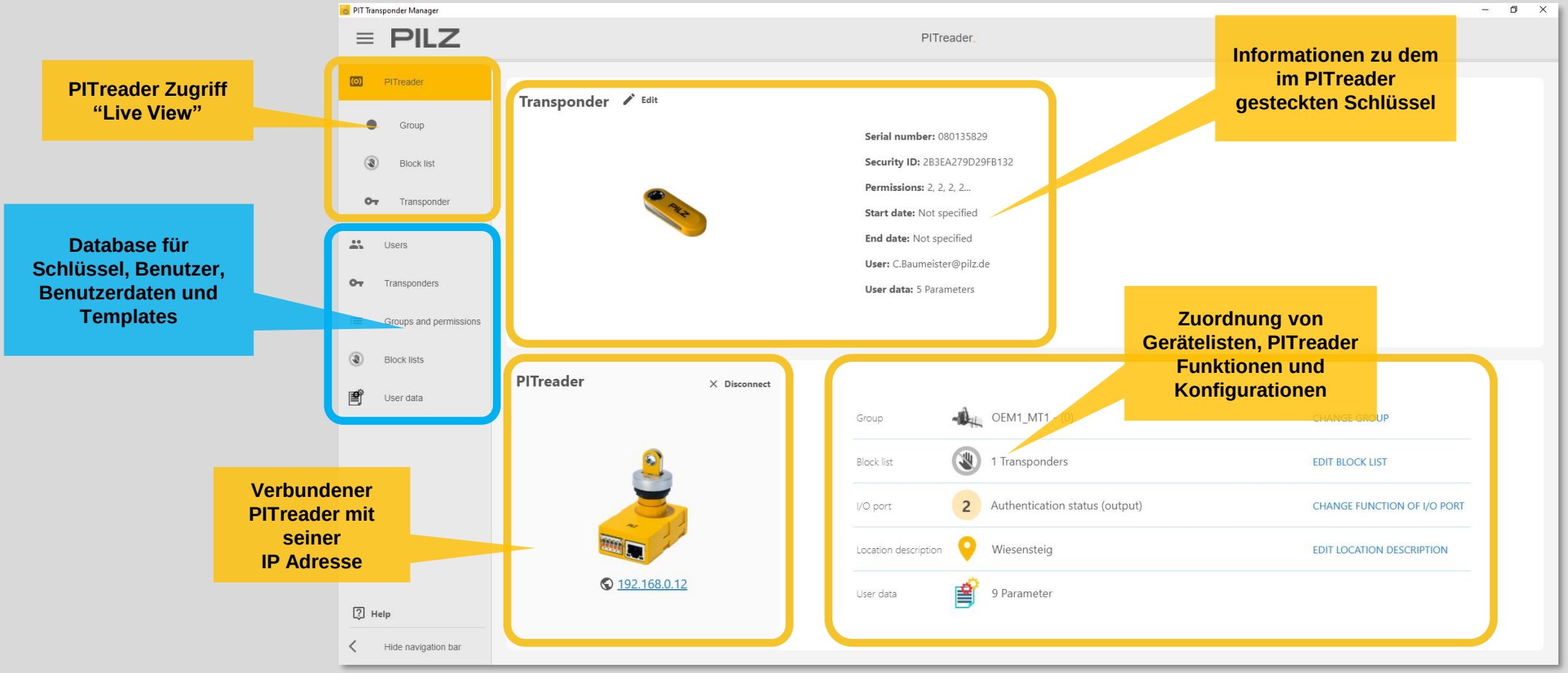
→ Zugangsberechtigungs-management für industrielle Türsysteme
→ Nur berechtigte Personen haben Zutritt

(Sichere) Betriebsartenwahl

→ Zugangsberechtigungs management für die funktional sichere Betriebsartenwahl
→ Nur autorisiertes & qualifiziertes Personal kann Betriebsarten sicher umschalten

Schlüsselverwaltung mit PIT Transponder Manager

PIT Transponder Manager = Verwaltung von Schlüsseln + PITreader



PIT Transponder Manager

Benutzermanagement + Schlüsselmanagement

Benutzerdatenbank

E-Mail-Adresse	Name	Anwender-ID	Rolle	Zugeordnete Schlüssel
abc@pilz.de	abc	001	SET_ALL	1
def@pilz.de	def	002	OP_1	1
ghi@pilz.de	ghi	003	OP_2	1
jkl@pilz.de	jkl	004	OP_3	0
mno@pilz.de	mno	005	OP_4	1
pqr@pilz.de	pqr	006	OP_5	1
stu@pilz.de	stu	007	OP_SUP	1

Zuordnung ↕ Verknüpfung

Schlüsseldatenbank

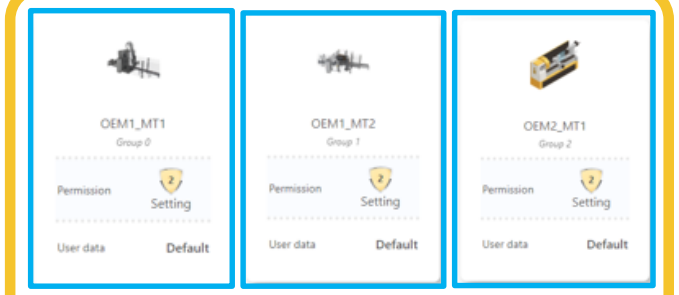
Serien-Nr.	Security-ID	Berechtigungen	Start	Ende	Anwender
000673192	EF95F1C834883006	Alle 4	NF	NF	abc@pilz.de
051372968	3231DB1D7F5C392A	2,4,1,3	17.10.2022	19.10.2022	def@pilz.de
734263912	53E859FC131F4E42	Alle 3	17.10.2022	19.10.2022	ghi@pilz.de
078835493	Z51D8617H56J7891	Alle 2	17.10.2022	19.10.2022	jkl@pilz.de
003294152	Q864T3761S753P51	2,2,3,4	01.10.2022	05.10.2022	mno@pilz.de
075438134	8IOP5374K65F168B	3,3,4,5	NF	NF	pqr@pilz.de

- Datenimport von gestecktem Schlüssel
- Blockierliste, Zeitlich begrenzte Berechtigung etc.

Programmierung Maschinengruppenberechtigung

Schlüsseldatenbank

Serien-Nr.	Security-ID	Berechtigungen	Start	Ende	Anwender
000673192	EF95F1C834883006	Alle 4	NF	NF	abc@pilz.de
051372968	3231DB1D7F5C392A	2,4,1,3	17.10.2022	19.10.2022	def@pilz.de
734263912	53E859FC131F4E42	Alle 3	17.10.2022	19.10.2022	ghi@pilz.de
078835493	Z51D8617H56J7891	Alle 2	17.10.2022	19.10.2022	jkl@pilz.de
003294152	Q864T3761S753P51	2,2,3,4	01.10.2022	05.10.2022	mno@pilz.de
075438134	8IOP5374K65F168B	3,3,4,5	NF	NF	pqr@pilz.de

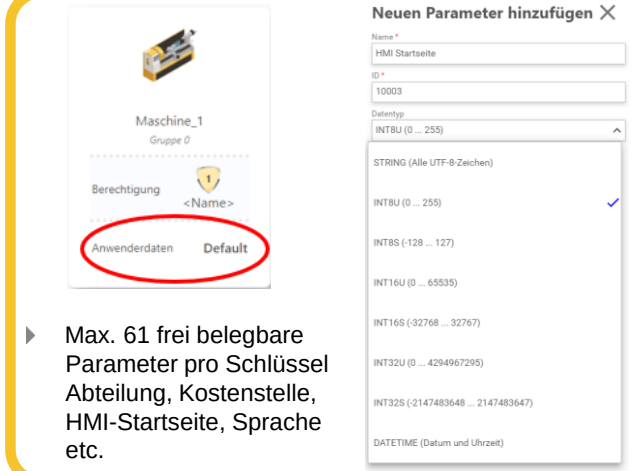


- Vergabe von unterschiedlichen Berechtigungen für mehrere Maschinen (max. 80) auf einem Schlüssel
- Maschine 1 → Automatik, Maschine 2 → Reinigung Maschine 3 → Einrichten usw.

Programmierung Benutzerdatenbereich

Schlüsseldatenbank

Serien-Nr.	Security-ID	Berechtigungen	Start	Ende	Anwender
000673192	EF95F1C834883006	Alle 4	NF	NF	abc@pilz.de
051372968	3231DB1D7F5C392A	2,4,1,3	17.10.2022	19.10.2022	def@pilz.de
734263912	53E859FC131F4E42	Alle 3	17.10.2022	19.10.2022	ghi@pilz.de
078835493	Z51D8617H56J7891	Alle 2	17.10.2022	19.10.2022	jkl@pilz.de
003294152	Q864T3761S753P51	2,2,3,4	01.10.2022	05.10.2022	mno@pilz.de
075438134	8IOP5374K65F168B	3,3,4,5	NF	NF	pqr@pilz.de



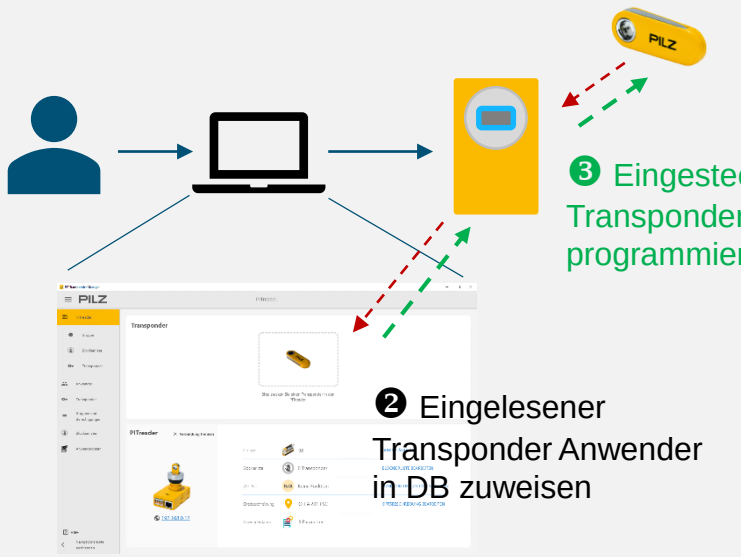
- Max. 61 frei belegbare Parameter pro Schlüssel Abteilung, Kostenstelle, HMI-Startseite, Sprache etc.

User Authentication Service - Ausblick

Einsatzszenario: heute

Verwaltung

❶ Eingesteckter Transponder in Transponder Manager DB einlesen



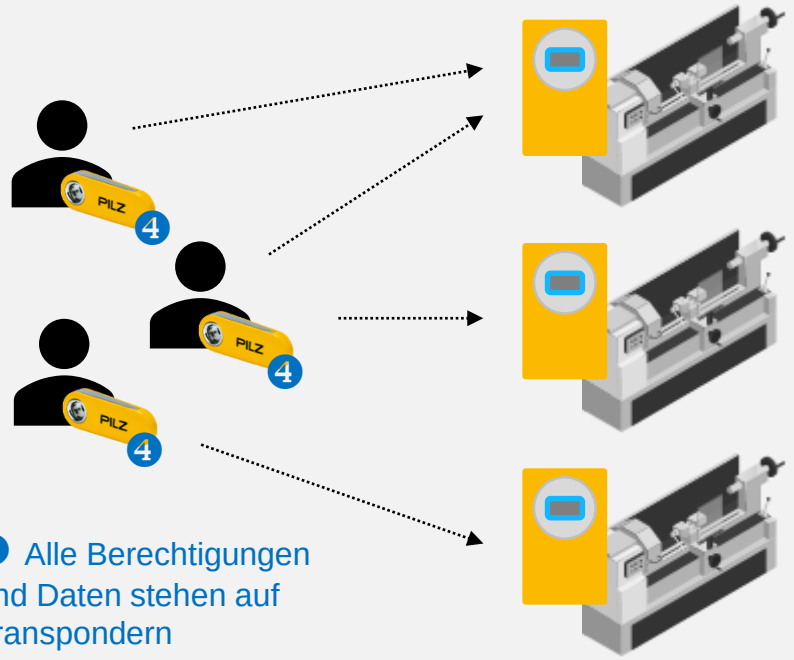
❸ Eingesteckten Transponder programmieren

❷ Eingelesener Transponder Anwender in DB zuweisen

PIT Transponder Manager

Bei Berechtigungs-Änderungen muss Transponder entsprechend in der Verwaltung neu beschrieben werden

Fertigung



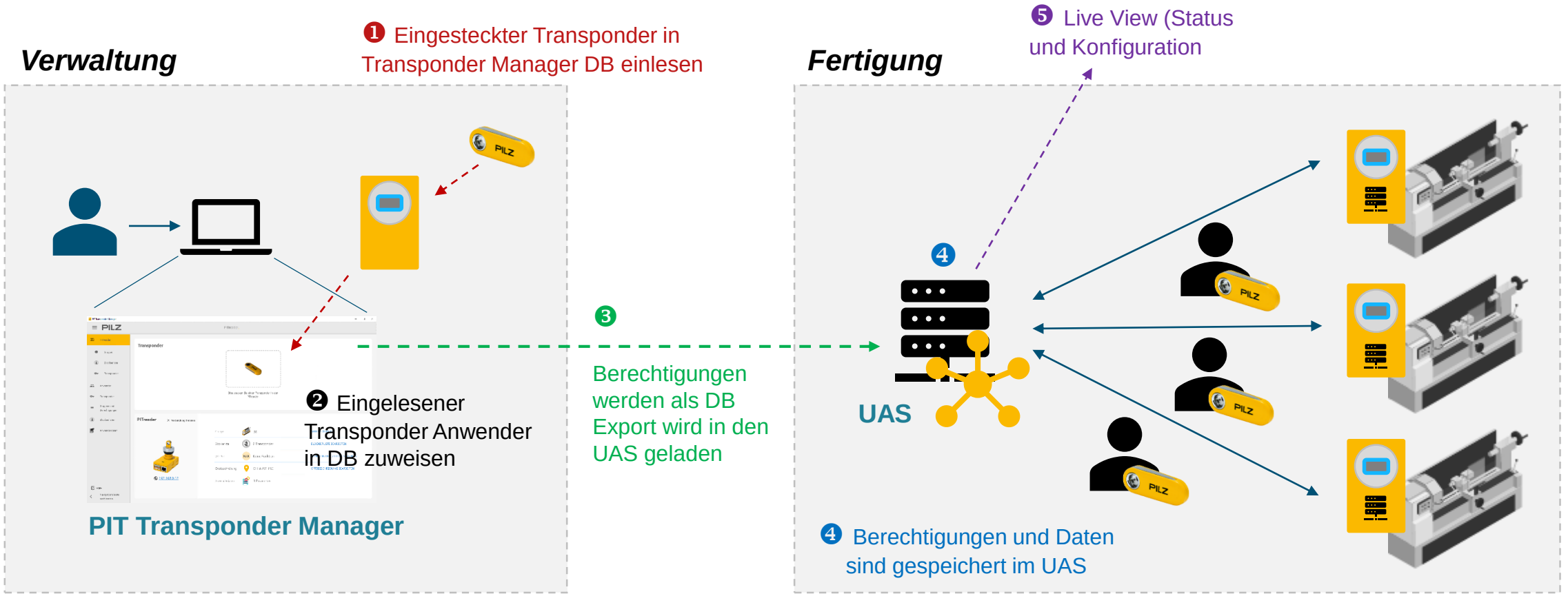
❹ Alle Berechtigungen und Daten stehen auf Transpondern

→ Blockierliste (z.B. verlorene Transponder) muss auf jedem Gerät „manuell“ aktualisiert werden.

Administrator *Transponder Nutzer*

User Authentication Service - Ausblick

Einsatzszenario: mit User Authentication Service



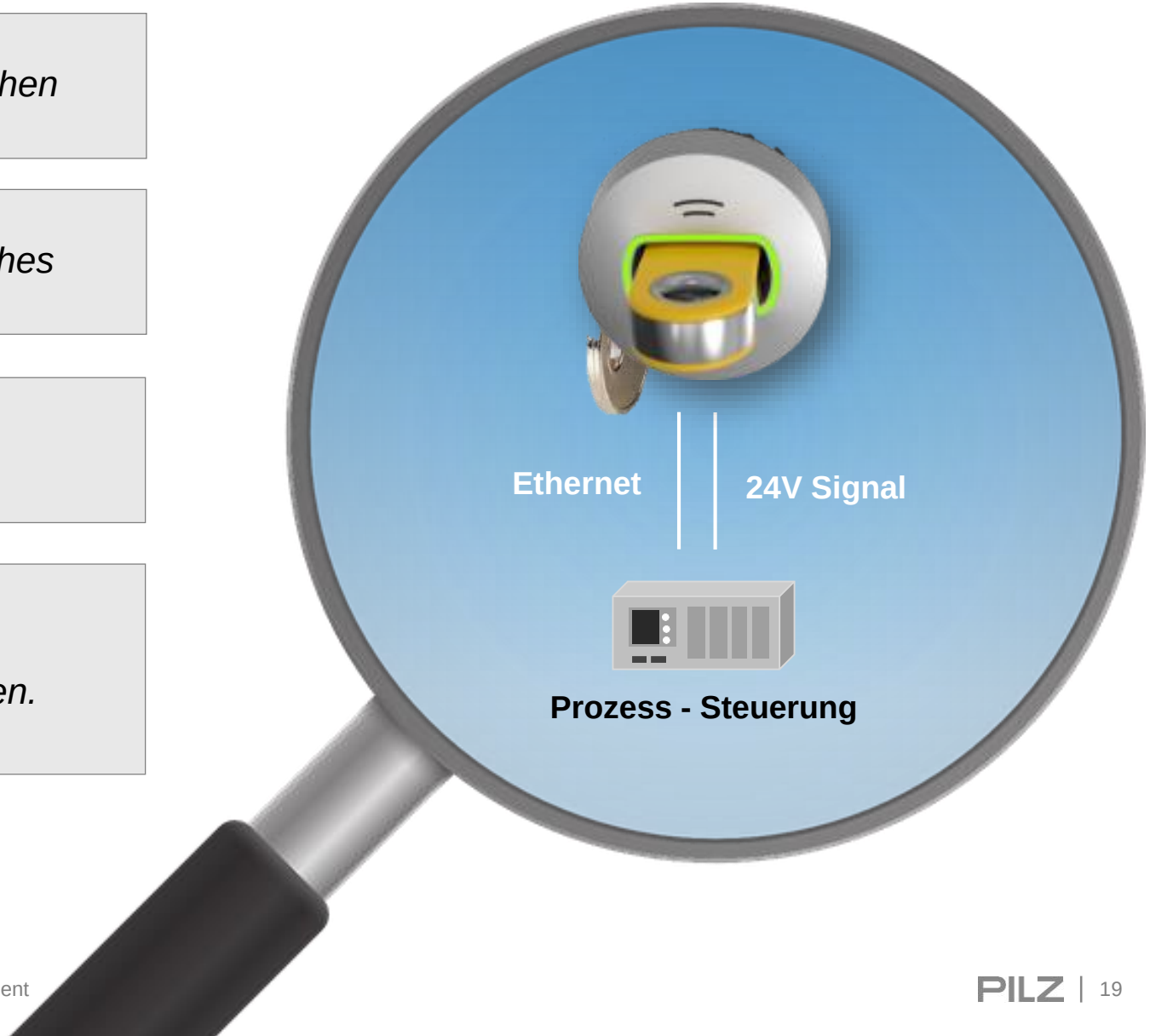
Praxisbeispiel 1.1: Security Retrofit an einer Alt-/ Neumaschine

Situation:
Eine Spezial-Funktion wird über einen mechanischen Schlüsselschalter ein- / ausgeschalten.

Maßnahme:
Schlüsselschalter durch PITreader als elektronisches Schloss ersetzen.

Realisierungs-Aufwand: ***Sehr gering***.
Nur 1:1 Tausch, bestehende Verdrahtung bleibt.

Vorteile:
- *Individualisierung des Zugriffes.*
- *Neue Schlüssel können einfach erzeugt werden.*
- *Bei Schlüsselverlust: Zugriffe sperren.*



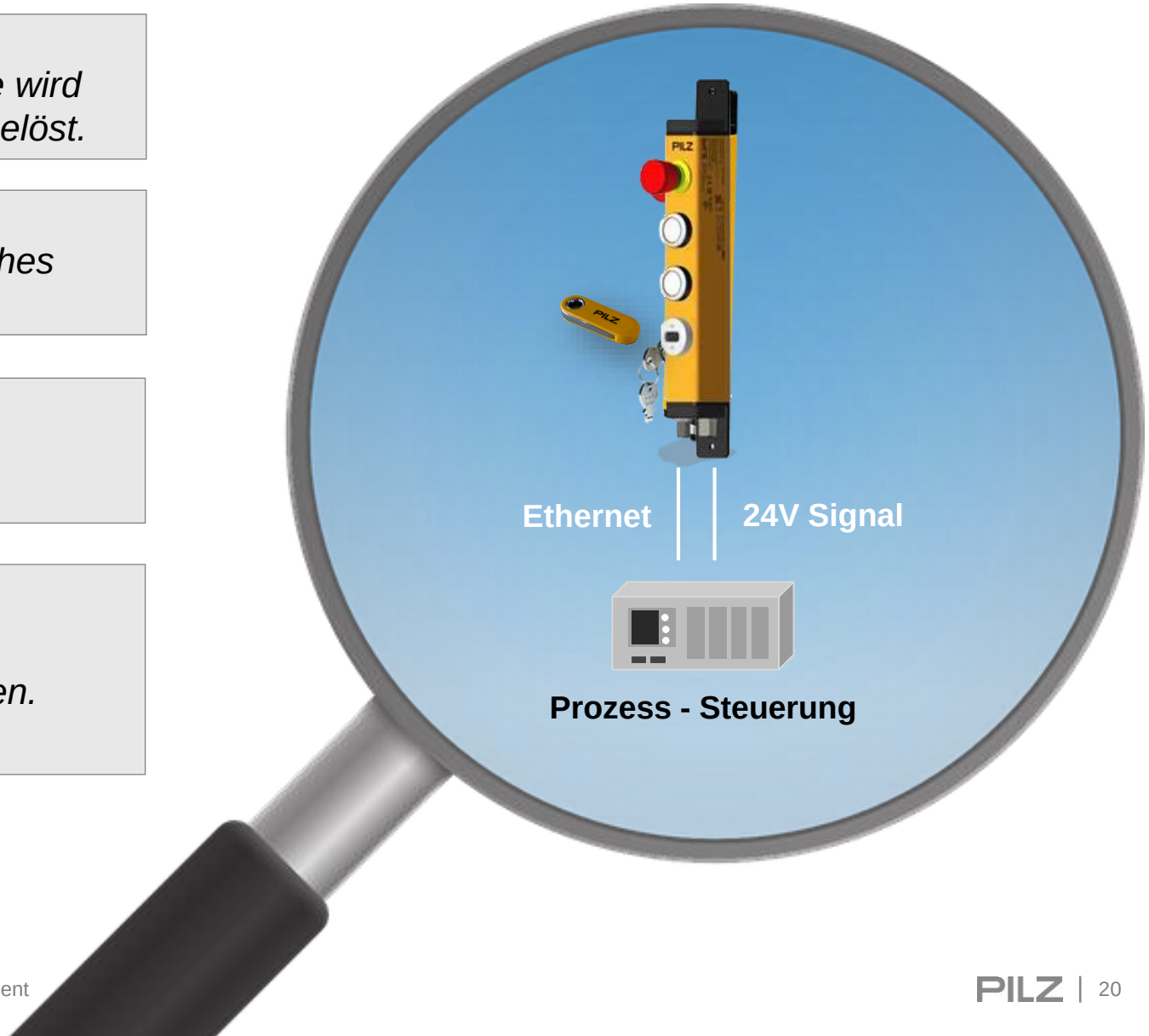
Praxisbeispiel 1.2: Security Retrofit an einer Alt-/ Neumaschine

Situation:
Das Herunterfahren einer Maschine an einer Türe wird über einen mechanischen Schlüsselschalter ausgelöst.

Maßnahme:
Schlüsselschalter durch PITreader als elektronisches Schloss ersetzen.

Realisierungs-Aufwand: ***Sehr gering***.
Nur 1:1 Tausch, bestehende Verdrahtung bleibt.

Vorteile:
- *Individualisierung des Zugriffes.*
- *Neue Schlüssel können einfach erzeugt werden.*
- *Bei Schlüsselverlust: Zugriffe sperren.*



Praxisbeispiel 2.1: Security Retrofit an einer Altmaschine

Situation:
Spezial-Funktionen werden über einzelne mechanische / mehrstufige Schlüsselschalter ein- / ausgeschalten.

Maßnahme:
Schlüsselschalter durch PITreader/Taster PIT oe ersetzen und über PIT m4SEU an Prozess-Steuerung anschließen.

Realisierungs-Aufwand: ***Gering***.
Nutzung der Normlöcher, Anschluss Pilz Komponenten, bestehende Verdrahtung zur Prozess-Steuerung bleibt.

Vorteile:
- *Individualisierung der Funktionen.*
- *Bis zu 5-stufiger Schalter mit LED Rückmeldung.*
- *Bei Schlüsselverlust: Zugriffe sperren.*

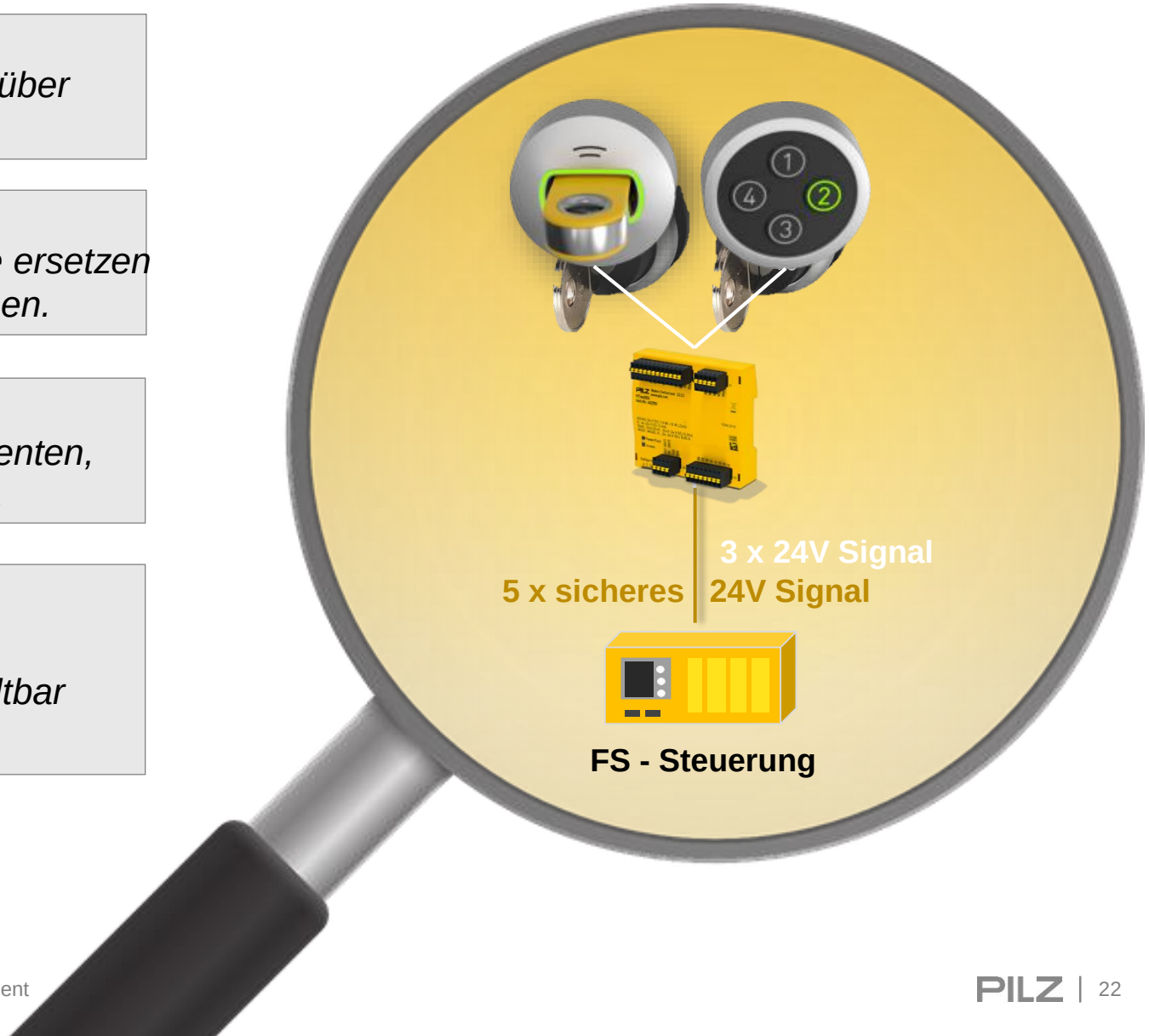
Praxisbeispiel 2.2: Security & Safety Retrofit an einer Altmaschine

Situation:
Mehrere funktional sichere Betriebsarten werden über mechanische Schlüsselschalter angwählt.

Maßnahme:
Schlüsselschalter durch PITreader / Taster PIT oe ersetzen und über PIT m4SEU an FS-Steuerung anschließen.

Realisierungs-Aufwand: *Gering*.
Nutzung der Normlöcher, Anschluss Pilz Komponenten, bestehende Verdrahtung zur FS-Steuerung bleibt.

Vorteile:
- *Individualisierung der Funktionen.*
- *Bis zu 5 funktional sichere Betriebsarten schaltbar*
- *Bei Schlüsselverlust: Zugriffe sperren.*



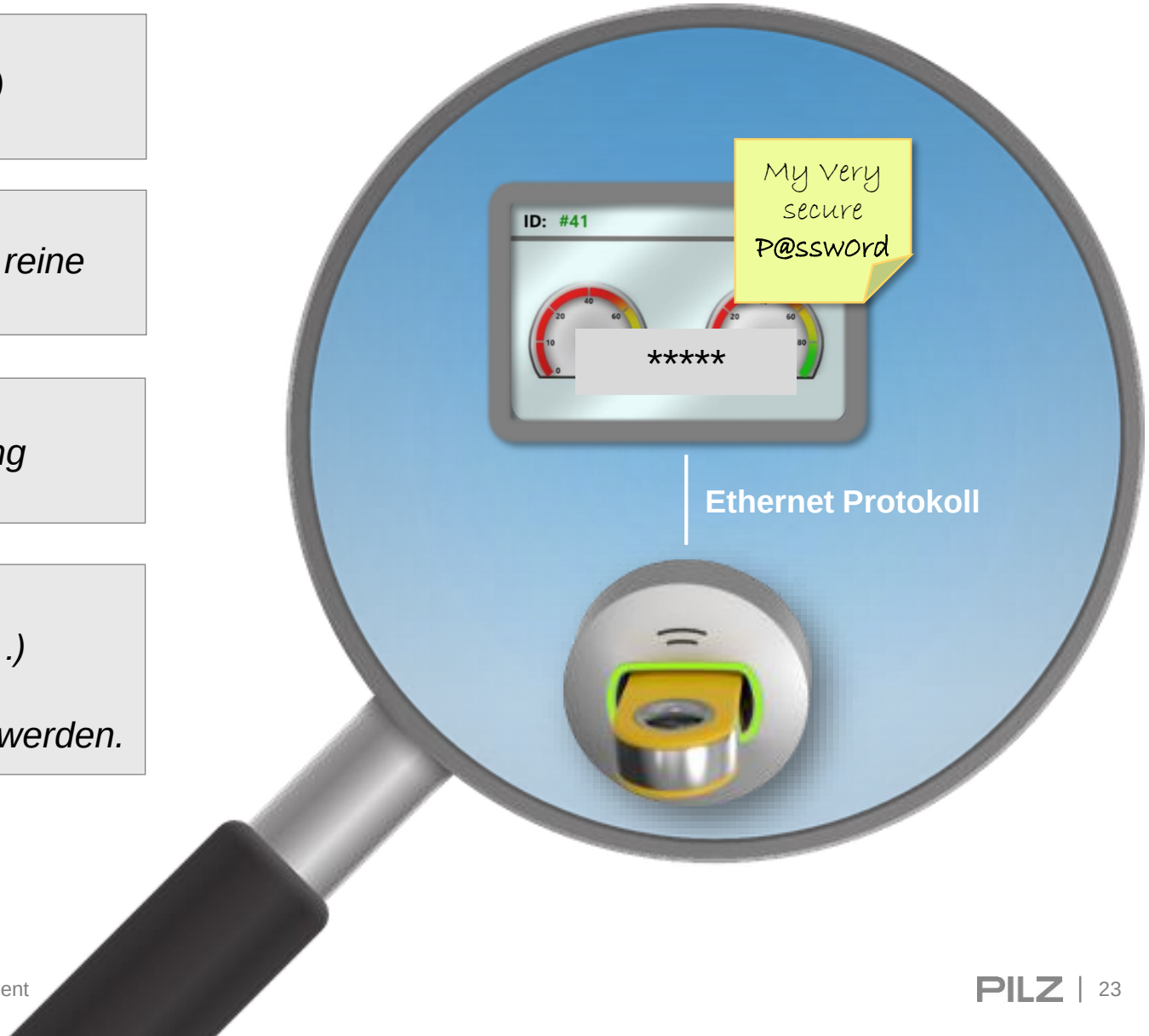
Praxisbeispiel 3: HMI Security Upgrade an einer Alt-/ Neumaschine

Situation:
HMI Funktionen werden über Passworteingabe(n) geschützt.

Maßnahme:
Passworteingabe durch PITreader ersetzen, bzw. reine Passworteingabe erweitern.

Realisierungs-Aufwand: ***Gering***.
Einbau PITreader, Einbettung in HMI Visualisierung über Ethernet Protokolle.

Vorteile:
- *Individualisierung (Sprache, Startbildschirm, …)*
- *Realisierung einer 2 Faktor Authentifikation.*
- *Komplizierte Passwörter müssen nicht notiert werden.*



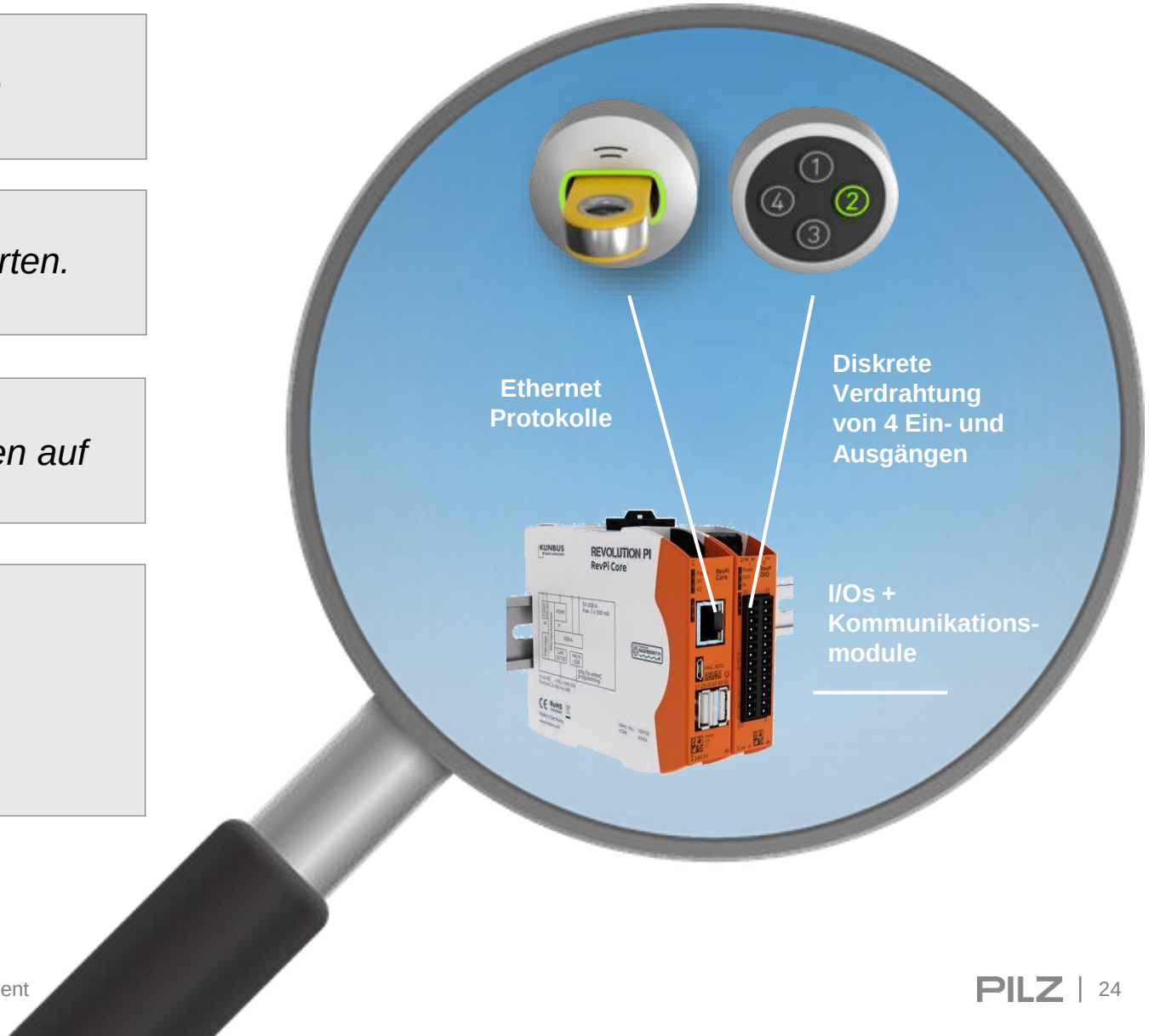
Praxisbeispiel 4: Security Upgrade an einer Alt-/ Neumaschine

Situation:
Zugriffe sollen state-of-the art, flexibel und secure geschützt werden.

Maßnahme:
PITreader an RevPi anschliessen und dort auswerten. Zusätzlich Taster PIT oe 4S verwendbar.

Realisierungs-Aufwand: *Überschaubar*.
Einbau PITreader, Montage des RevPi mit Modulen auf Hutschiene. Verkabeln.

Vorteile:
- *Sehr flexibles und universelles System.*
- *Anschluss an alle relevanten Steuerungen (=Kommunikationsmodule anreibar.*
- *Leicht erweiterbar.*



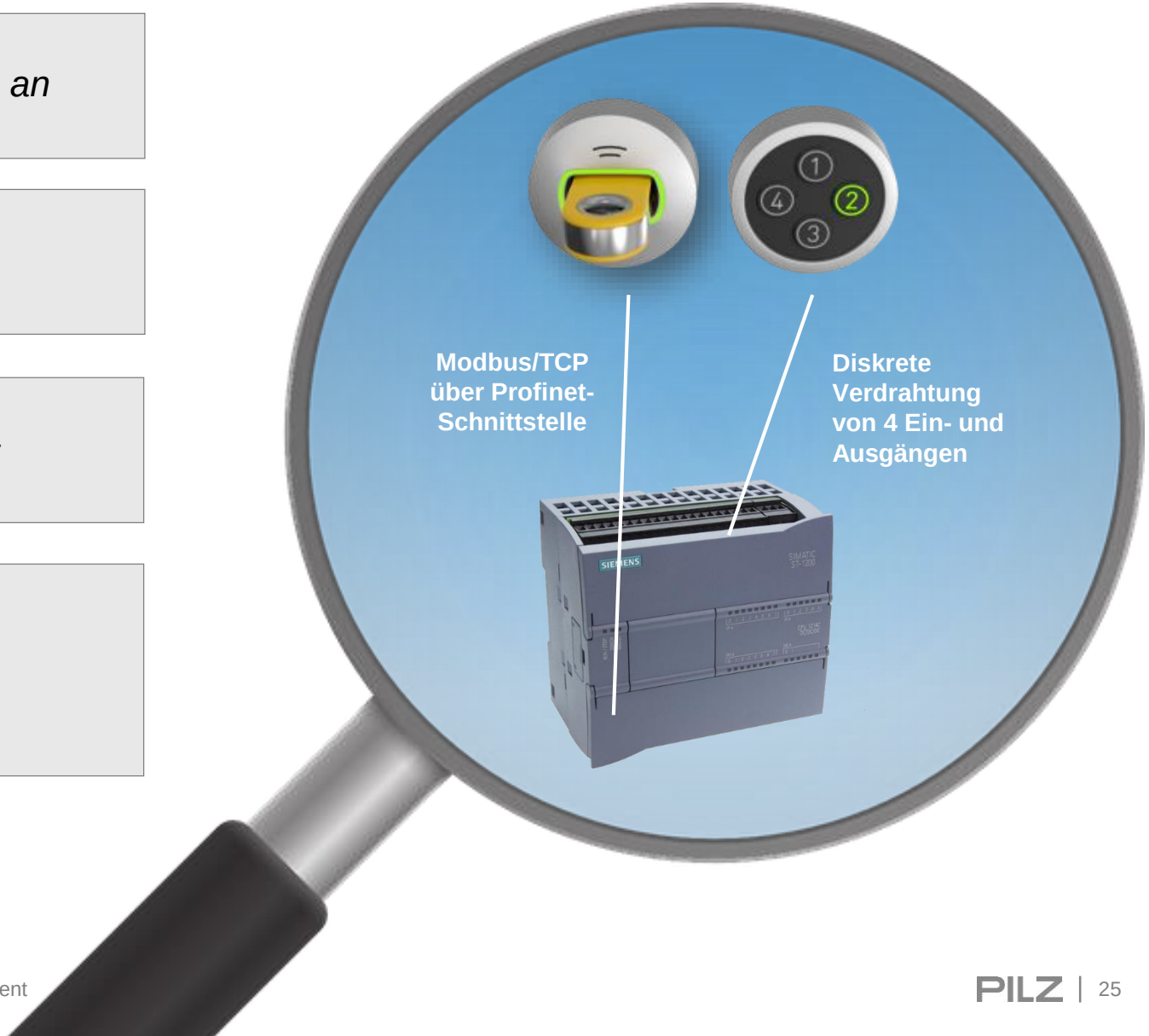
Praxisbeispiel 5: Security Upgrade an einer „Siemens“ Maschine

Situation:
Zugriffe sollen state-of-the art, flexibel und secure an Siemens Steuerungen geschützt werden.

Maßnahme:
PITreader und z.B. Siemens S7 1200 vernetzen.
Zusätzlich Taster PIT oe 4S verwendbar.

Realisierungs-Aufwand: ***Gering***.
Einbau PITreader, Ethernet Anschluss an S7 über Profinet Schnittstelle (über Modbus/TCP).

Vorteile:
- *Anschluss an alle Siemens Steuerungen.*
- *Einfach nachrüstbar*
- *Flexibles und universelles System.*



04

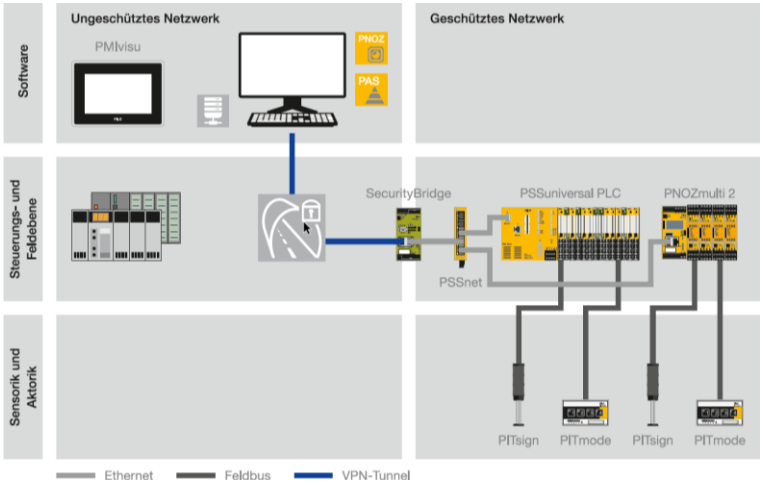
Retrofit Lösungen für Zugriffsberechtigungen auf Schnittstellen und Systeme

Lösungen für Zugriffsberechtigungen auf Schnittstellen und Systeme

Firewall - Implementierung

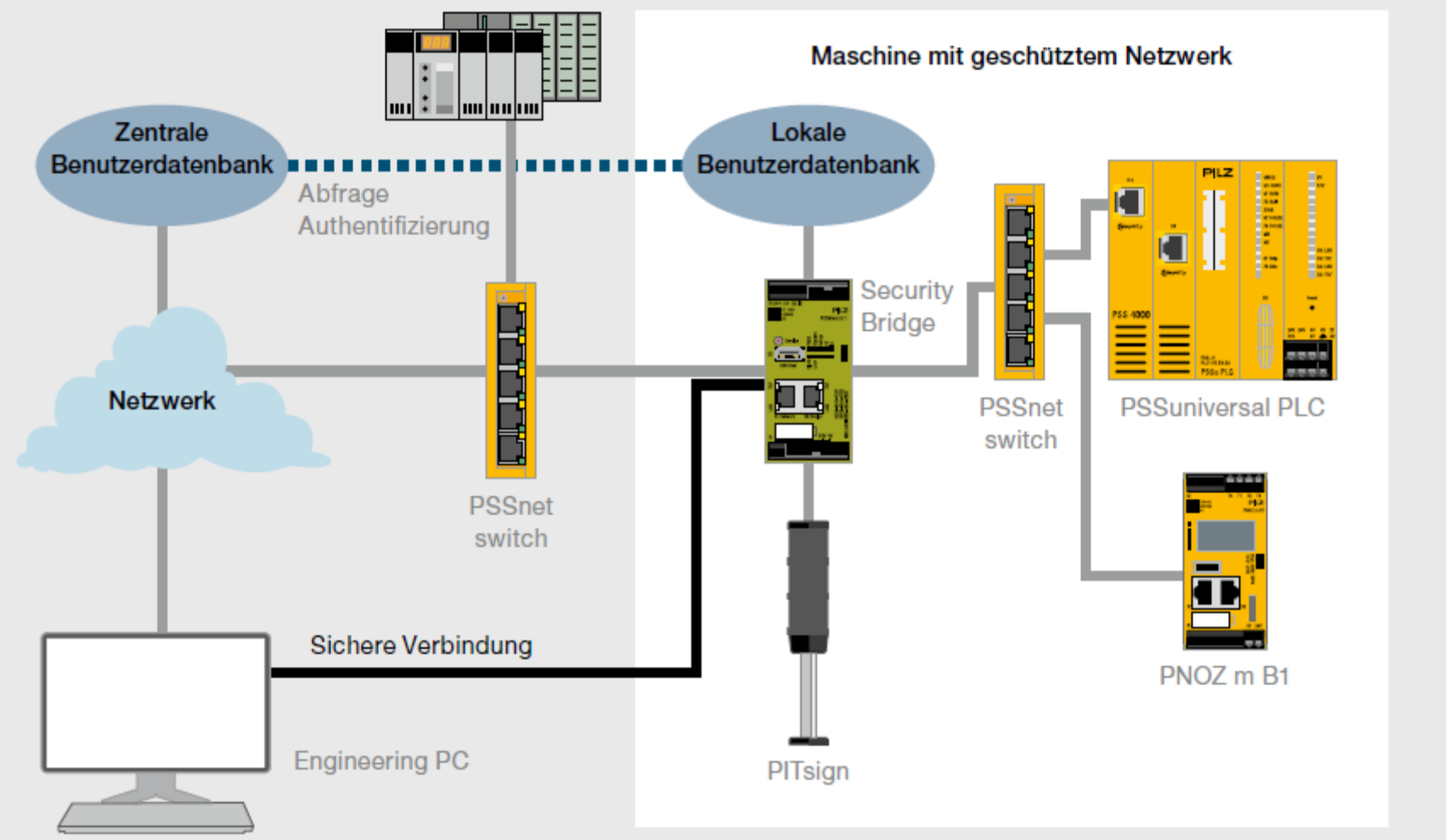
Pilz SecurityBridge – Die Firewall für Industrial Security

- TÜV Süd zertifizierte und entwickelt gemäß Normen IEC 62443-4-1 und IEC 62443-3-3
- Realisierung der Security – Prinzips „Zones and Conduits“
- VPN Server zum Aufbau eines VPN-Tunnel zur sicheren Datenübertragung
- **Schutz vor Manipulation** der Daten durch Authentifizierungs- und Berechtigungsmanagement
- **Erhöht die Verfügbarkeit** der Anlage, da nur notwendige Daten (autorisierte Konfiguration und Prozessdaten) übertragen werden
- Weiterleitung von Prozessdaten mit geringer Latenz
- **Deckt unerlaubte Veränderungen** am Projekt durch Überwachung der Prüfsumme (CRC) **auf**
- **Verhindert unerlaubten Zugriff**, da sich nachgeschaltete Geräte in einem geschützten Netzwerk befinden
- Konfigurationsänderungen an einem Projekt können nur Anwender mit entsprechender **Berechtigung** durchführen



Lösungen für Zugriffsberechtigungen auf Schnittstellen und Systeme

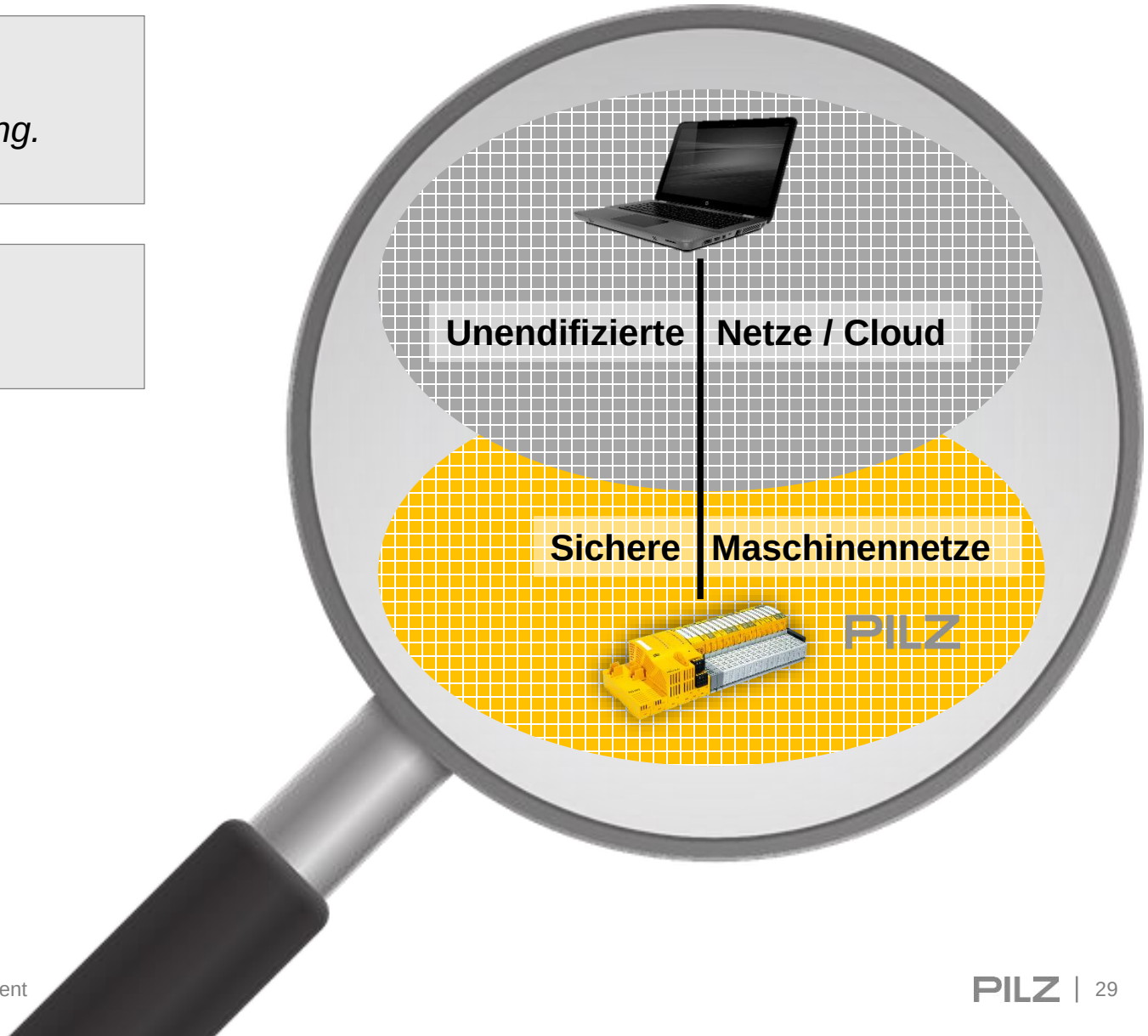
Firewall – Implementierung



Praxisbeispiel 6: Security Upgrade Remote Zugriff auf sichere Netzwerke

Situation:
Netzwerke sind nicht getrennt und geschützt.
Office- und Maschinennetz im fließenden Übergang.
Keine secure Abschottung der Safety Produkte.

Maßnahme:
Netze konsequent trennen, Security Bridge zwischenschalten und Freigabe mit PITreader.



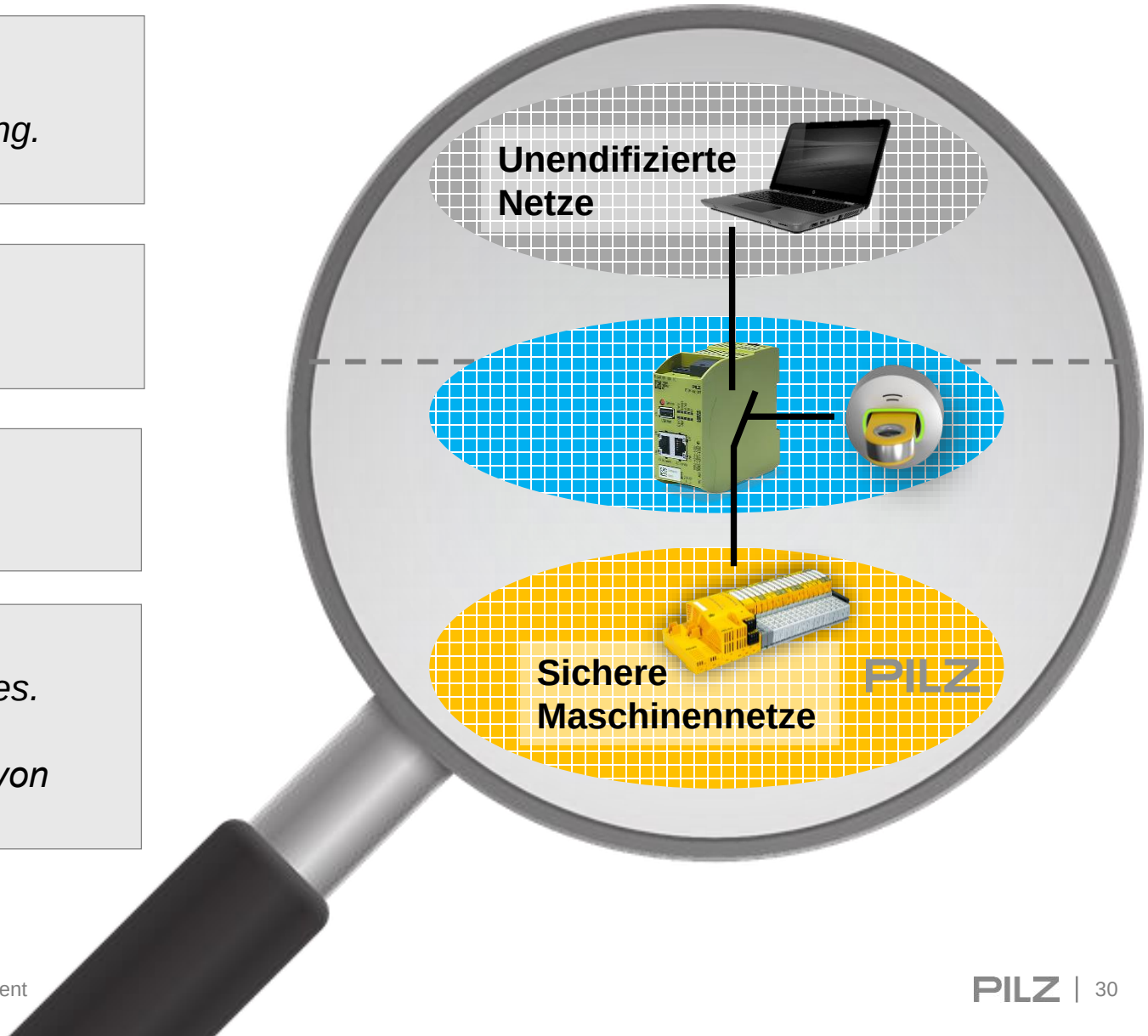
Praxisbeispiel 6: Security Upgrade Remote Zugriff auf sichere Netzwerke

Situation:
Netzwerke sind nicht getrennt und geschützt.
Office- und Maschinennetz im fließenden Übergang.
Keine secure Abschottung der Safety Produkte.

Maßnahme:
Netze konsequent trennen, Security Bridge zwischenschalten und Freigabe mit PITreader.

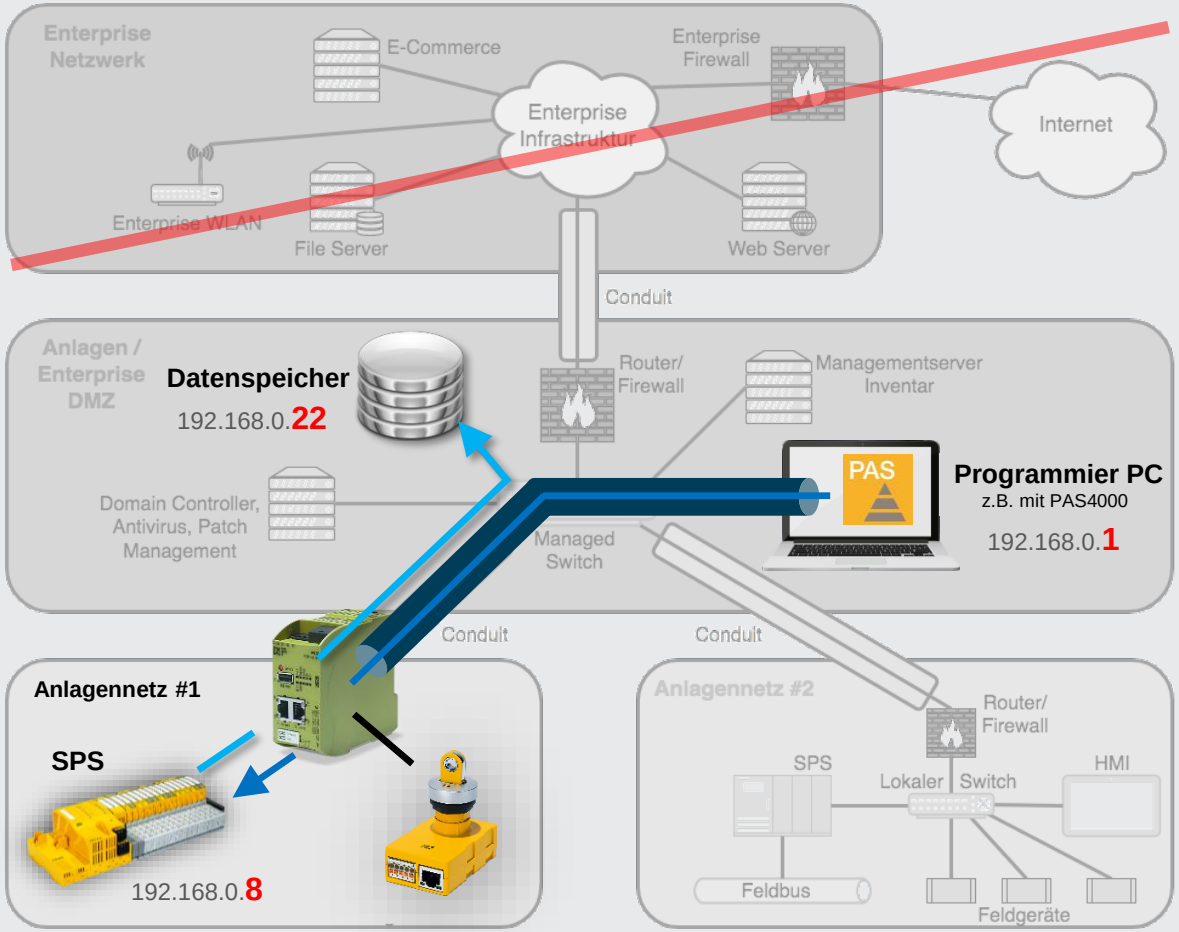
Realisierungs-Aufwand: *Überschaubar*.
Einbau PITreader, Security Bridge konfigurieren.

Vorteile:
- *Sehr sicherer Schutz des Maschinennetzwerkes.*
- *Volle Kontrolle über Zugriffe “von aussen”.*
- *Freigabe des Zugriffes erfolgt ausschließlich “von innen” über bewußte Bedienerhandlung.*



Lösungen für Zugriffsberechtigungen auf Schnittstellen und Systeme

Das Konzept von „zones and conduit“ aus der IEC 62443

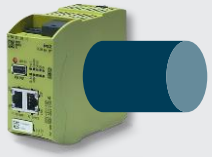


→ *Gegenmaßnahmen gegen die Bedrohung*

1. Firewall mit Regeln.

Initiator	über Protocol / Port	nach
192.168.0.**1**	**RTFN**	192.168.0.**8**
192.168.0.**8**	**OPC UA**	192.168.0.**22**

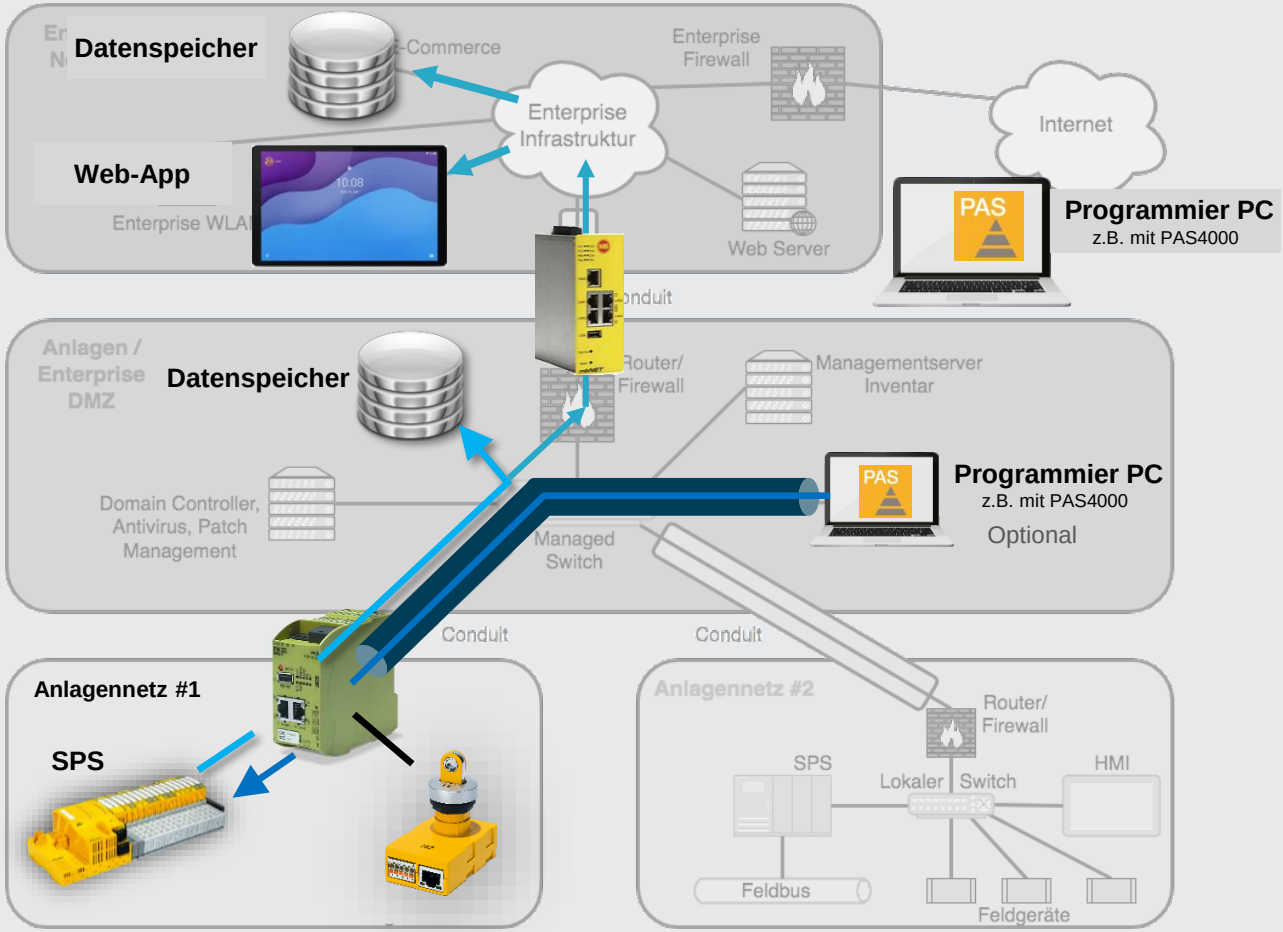
2. Securer, verschlüsselter VPN tunnel.



3. PITreader startet die Daten-verbindung "von innen".

Lösungen für Zugriffsberechtigungen auf Schnittstellen und Systeme

Das Konzept von „zones and conduit“ aus der IEC 62443

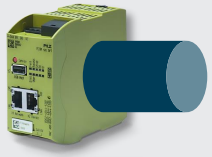


→ ***Gegenmaßnahmen** gegen die **Bedrohung***

1. VPN / Firewall: Cloud + Hardware

2. Firewall mit Regeln.

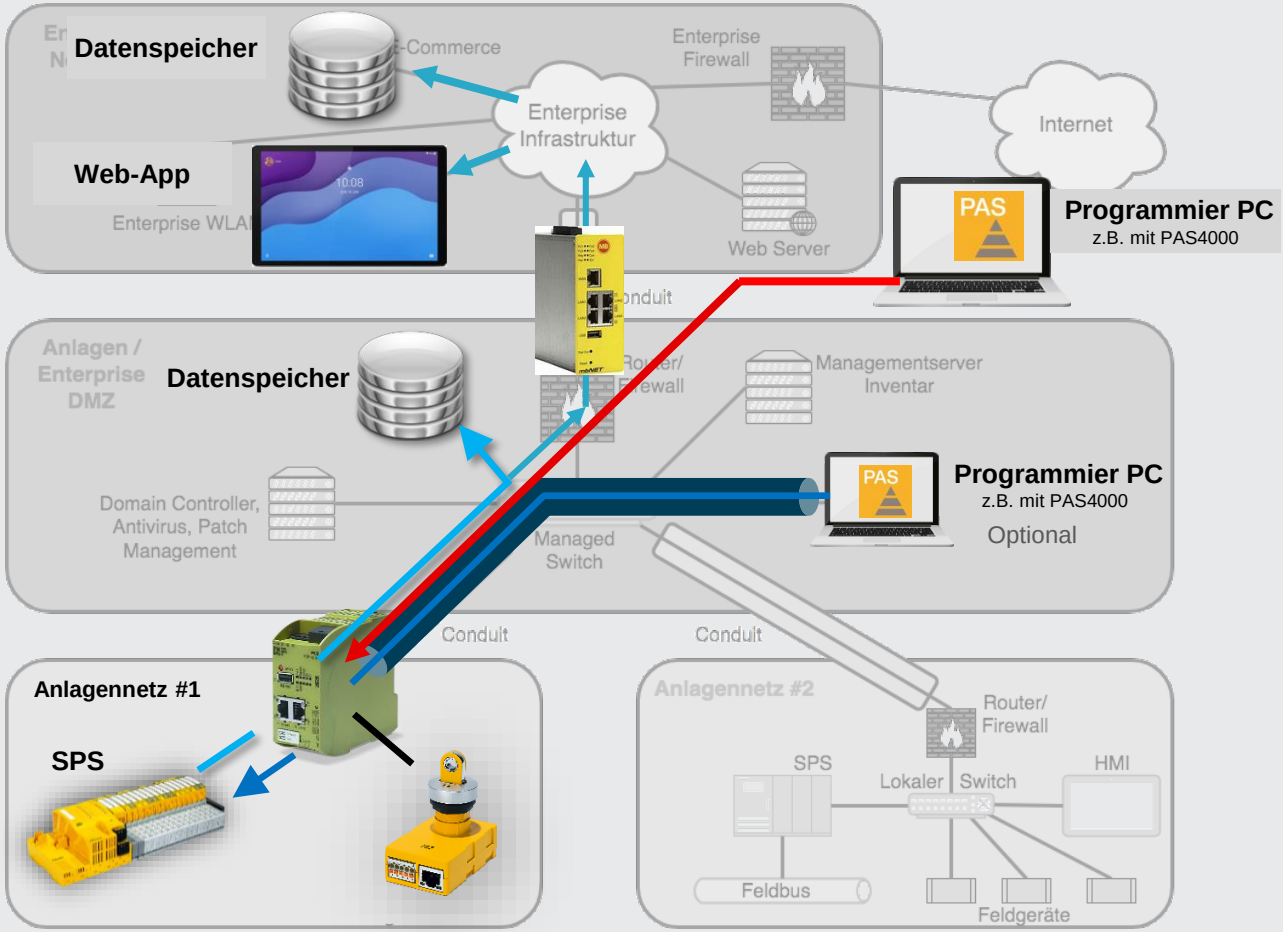
3. Securer, verschlüsselter VPN tunnel.



4. PITreader startet die Daten-verbindung "von innen".

Lösungen für Zugriffsberechtigungen auf Schnittstellen und Systeme

Das Konzept von „zones and conduit“ aus der IEC 62443



→ ***Gegenmaßnahmen** gegen die **Bedrohung***

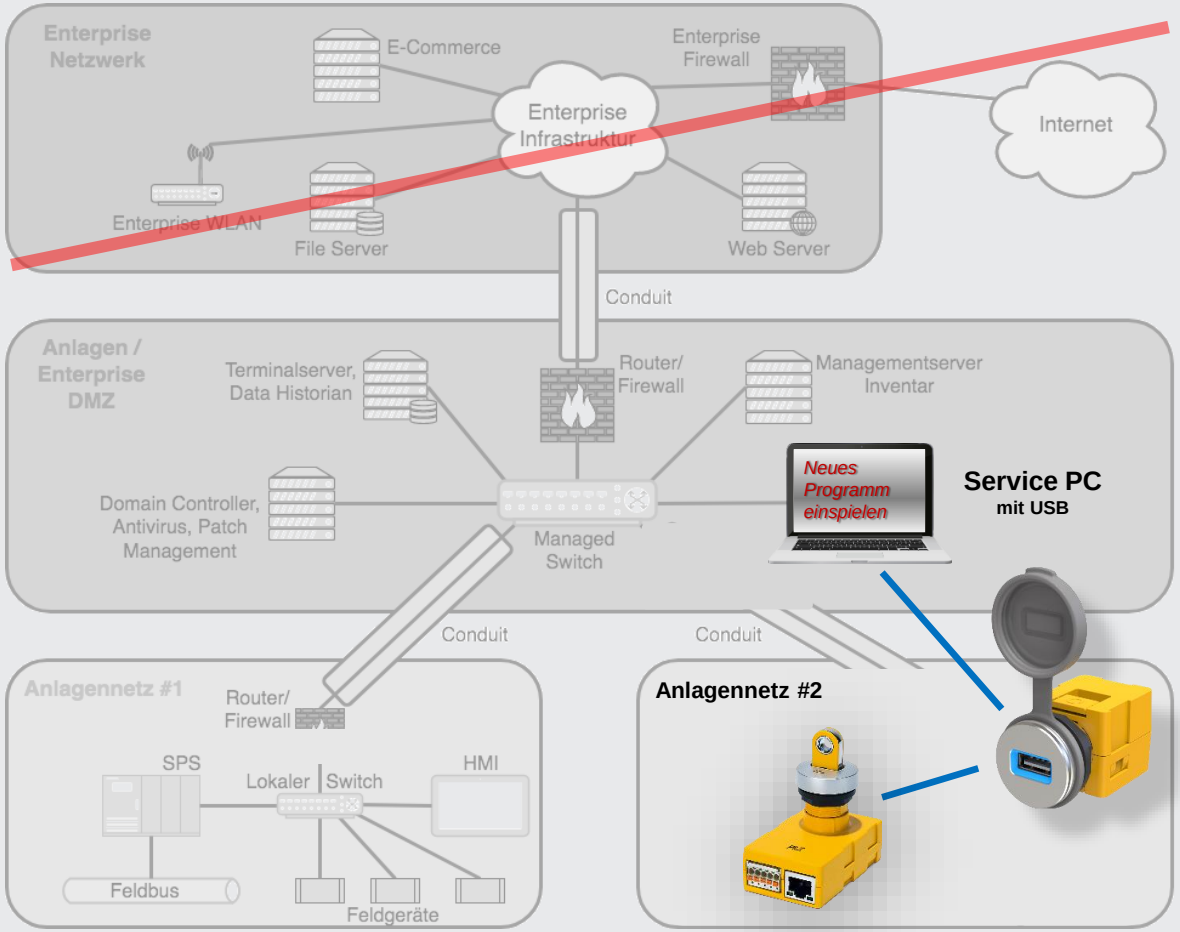
Remote Zugriff von einem externen Programmier-PC nur, wenn das Gerät in der Security Bridge deklariert und bekannt ist und der Authentifizierungsprozess Ok ist.

Verbindung über einen sicheren VPN-Tunnel.

Freischaltung Security Bridge über PITreader

Lösungen für Zugriffsberechtigungen auf Schnittstellen und Systeme

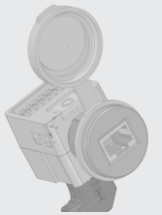
Das Pilz – Konzept zur Freischaltung von Zugriffen auf Maschinenschnittstellen



→ ***Gegenmaßnahmen*** *gegen die* ***Bedrohung***

PIT oe USB mit aktivierbarem USB Port an der Maschine.

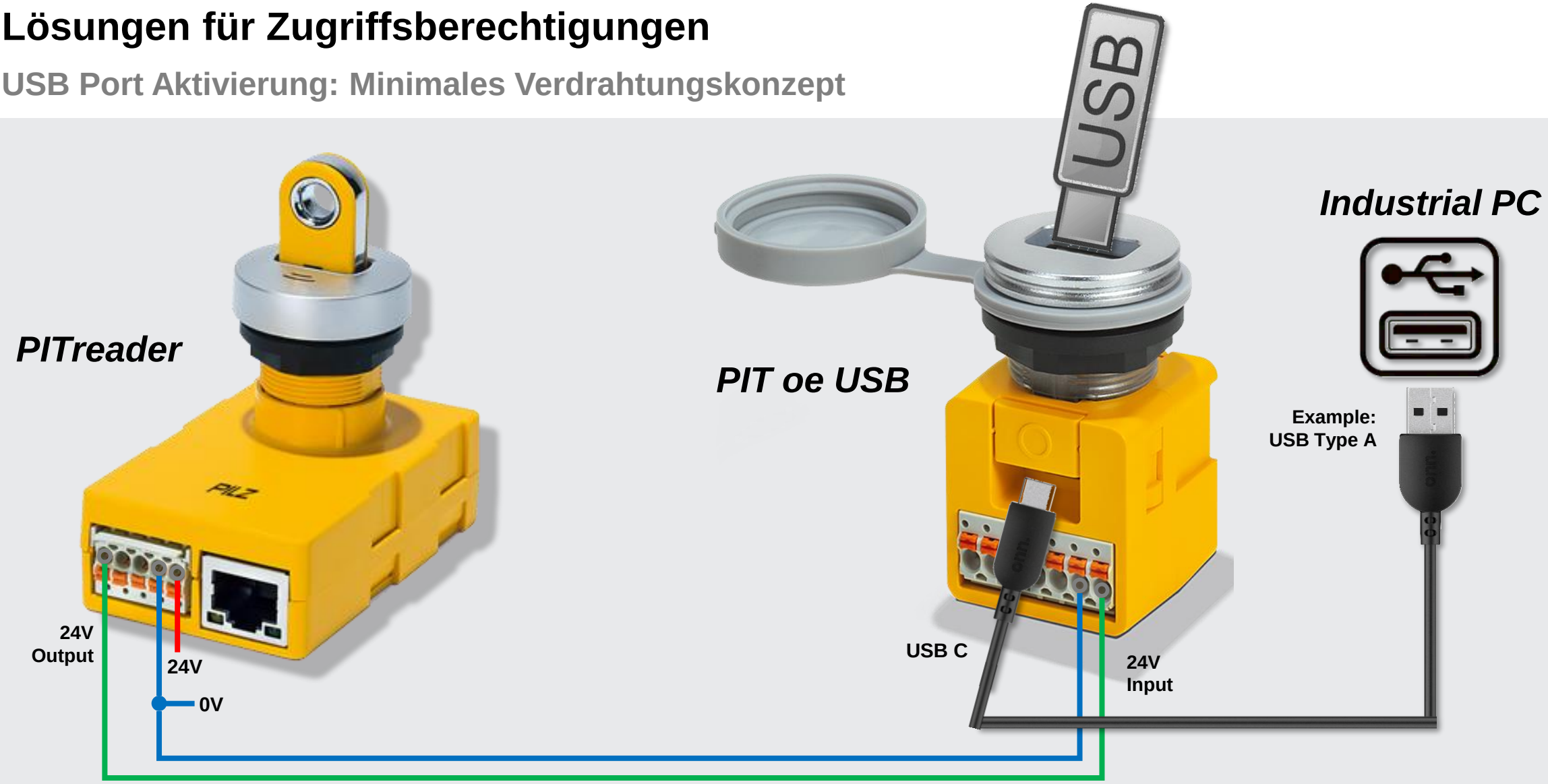
PIT oe ETH mit aktivier-barem Ethernet Port an der Maschine.



PITreader gibt die Daten-Schnittstelle "von innen„ frei.

Lösungen für Zugriffsberechtigungen

USB Port Aktivierung: Minimales Verdrahtungskonzept



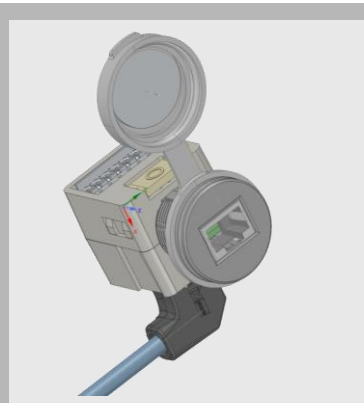
Lösungen für Zugriffsberechtigungen

Schnittstellenfreigabe mit PITreader

Security Bridge

PIT oe USB

PIT oe ETH



Schulungsmöglichkeiten

Erfolgreicher Einstieg in Industrial Security

- **Seminare** für Installateure, Planer, Inbetriebnehmer, Instandhalter, die sich mit dem Thema Planung und Errichtung einer IT-Infrastrukturverkabelung im Industrieumfeld beschäftigen
- Diese Schulung vermittelt alle notwendigen Informationen zum Thema Netzwerk-Security. Ferner wird erläutert, wie Gefahren und Risiken minimiert werden können.

- **Inhalte**
  - **Sicherheitsaspekte**
  - **Authentifizierung, Autorisierung**
  - **Verschlüsselung, Integrität, Zertifikate**
  - **Infrastruktur, Topologie, Fernwartung**
  - **Anbindung an Office-Netzwerke**
- Seminarorte: in Präsenz Ostfildern


PILZ
THE SPIRIT OF SAFETY
Wir automatisieren.
Sicher.
PILZ