Hintergrundinformation

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Deutschland/Germany
www.pilz.com

Ganzheitliche Sicherheitskonzepte nehmen den Zugang in den Fokus, um Safety und Industrial Security an der Maschine zu gewährleisten

Ganzheitliche Sicherheit durch individuelles Berechtigungsmanagement

Ostfildern, Februar 2023 – **Überall, wo wir etwas Wertvolles schützen möchten, setzen wir Türen, Schlösser und Schlüssel ein, um den Zugriff zu beschränken. Dasselbe gilt für das höchste Gut: Unsere Sicherheit in all ihren Ausprägungen. In der Industrieumgebung gilt es einerseits den Menschen zu schützen (Safety) und andererseits die Maschine sowie sensible Daten (Industrial Security). Ein Sicherheitsmangel kann verschiedene Folgen haben: Von der Fehlbedienung über einen Unfall bis hin zu einem schwerwiegenden Cyberangriff. Ein umfassendes Identification and Access Management, das Zugriffs- und Zugangsberechtigungen klar regelt, trägt zu einem ganzheitlichen Sicherheitskonzept und effizienten Abläufen bei.**

In der Produktionsumgebung gehören sie zum gewohnten Bild: Trennende Schutzeinrichtungen, die dem Menschen das klare Signal geben, dass sich hinter der Schutztür ein sensibler Bereich befindet und Vorsicht geboten ist. Über ein Human Machine Interface (HMI) oder einen Schlüssel erhalten Personen Zugang zum Prozess hinter dem Schutzzaun. Aber was, wenn die Person dafür gar nicht qualifiziert respektive autorisiert ist und sich oder andere Personen in Gefahr bringt? Auch eine Person mit böswilligen Absichten kann den Prozess manipulieren – ob direkt an der Maschine oder über einen Fernzugriff. Beim Thema Zugangsberechtigung zeigt sich, dass Safety und Industrial Security

eng ineinandergreifen. Weiter noch: Industrial Security stellt an der Maschine die Integrität der Safety sicher. Sie bietet beispielsweise Maschinen oder Anlagen in der Fertigung Schutz vor unbefugten Zugriffen und Zutritten von außen und schützt sensible Prozess- und Maschinendaten vor Verfälschung, Verlust und unbefugtem Zugriff im Innenverhältnis. Dazu zählen sowohl explizite Angriffe als auch unbeabsichtigte Security-Vorfälle.

Safety und Industrial Security gehören zusammen

Für Betreiber von Maschinen und Anlagen ist es erforderlich, dass sie Aufgaben und Berechtigungen klar vergeben und zuordnen, also ein Identification and Access Management etablieren. Das bedeutet zum einen organisatorische Maßnahmen wie Arbeitsanweisungen oder regelmäßige Kontrollen von Abläufen, sowie zum anderen die Integration passender Sicherheitslösungen in die Produktionsumgebung. Werden solche Maßnahmen versäumt, können die verantwortlichen Personen in einem Unternehmen bei Unfällen oder Produktionsausfällen persönlich haftbar gemacht werden. Bisher basierten solche Security-Lösungen auf Freiwilligkeit, vielerorts wurde noch kein Handlungsbedarf gesehen. Dass Safety und Security ineinandergreifen, hat inzwischen jedoch der Gesetzgeber erkannt. Die neue Maschinenverordnung schreibt deshalb ab 2025 Security-Maßnahmen verpflichtend vor.

Betriebsarten erhöhen die Sicherheit

Darüber hinaus geben verschiedene C-Normen bereits vor, dass unterschiedliche Betriebsarten auch entsprechende Sicherheitsfunktionen enthalten müssen. Betriebsarten können beispielsweise der Automatikbetrieb, manuelles Eingreifen unter eingeschränkten Bedingungen oder Servicebetrieb sein. Die EN ISO 16090-1 für Bearbeitungszentren und Sondermaschinen

schreibt mindestens zwei dieser Betriebsarten verbindlich vor, um funktionale Sicherheit zu gewährleisten. Wichtig ist, dass immer nur eine Betriebsart ausgewählt und aktiv ist und diese klar angezeigt wird.

Anonymen Zugriff verhindern

Doch wie wird entschieden, welche Personen bei welcher Betriebsart Zutritt oder Zugriff haben oder gar die Betriebsart ändern dürfen? Dafür werden unterschiedliche Personengruppen definiert, wie zum Beispiel Bedienungs-, Reinigungs- oder Wartungspersonal, die mit der Maschine in Berührung kommen. Anschließend werden die Mitarbeiter entsprechend ihrer Aufgabe oder Qualifikation den Gruppen zugeordnet. Je nach Unternehmensgröße können Freigaben oder Zugriffsrechte auch für unterschiedliche Benutzergruppen oder beispielsweise für einen Maschinentyp, der konzernweit eingesetzt wird, vergeben werden. Im Zuge einer Risikobeurteilung schätzen Sicherheitsexperten für jede Gefährdung das Risiko des anonymen Zugriffs ein und bewerten es. Anschließend werden Maßnahmen nach dem Stand der Technik und unter Beachtung der harmonisierten Normen festgelegt, die das Risiko reduzieren.

Benutzerfreundlichkeit beugt Manipulation vor

Bei der Umsetzung der Maßnahmen ist es wichtig, die Handhabung und Gebrauchstauglichkeit für Anwender im Betrieb sicherzustellen, um Manipulation auszuschließen. Für Maschinenbauer gilt das bereits für den Entwicklungsprozess. Intuitive Bediensysteme, die Anwender einfach handhaben können, verhindern, dass Sicherheitsvorkehrungen ausgehebelt oder Maschinen falsch bedient werden. Zudem trägt ein durchdachtes Sicherheitssystem zu effizienten Abläufen ohne unnötige Stillstandszeiten bei. Das

Thema „Umgehen von Schutzeinrichtungen“ ist ein zentraler Punkt der EN ISO 14119. Die Norm definiert Leitsätze für die Gestaltung und Auswahl von Schutztürsystemen und bietet so konkrete Hilfestellung, wie Manipulation vermieden werden kann.

Individuelles Sicherheitskonzept

Damit mutwilliges oder versehentliches Öffnen von Zugangstüren nicht zu Gefährdungen führt, sind diese mit einem sicheren Schutztürsystem gesichert. Im Mittelpunkt steht dabei im Sinne von Safety der Schutz des Werkers vor gefährlichen Maschinenbewegungen. Je nachdem, ob es sich um eine Stand-Alone-Maschine oder aber um komplexe, verkettete Anlagen handelt, ist dafür ein maßgeschneidertes Sicherheitskonzept gefragt. Haben Maschinen einen gefährlichen Nachlauf, spielt Zuhaltung eine wichtige Rolle, sind Türen begehbar, ist eine Fluchtentriegelung ein Muss.

Schutztüren maßgeschneidert absichern

Ein modular aufgebautes Schutztürsystem wie PSENmlock von Pilz kombiniert die sichere Schutztürüberwachung mit sicherer Zuhaltung in einem System und verfügt zusätzlich über Sicherheitsfunktionen wie Not-Halt, Fluchtentriegelung sowie eine mechanische Wiederanlaufsperre. Es bietet die Flexibilität und die dezentrale Intelligenz, um vielfältige Anwendungen abzusichern. Eine individuelle Lösung besteht aus einer Kombination von Sensoren, Fluchtentriegelung, Türgriffen sowie einer Bedien- und Taster-Unit. Je nach Applikation stellen Anwender so ihre individuelle Schutztürlösung. Um die Anforderungen an Industrial Security zu erfüllen, werden nun die Zugänge und Berechtigungen in den Blick genommen.

Ein System für Safety und Industrial Security

Der Schutz vor unberechtigtem Zugriff kann in der Praxis mit einem Betriebsartenwahl- und Zugangsberechtigungssystem realisiert werden. Es vereint Safety und Industrial Security: Die Wahl der Betriebsart und die Regelung der Zugangsberechtigung zur Maschine. Eine solche Lösung stellen die Geräte der Produktgruppe PITmode von Pilz dar, die ein Umschalten zwischen definierten Betriebsarten und die Regelung der Zugangsberechtigung ermöglichen. Die Bedienung ist intuitiv, denn jeder Anwender erhält seinen individuell kodierten Transponder, der eine eindeutige Nutzer-Authentifizierung ermöglicht und Manipulation vermeidet.

Zugänge und Betriebsarten individuell managen

Um das Sicherheitskonzept individuell zu gestalten, gibt es PITmode in verschiedenen Ausführungen. Als kompaktes All-in-one Gerät beinhaltet PITmode die Taster für die Betriebsartenwahl sowie eine Auswerteeinheit, was eine platzsparende Installation ermöglicht. Das modular aufgebaute System PITmode fusion besteht dagegen aus der Ausleseeinheit PITreader mit RFID-Technologie und integriertem Webserver sowie einer sicheren Auswerteeinheit Safe Evaluation Unit (SEU). Eine weitere Variante ist PITmode flex: Dabei wird PITreader gemeinsam mit einer Pilz Steuerung und einem Softwarebaustein für die sichere Auswertung eingesetzt. Der modulare Aufbau macht die Integration der Zugangsberechtigung und Betriebsartenwahl in das Design bestehender Bedienpulte möglich. Dort können vorhandene Taster für die Auswahl der Betriebsart genutzt werden, was dem Anwender eine einfache Bedienung ermöglicht. Die Identifikation mit dem Transponder erfolgt durch die Ausleseeinheit PITreader. PITmode

und PITmode fusion bieten funktional sichere Betriebsartenwahl und Zugangsberechtigung bis PL d.

Einfache Authentifizierung – auch aus der Ferne

Um die Betriebsart auszuwählen, steckt der Anwender seinen Transponder direkt an PITmode und betätigt eine für die Betriebsart definierte Taste oder die entsprechende Schaltfläche an einem HMI. Ist die Berechtigung vorhanden, erhält der Anwender Zugang zum Prozess. Dasselbe funktioniert auch, wenn ein Servicemitarbeiter per Fernwartung auf eine Maschine zugreifen möchte: Erst wenn eine Person vor Ort die entsprechende Freigabe im System gibt, kann die Fernwartung beginnen. Nach den Wartungsarbeiten wird dieser Zugang wieder geschlossen, bevor die Maschine wieder anläuft. Eine Manipulation durch Unautorisierte oder ein Port, der versehentlich nach den Wartungsarbeiten offenbleibt, kann so ausgeschlossen werden. Betreiber erhöhen die Industrial Security, weil sie steuern, wer welche Berechtigung und damit Zugang zum Prozess erhält.

Komplettlösung für Zugangsmanagement

Soll ausschließlich die Regelung der Zugänge realisiert werden, kann PITreader auch alleinstehend oder in Kombination mit einer Steuerung von Pilz als Zugangsberechtigungssystem eingesetzt werden. In Kombination mit der konfigurierbaren Kleinsteuerung PNOZmulti 2 konfiguriert der Administrator die Zugangsberechtigungen für Maschinen und Anlagen einfach per „drag and drop“ mit dem dazugehörigen Konfigurationstool PNOZmulti Configurator. Diese werden anschließend über die Ausleseeinheit PITreader auf die RFID-Transponderschlüssel übertragen. Die Variante PITreader S ist durch die Integration des OPC UA Standards unabhängig von einer Pilz Steuerung auch

herstellerübergreifend einsetzbar. Wie bereits erwähnt, können PITmode Geräte einfach in bestehende Bedienpanels integriert werden.

Die Wahl zwischen Schlüssel, Karte oder Sticker

Weitere Flexibilität für Betreiber und Anwender bietet die Variante PITreader card unit: Damit können RFID-fähige Karten und Sticker gemeinsam mit oder anstelle eines RFID-Transponderschlüssels eingesetzt werden. Werden im Unternehmen bereits RFID-fähige Karten verwendet, können diese ebenfalls im Verbund mit PITreader card unit genutzt werden: Der Anwender benötigt dann nur eine Karte für mehrere Funktionen. Grundsätzlich liegt der Vorteil der RFID-Transponder – ob Schlüssel, Karte oder Sticker – darin, dass mehrere Funktionen auf einem Transponder gebündelt werden und so ein ganzer mechanischer Schlüsselbund vereint werden kann. Für den Anwender ist das komfortabel, weil er nur ein Identifikationsmedium bei sich trägt. Administratoren dagegen sparen Zeit und Aufwand bei der Verwaltung und Pflege der Schlüssel.

Ein Plus an Security

Und auch Security-Aspekte sind mit Blick auf Benutzerauthentifizierung, Qualifizierung und Zugriffsschutz berücksichtigt. Sollte sich trotz aller Sicherheitsmaßnahmen ein Unfall oder Security-Vorfall an der Maschine ereignen, ist über das Auslesen des RFID-Transponders nachvollziehbar, wer welche Änderung vorgenommen hat. Ist diese optionale Funktion gewünscht, erfasst das Steuerungssystem anhand der Authentifizierung auch die Zeit des Zugangs im internen, nicht veränderbaren Audit Trail (Ereignislog).

Die sorgfältige Administration ist der Schlüssel

Damit Safety und Industrial Security über den gesamten Lebenszyklus der Anwendung gewährleistet sind, stecken Administratoren viel Sorgfalt in die Pflege der Berechtigungen. Um die Administration einfach zu gestalten, unterstützen passende Software-Werkzeuge von Pilz die Anwender- und Transponderorganisation. So können sich hinter einem kleinen RFID-Schlüssel komplexe Berechtigungsmatrizen oder konzernweit geregelte Vorgaben verbergen. Mit dem integrierten PITreader Webserver programmieren Administratoren die zu PITmode oder PITreader gehörigen RFID-Transponder und hinterlegen darauf die Benutzerdaten und Berechtigungen. Alle wichtigen Einstellungen erfolgen direkt an der Ausleseeinheit, was die Inbetriebnahme inklusive Konfiguration von Schnittstellen beschleunigt.

Zugang zu Schnittstellen einschränken

Die Möglichkeiten des Identification and Access Managements reichen bis hin zur Freigabe von speziellen Industrie USB-Ports, einem der Haupteinfallstore bei Security-Vorfällen. Dafür wird das Zugangsberechtigungssystem PITreader mit einem Bedienelement wie PIT oe USB, das über eine aktivierbare USB 2.0 Host-Schnittstelle verfügt, kombiniert. Diese Lösung macht das manipulationssichere Einspielen von Programmen, Abziehen von Daten sowie den Anschluss einer Tastatur oder Computermaus möglich. Denn die Aktivierung der Schnittstelle erfolgt ausschließlich bei entsprechender Berechtigung und schützt damit den Datenfluss einer Fertigung. Gemeinsam mit einer industriellen Firewall wie SecurityBridge von Pilz, die die Datenkommunikation innerhalb eines industriellen Automatisierungsnetzwerks kontrolliert, können

Maschinen so vor unautorisierten Zugriffen und Manipulation geschützt werden.

Bestandsmaschinen – safe und secure

Sollen Bestandsmaschinen auf den Stand der Technik gebracht werden oder wurde im Zuge einer Risikobeurteilung Handlungsbedarf identifiziert, kann das Zugangsberechtigungssystem PITreader einfach nachgerüstet werden: An den genormten Auslässen für Schlüsselschalter mit 22,5 Millimetern Durchmesser kann das Gerät direkt montiert werden. Zusammen mit einer Pilz Steuerung kann die gewünschte Sicherheitsfunktion direkt eingerichtet werden. Ist eine Fremdsteuerung im Einsatz, wird PITmode fusion eingesetzt, um die Auswertung der Zugangsberechtigung und Betriebswahl zu integrieren. Je nachdem welches Transpondermedium in Frage kommt, können vorhandene RFID-Keycards im Unternehmen für die Authentifikation genutzt werden.

Fazit

Um das höchste Gut, nämlich unsere Sicherheit zu schützen, ist es erforderlich Sicherheitskonzepte ganzheitlich zu gestalten und regelmäßig auf Aktualität zu hinterfragen. Ein wichtiger Baustein ist ein Identification and Access Management, das Berechtigungen und Zugänge in einem Unternehmen klar regelt. Die Lösung ist ein Konzept, das organisatorische Maßnahmen und Vorgaben einschließt sowie passende Sicherheitsfunktionen umfasst. Ein Zugangsberechtigungssystem wie PITreader ist dafür der passende Hardware-Baustein, der mit den ergänzenden Softwarekomponenten zur Organisation der Anwender und Transponder komplettiert wird. Weitere Komponenten aus Schutztürsystem, Steuerung und Software sowie Funktionen wie die

Betriebsartenwahl erweitern die Lösung zu einem ganzheitlichen Safety und Industrial Security Konzept. Für den Anwender ist es dabei einfach zu handhaben, nämlich mit dem individuellen Schlüssel in der Hand.

Zeichen: 14.675

Abbildungen

Abb. 1:
F_Press_IAM_Man_using_PITreader_Key_cold1.jpg (© Pilz GmbH & Co. KG)

BU: Ein umfassendes Identification and Access Management regelt den Zugang zur Anwendung und gewährleistet damit die Integrität von Sicherheitsfunktionen und -maßnahmen – Safety und Industrial Security inklusive.

Abb. 2:

F_Press_PITmode_fusion_402251_PIT_oe_4023311_P1_B_8_2_cold_2020_01 (Pilz GmbH & Co. KG)

BU: PITmode fusion von Pilz ist ein modular aufgebautes Betriebsartenwahl- und Zugangsberechtigungssystem, das Safety und Industrial Security in einem System vereint.

Abb. 3:

F_Press_PITreader_S_card_unit_402321_and_PITreader_card_ye_g_402330_P1_B8_2_cold.jpg (Pilz GmbH & Co. KG)

BU: Das Zugangsberechtigungssystem PITreader card unit von Pilz bietet mit den RFID-fähigen Karten PITreader card und Sticker PITreader sticker weitere Formate für die Umsetzung eines effizienten Zugangsberechtigungssystems.

Abb. 4:
F_Press_PITreader_Webserver.jpg (© Pilz GmbH & Co. KG)

BU: Die RFID-Transponderschlüssel werden im PITreader eingelesen und angelernt. Die Vergabe der Zugangsberechtigungen und die der Betriebsarten erfolgt einfach über den dazugehörigen Webserver.

Abb. 5:
F_Press_Group_7_Modular_safety_gate_system_with_diagnostic_and_evaluation_P1_B8_2_cold_v0.jpg (© Pilz GmbH & Co. KG)

BU: Die flexible Kombination aus Schutztürsystem PSENmlock mit dem passenden Türgriffmodul (oben links), der Taster-Unit PITgatebox mit integriertem Zugangsberechtigungssystem PITreader (oben rechts) sowie der konfigurierbaren Kleinsteuerung PNOZmulti 2 (unten rechts) und der Diagnoselösung Safety Device Diagnostics (unten links) bietet eine komplette Schutztürlösung mit Zugangsberechtigung.

Kasten: Digitale Wartungssicherung Key-in-pocket

Über die reine Zugangsberechtigung hinaus kann PITreader mit einer Pilz Steuerung wie der konfigurierbaren Kleinsteuerung PNOZmulti 2 oder dem Automatisierungssystem PSS 4000 für die effiziente digitale Wartungssicherung „Key-in-pocket“ eingesetzt werden. Diese stellt sicher, dass die Maschine während Wartungsarbeiten nicht wiederanläuft und unautorisierte Personen keinen Zugang erhalten. In der Praxis funktioniert das folgendermaßen: Ein oder mehrere für Wartungsarbeiten autorisierte Benutzer authentifizieren sich an der Anlage. Nach erfolgreicher Authentifizierung wird in der Pilz Steuerung für den Benutzer eine personalisierte Security-ID in einer sicheren Liste hinterlegt. Die Maschine kann nun abgeschaltet, die Schutztür geöffnet und die Maschine betreten werden. Währenddessen verbleiben die RFID-Schlüssel bei den jeweiligen Benutzern „in der Hosentasche“. Nach erfolgter Wartung und nach Verlassen des Gefahrenbereichs melden sich alle Personen ab, die Security-IDs werden aus der sicheren Liste der Pilz Steuerung entfernt und die Maschine kann wieder gestartet werden. Im Gegensatz zu einer Wartungssicherung mit mechanischen Schlüsseln, kann die Anlage an jeder Schutztür betreten oder verlassen werden. Damit bietet „Key-in-pocket“ dem Personal mehr Flexibilität und Zeitersparnis bei der Wartung. Die digitale Wartungssicherung ist speziell für Maschinen mit gefährlichen Bereichen, die durch Schutzzäune gesichert sind, konzipiert. Der Betreiber weiß jederzeit, wer Zugang für welche Aufgabe erhält und kann auch temporäre Berechtigungen vergeben.

1.578 Zeichen

Abb. Kasten Key-in-pocket:
F_Press_Group_PIT_Key_in_pocket_solutions_P1_B8_2_cold.jpg (© Pilz GmbH & Co. KG)

BU: Die Wartungssicherung „Key-in-pocket“ besteht aus dem Zugangsberechtigungssystem PITreader, der Taster-Unit PITgatebox sowie einer Pilz Steuerung wie der konfigurierbaren Kleinsteuerung PNOZmulti 2 oder dem Automatisierungssystem PSS 4000.

Kasten: Berechtigungen vergeben und pflegen

Wird ein Zugangsberechtigungssystem im Unternehmen eingesetzt, ist die regelmäßige Pflege und Verwaltung der Berechtigungen und Benutzerdaten zentral, um ein hohes Maß an Sicherheit zu gewährleisten. Pilz stellt dafür das Software-Tool PIT Transponder Manager (PTM) zur Verfügung: Auf einer grafischen Oberfläche verwaltet der Administrator seine Benutzereinstellungen, Blockierlisten und Anwenderdaten. Mit vorkonfigurierten Templates und einer Importfunktion werden individuelle Benutzerberechtigungen in wenigen Schritten auf den Transponderschlüssel geschrieben.

Sind mehrere PITmode oder PITreader in einem Unternehmen im Einsatz, werden diese Geräte mit der Software PIT User Authentication Service (UAS) von Pilz organisiert. Er ermöglicht die Verbindung von Managementsystemen wie dem PTM oder einer

anderen Benutzerverwaltungssoftware mit PITreader. PIT UAS verfügt über eine zentrale Autorisierungsdatenbank für die Anwender und macht so den Import und das Zuweisen von Daten aus dem PTM an alle PITreader möglich. Administratoren können den aktuellen Status sämtlicher PITreader einsehen und sich eine Diagnoseliste anzeigen lassen. So wird der schnelle Überblick auch beim Einsatz mehrerer Geräte gewahrt.

1.218 Zeichen

Abb. Kasten Benutzerverwaltung:
((Bild folgt)).jpg (© Pilz GmbH & Co. KG)

BU: Sind mehrere Ausleseeinheiten PITreader in einem Unternehmen im Einsatz, werden diese Geräte mit dem User Authentication Service (UAS) organisiert.

Pilz Gruppe

Die Pilz Gruppe ist globaler Anbieter von Produkten, Systemen und Dienstleistungen für die Automatisierungstechnik. Das Familienunternehmen mit Stammsitz in Ostfildern beschäftigt rund 2.500 Mitarbeiter. Mit 42 Tochtergesellschaften und Niederlassungen schafft Pilz weltweit Sicherheit für Mensch, Maschine und Umwelt.
Der Technologieführer bietet komplette Automatisierungslösungen, die Sensorik, Steuerungs- und Antriebstechnik umfassen – inklusive Systeme für die industrielle Kommunikation, Diagnose und Visualisierung. Ein internationales Dienstleistungsangebot mit Beratung, Engineering und Schulungen rundet das Portfolio ab. Lösungen von Pilz kommen über den Maschinen- und Anlagenbau hinaus in zahlreichen Branchen, wie etwa der Intralogistik, der Bahntechnik oder im Bereich Robotik zum Einsatz.

www.pilz.com

Kontakt für die Presse:

Martin Kurth
Unternehmens- und Fachpresse
Tel: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer
Fach- und Unternehmenspresse
Tel: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman
Fachpresse
Tel: +49 711 3409-1067
j.skarman@pilz.de

Sabrina Schilling
Fachpresse
Tel: +49 711 3409-7147
s.schilling@pilz.de

Hansjörg Sperling-Wohlgemuth
Kongress- und Vortragsmanagement
Tel: +49 711 3409-239
h.sperling@pilz.de