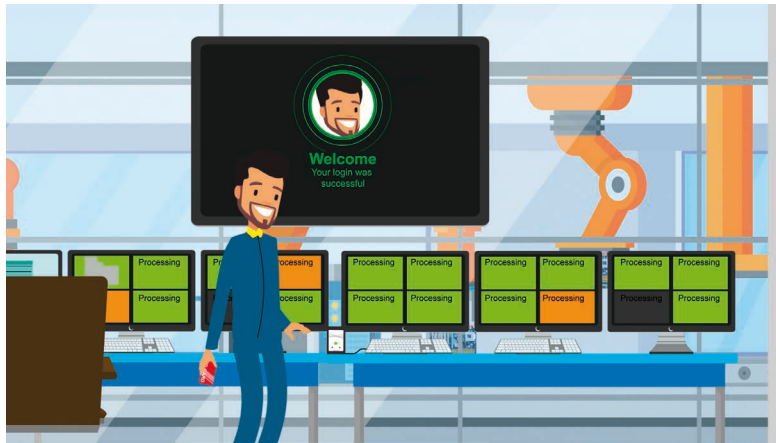


Die Zukunft industrieller Zugangskontrolle

Integrierte Authentifizierungslösung für erhöhte Anlagensicherheit



In einer Zeit, in der Industrie 4.0 und das Internet der Dinge (IoT) immer mehr an Bedeutung gewinnen, ist es unerlässlich, dass smarte Fabriken adäquate Sicherheitsmaßnahmen ergreifen, um Menschen, Maschinen und Daten zuverlässig zu schützen. Dabei spielt die Implementierung einer flexiblen und skalierbaren Sicherheitsinfrastruktur eine entscheidende Rolle. Eine Voraussetzung, um einen sicheren und reibungslosen Produktionsbetrieb zu ermöglichen, ist der Einsatz einer modernen Authentifizierungslösung auf Basis von Radio-Frequency Identification (RFID) und mobilen Technologien.

Daten schützen

Im Zuge der digitalen Transformation sind Maschinen, Roboter und Logistiksysteme in modernen Produktionsbetrieben immer häufiger über das Internet of Things (IoT) miteinander vernetzt. So lassen sich nicht nur Produktionsprozesse optimieren, sondern auch Durchsätze und Qualität verbessern sowie Kosten reduzieren. Dieser hohe Vernetzungsgrad ist jedoch

mit Herausforderungen verbunden. Zum einen gilt: Je automatisierter die Fabrik, desto mehr Daten werden generiert, gesammelt und analysiert. Diese wertvollen Informationen müssen vor unbefugtem Zugriff geschützt werden. Zum anderen ist es erforderlich, Bedienungsfehler oder Sabotageakte zu verhindern, die in einer vernetzten Umgebung gravierende Folgen wie Fehlproduktionen oder Anlagenstillstände verursachen können.

Stillstand in der Produktion

- Eine Herausforderung für die Industrie. Anlagenstillstände haben erhebliche negative Auswirkungen für Unternehmen. Die Ursachen sind vielfältig und reichen von technischen Defekten über menschliches Versagen bis hin zu gezielten Cyberangriffen. Neueste Umfrageergebnisse [1] zeigen, dass Sicherheitsprobleme und Nachlässigkeit der Endbenutzer zu den Hauptursachen für ungeplante System- und Netzausfälle im Jahr 2021 gehörten. Unabhängig von der Ursache führen Anlagenstillstände zu Produktionsausfällen und beeinträchtigen somit die Rentabilität des Unternehmens. Darüber hinaus können sie zu Verzögerungen bei der Lieferung von Produkten führen, mit negativen Auswirkungen auf Reputation und Kundenbeziehungen. Die finanziellen Auswirkungen sind also beträchtlich. Laut einer Studie [2] kosten ungeplante Ausfallzeiten Hersteller heute mindestens 50 Prozent

mehr als noch vor drei Jahren. Ursachen dafür sind die steigende Inflation sowie Produktionslinien mit zunehmend höherer Kapazität. Die Kosten für eine Stunde Ausfallzeit belaufen sich auf 39.000 US-Dollar für Konsumgüter bis hin zu über zwei Millionen US-Dollar im Automobilsektor. Um solche Situationen zu verhindern, ist es wichtig, dass Unternehmen in präventive

Maßnahmen investieren, wie zum Beispiel regelmäßige Wartungsarbeiten, Schulungen für Mitarbeiter und den Aufbau einer robusten Sicherheitsinfrastruktur, die Cyberangriffe abwehrt und den Zutritt und Zugang in der Produktion zuverlässig auf autorisierte Personen beschränkt.

All-in-One-Authentifizierungslösung für höhere Sicherheit

In den gewachsenen Strukturen einer Fabrik werden Zugang und Zutritt häufig mit vielen unterschiedlichen Methoden geregelt: Der Zugang zur Maschinensteuerung erfordert die Eingabe einer PIN, der Staplerfahrer benötigt einen Schlüssel, der Spindel mit einem Vorhängeschloss gesichert und der Computer mit einem Passwort geschützt. Dieser Flickenteppich beeinträchtigt jedoch nicht nur die Effizienz, beispielsweise indem

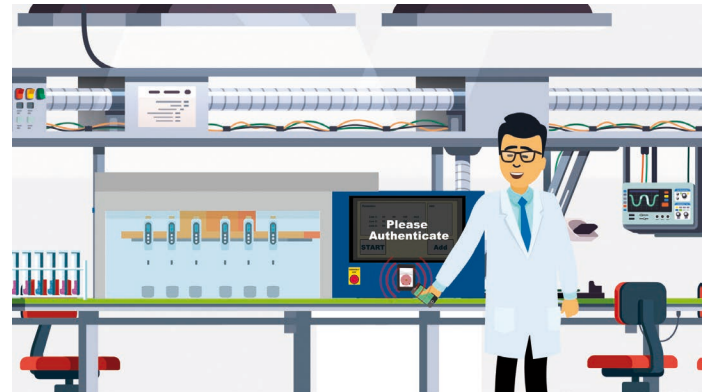
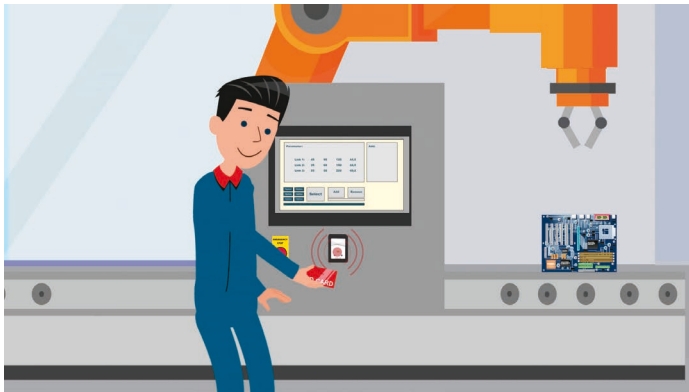
Schlüssel verwaltet oder immer wieder PINs eingegeben werden müssen. Er gefährdet auch die Sicherheit, wenn beispielsweise Passwörter geteilt oder gehackt werden. Einen innovativen Ansatz für den Schutz von industriellen Anlagen in der heutigen zunehmend vernetzten Welt bietet eine All-in-One-Authentifizierungslösung auf der Grundlage von RFID und den mobilen Technologien Near Field Communication (NFC) und Bluetooth Low Energy (BLE). Sie kann unterschiedlichste Anwendungen mit einem System abdecken – das Spektrum reicht vom Zugang zur Robotersteuerung bis zum Zutritt zu Reinräumen in der Produktion.

Identifikationsmedium

Als Identifikationsmedium lässt sich sowohl der bereits vorhandene Mitarbeiterausweis als auch das immer griffbereite Smartphone oder ein Keyfob nutzen. Durch maximale Flexibilität bei der Wahl des Identifikationsmediums kann für jeden Unternehmensbereich die beste Lösung gefunden werden. In der Verwaltung sind digitale Ausweise besonders geeignet, während sich in der Produktion der Einsatz der robusten Karten empfiehlt. Egal, ob es sich um ein Smartphone, eine Karte oder einen Keyfob handelt - das Identifikationsmedium wird einfach an das entsprechende Lesegerät gehalten, um Zugang und Zutritt unverzüglich zu gewähren. Dies spart erheblich Zeit und erhöht die Pro-



Autor:
Burhan Gündüz
Vice President Business
Development
ELATEC GmbH
info-rfid@elatec.com
www.elatec.com



duktivität, insbesondere wenn zahlreiche Authentifizierungsprozesse pro Schicht erforderlich sind. Wichtig zu beachten: Am internationalen Markt sind eine Vielzahl von Kartentechnologien mit jeweils eigenen Datenformaten, Kommunikationsfrequenzen und Sicherheitsfunktionen verfügbar. Innerhalb eines Unternehmens können daher unterschiedliche Technologien im Einsatz sein. Multifrequenz-Lesegeräte, wie sie beispielsweise der Lösungsanbieter Elatec im Portfolio hat, unterstützen mehr als 60 weltweit gängige Transpondertechnologien und bieten damit maximale Flexibilität.

Höheres Sicherheitsniveau

Durch die Integration verschiedener Authentifizierungsanwendungen in einer einzigen Lösung wird nicht nur die Komplexität reduziert, sondern auch das Sicherheitsniveau erheblich erhöht. Die Vorteile dieser umfassenden Lösung liegen auf der Hand: Sie ermöglicht es Unternehmen, ihre Sicherheitsprotokolle effektiver zu gestalten. Berechtigungen können für jede Person individuell zugewiesen und bei Bedarf entzogen werden. Bei einem Verlust lässt sich der Ausweis über das zentrale System sperren. Darüber hinaus kann eine All-in-One-Lösung dazu

beitragen, menschliche Fehler bei der Identitätsprüfung zu minimieren und somit potenzielle Risiken weiter zu reduzieren. In Zeiten von Industrie 4.0 und dem Internet of Things (IoT) ist dies von entscheidender Bedeutung, um den wachsenden Anforderungen an Sicherheit und Datenschutz gerecht zu werden.

Erfolgreiche Umsetzung

Schritte und Best Practices: Mit einer All-in-one-Lösung lassen sich alle Bedarfe in Bezug auf Zutritt und Zugang in einer Fabrik abdecken. Doch dies bedeutet keinesfalls, dass es für alle Unternehmen sinnvoll ist, eine identische Lösung einzuführen. Denn kein produzierendes Unternehmen ist wie das andere. Faktoren wie Herstellungsverfahren und -maschinen, Mitarbeiterzahl oder die Anzahl der Fertigungsstandorte machen jeden Betrieb einzigartig. Unternehmen sollten daher eine Gesamtlösung implementieren, die maximale Flexibilität und jederzeit Anpassungen ermöglicht. Ein solches skalierbares System erlaubt es beispielsweise mit der Maschinenauthentifizierung zu starten und den Ausweis zudem für Anwendungen wie die Nutzung von Flurförderfahrzeugen zu verwenden. Weitere Applikationen wie Kiosklö-

sungen für die Nutzung von Werkzeugwagen, die Einmalanmeldung im Firmennetzwerk oder die Zeiterfassung können bei Bedarf sukzessive ergänzt werden. Dabei verbessert ein einheitliches Zutrittssystem, das über alle Anwendungen hinweg funktioniert, nicht nur Sicherheit und Komfort, sondern bildet auch die Grundlage für Effizienzsteigerungen in der Produktion: Die Harmonisierung der generierten Daten über alle Zugangssysteme hinweg sorgt für mehr Transparenz hinsichtlich der Aktivitäten der Mitarbeiter. So lässt sich Optimierungspotenzial in Bezug auf die Produktionsprozesse identifizieren und umsetzen. Darüber hinaus können Schichtdienste sowie die effiziente Nutzung von Räumen und Ressourcen besser geplant werden.

Einführung

Um eine einheitliche Authentifizierungslösung auf der Basis von RFID, NFC und BLE erfolgreich in der modernen Fabrik zu implementieren, gilt es die folgenden Aspekte zu beachten:

1. **Bedarfsanalyse:** Identifizierung der spezifischen Anforderungen des Unternehmens an das Authentifizierungs- und Zugangskontrollsystem
2. **Zukunftssicherheit:** Nur ein System, das skalierbar ist und regelmäßige Updates sowie Upgrades bietet, ist langfristig die richtige Lösung
3. **Integrationsmöglichkeit in bestehende Infrastruktur:** Nahtlose Einbindung der ausgewählten Lösung in die vorhandene IT-Landschaft
4. **Flexibilität:** Multifrequenz-Lesegeräte bieten Unternehmen die Möglichkeit, Identifikationsmedien mit unterschiedlichen Transpondertechnologien einzusetzen
5. **Schulung der Mitarbeitenden:** Vermittlung von notwendigem Know-

how im Umgang mit den neuen Systemen und Sensibilisierung für Sicherheitsaspekte

6. **Compliance und Datenschutzrichtlinien:** Berücksichtigung der geltenden gesetzlichen Bestimmungen und Compliance-Vorschriften im jeweiligen Land sowie entsprechender Arbeitsgesetze, die die Nutzung von Systemen zur Qualitätssicherung und Zeiterfassung regeln
7. **Kontinuierliches Monitoring und Optimierung:** Regelmäßige Überprüfung der implementierten Lösung auf Effektivität und eventuelle Anpassungen bei Bedarf

Fazit

Die Vorteile einer umfassenden Authentifizierungslösung für die moderne Fabrik sind immens. Die Einführung einer All-in-One-Authentifizierungslösung bietet also zahlreiche Vorteile für Produktionsumgebungen. Durch die Reduzierung von Komplexität, die Verbesserung der Sicherheit und die Auswertungen der generierten Daten können Unternehmen ihre Produktivität steigern und mögliche Anlagenstillstände vermeiden. Zudem schaffen sie eine solide Basis für den Schutz ihrer Infrastruktur im Rahmen von Industrie 4.0 und IoT-Anwendungen. Somit stellt eine integrierte Authentifizierungslösung den entscheidenden Schritt in Richtung einer zukunftssicheren industriellen Zugangskontrolle dar.

Referenzen

1. <https://www.ibm.com/reports/data-breach>
2. <https://assets.new.siemens.com/siemens/assets/api/uuid:3d606495-dbe0-43e4-80b1-d04e27ada920/dics-b10153-00-7600truecostofdown-time2022-144.pdf> ◀

