AUTHENTIFIZIERUNGSLÖSUNG

Authentifizierung in der vernetzten Fabrik

Schutz von Mensch, Infrastruktur und Daten in modernen Produktionsumgebungen

In modernen Fabriken eröffnen die zunehmende Vernetzung und Automatisierung ein breites Spektrum an Möglichkeiten, um Effizienz und Produktivität zu steigern. Doch mit der Digitalisierung gehen auch neue Herausforderungen in Bezug auf die Sicherheit einher. Denn jede Störung kann in einer solch komplexen Umgebung gravierende Folgen haben. Eine intelligente Authentifizierungslösung leistet hier einen wichtigen Beitrag zum Schutz von Menschen, Infrastruktur und Daten.

Hochautomatisierte Produktionsstätten nutzen heute fortschrittliche Technologien wie das Internet of Things (IoT), künstliche Intelligenz und Datenanalyse, um Fertigungsprozesse und -anlagen miteinander zu vernetzen und somit eine nahtlose Kommunikation und Datenübertragung zu ermöglichen. Durch den Einsatz von Sensoren und IoT-Geräten werden riesige Mengen an Daten generiert und analysiert, um Effizienz und Qualität zu maximieren. Bester Beleg dafür, dass diese Entwicklung in immer mehr Fabriken Einzug hält, sind aktuelle Daten der International Federation of Robotics (IFR): Im Jahr 2022 wurden in den EU-Ländern rund 72.000 neue Roboter in Betrieb genommen, was einem Anstieg von 6 % gegenüber dem Vorjahr entspricht.

Sicherheitsherausforderungen in der modernen Fabrik

Intelligente Produktionsumgebungen bringen bei allen Vorteilen auch neue Sicherheitsrisiken mit sich: Eine Bedrohung sind Cyberattacken. Die Vernetzung von Maschinen und Systemen bietet Angreifern zahlreiche Eintrittspunkte, um in das Fabriknetzwerk einzudringen. Sind die Sicherheitsvorkehrungen nicht ausreichend, können Hacker nicht nur Produktionsprozesse stören, sondern auch wertvolle Geschäftsdaten und geistiges Eigentum stehlen.

Auch innerhalb des Unternehmens gibt es ein Risikopotenzial: Erhalten beispielsweise ungeschulte Mitarbeiter Zugang zu den Anlagen, kann ein menschlicher Fehler schwerwiegende Konsequenzen haben, einschließlich Sicherheitsrisiken und Produktionsausfällen.

Doch nicht nur im Hinblick auf Sicherheitsaspekte ist Transparenz gefragt, wenn es darum geht, wer zu welchen Zeiten und wie lange auf Geräte oder Systeme zugegriffen hat. Betriebsleiter benötigen diese Informationen zudem, um die betriebliche Effizienz zu steigern und Anlagenprozesse zu optimieren.

All-in-One-Authentifizierung

Verlässliche Sicherheitsvorkehrungen sind entscheidend, um die genannten Risiken zu bewältigen und Transparenz zu schaffen. Ein unerlässlicher Teil einer umfangreichen Sicherheitsstrategie ist eine leistungsfähige Authentifizierungslösung, die Zugang und Zutritt regelt und zuverlässig auf berech-

◀ Intelligente Produktionsumgebungen bringen bei allen Vorteilen auch neue Sicherheitsrisiken mit sich

tigte Personen beschränkt. In der Realität gibt es in einer Fertigungsumgebung jedoch häufig eine Vielzahl von verschiedenen Authentifizierungssystemen. Mitarbeiter jonglieren mit mehreren Passwörtern und PINs, physischen Schlüsseln und Authentifizierungssystemen. Dies führt zu Passwort-Ermüdung, Ineffizienz und letztlich zu einem erhöhten Risiko durch Sicherheitslücken. Hinzu kommt, dass IT-Mitarbeiter mit der Verwaltung mehrerer Systeme konfrontiert sind. Dies erhöht die Arbeitsbelastung und Sicherheitsrisiken können leichter übersehen werden.

Einen innovativen Ansatz für den Schutz von industriellen Anlagen bietet eine All-in-One-Authentifizierungslösung auf der Grundlage von Radio Frequency Authentication (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 von der Maschinenauthentifizierung über die Anmeldung im Unternehmensnetzwerk bis zum Zutritt zu sensiblen Bereichen oder der Zahlung in der Kantine. Mit einem einheitlichen System lassen sich alle Bedarfe in Bezug auf Zutritt und Zugang in einer Fabrik abdecken.

Als Identifikationsmedium dient in der Produktion in der Regel der bereits vorhandene, robuste Mitarbeiterausweis. Aber auch Smartphones lassen sich bei Bedarf als Berechtigungsausweis einsetzten.

Als Identifikationsmedium dient in der Produktion in der Regel der Mitarbeiterausweis – aber auch Smartphones lassen sich einsetzen

Erfolgsfaktoren

Entscheidend für den nachhaltigen Erfolg einer solchen Authentifizierungslösung ist die Auswahl eines flexiblen und skalierbaren Systems, das auf die individuellen Bedürfnisse des Unternehmens zugeschnitten ist. Dabei sind folgende Aspekte zu beachten:

1. **Bedarfsanalyse:** Ermittlung der unternehmensspezifischen Anforderungen an das Authentifizierungs- und Zugangskontrollsystem
2. **Zukunftssicherheit:** Nur ein skalierbares System mit regelmäßigen Updates und Upgrades ist langfristig die richtige Lösung
3. **Integrationsmöglichkeit in bestehende Infrastruktur:** Nahtlose Integration der ausgewählten Lösung in die bestehende IT-Landschaft
4. **Flexibilität:** Multifrequenz-Lesegeräte ermöglichen Unternehmen den Einsatz von Identifikationsmedien mit unterschiedlichen Transpondertechnologien
5. **Schulung der Mitarbeitenden:** Vermittlung des notwendigen Know-hows im Umgang mit den neuen Systemen und Sensibilisierung für Sicherheitsaspekte
6. **Compliance und Datenschutzrichtlinien:** Berücksichtigung der im jeweiligen Land geltenden gesetzlichen Bestimmungen und Compliance-Richtlinien sowie der entsprechenden Arbeitsgesetze, die den Einsatz von Qualitätssicherungs- und Zeiterfassungssystemen regeln
7. **Kontinuierliches Monitoring und Optimierung:** Regelmäßige Überprüfung der implementierten Lösung auf Effektivität und eventuelle Anpassungen bei Bedarf

Unerlässlich für eine Sicherheitsstrategie ist eine leistungsfähige Authentifizierungslösung, die Zugang und Zutritt regelt und zuverlässig auf berechtigte Personen beschränkt

Eine einheitliche Authentifizierungslösung ist für moderne, vernetzte Fabriken unerlässlich, da sie die Komplexität reduziert und die Sicherheit erhöht. Dies steigert nicht nur die Produktivität, sondern minimiert auch das Risiko von Anlagenstillständen. Gleichzeitig schafft sie eine robuste und zukunftssichere Grundlage für den Schutz der Infrastruktur im Zeitalter von Industrie 4.0 und IoT-Anwendungen. GIT

Elatec GmbH
www.elatec-rfid.com