Möglichkeiten und Risiken der digitalen Transformation durch Industrial IoT

Mehr Chancen als Risiken

Die digitale Transformation hat in den letzten Jahren eine Revolution in der industriellen Landschaft eingeleitet. Das Industrial Internet of Things, oder auch IIoT genannt, spielt dabei eine zentrale Rolle.

In Zeiten der Vernetzung und Automatisierung bieten sich Unternehmen vielfältige Möglichkeiten, ihre Betriebsabläufe zu optimieren und die Produktivität zu steigern. Industrial IoT verspricht hier nicht nur eine nahtlose Integration von Maschinen, Geräten und Sensoren, sondern auch die Generierung und Analyse von umfangreichen Datenmengen in Echtzeit. Ohne Frage eröffnen diese technologischen Fortschritte neue Potenziale, gleichzeitig bringen sie jedoch auch Risiken mit sich.

In diesem Beitrag werden diverse Herausforderungen der Industrial IoT genauer betrachtet und Empfehlungen zur Gewährleistung einer sicheren und effektiven Nutzung von Industrial IoT beschrieben.

Digitale Transformation = Risiko? Gemäß einer Untersuchung des Marktforschungsunternehmens IDC aus dem Jahr 2022 liegt der Fokus vieler Industrieunternehmen hauptsächlich auf der Sicherstellung der Produktionsstabilität durch den Einsatz von Industrial Internet of Things (IIoT). Dabei gaben 30 % der befragten Unternehmen an, dass die Reduzierung von Ausfallzeiten sowie die Steigerung der Geschäftskontinuität und Resilienz zu ihren vorrangigen Zielen gehören. Die digitale Transformation der Industrie erscheint als entscheidender Schritt zur Schaffung dieser Stabilität. Bei den Kernkomponenten dieser Transformation handelt es sich um das Industrial Internet of Things und eine ganzheitliche Datenstrategie.

Allerdings haben laut der Studie lediglich 13 % der Industrieunternehmen eine Datenstrategie implementiert, die auch industrielle IoT-Projekte berücksichtigt. Sicherheitsbedenken stellen für 21 % der Industrieunternehmen eine große Herausforderung bei der Umsetzung von IIoT-Projekten dar. Diese Bedenken sind nicht unbegründet. Industrieanlagen sind seit einigen Jahren zunehmend Ziel von Cyberangriffen verschiedenster Art. Ein erfolgreicher Angriff kann schwerwiegende Auswirkungen auf die Betriebssicherheit, Umwelt, Wirtschaftlichkeit und Reputation haben. IIoT-Lösungen müssen daher robuste Sicherheitsmechanismen implementieren, die sowohl physische als auch cyberbezogene Bedrohungen abwehren können. Zusätzlich zählen aber auch die mangelnde Kommunikation zwischen IT und OT hinsichtlich gemeinsamer Risiken (28 %), der Schutz von IoT-Daten während der Übertragung und in Ruhe (26 %) sowie die unzureichende Übersicht über IIoT-Endpunkte im eigenen Netzwerk (23 %) zu weiteren Herausforderungen bei der Nutzung von Industrial IoT.

»IIoT & IoT ist doch dasselbe, oder?« – Eine Begriffserklärung. Oftmals werden die Begriffe IIoT und IoT im gleichen Kontext genannt, sind aber eigentlich zwei verwandte Konzepte, die sich in ihren Anwendungsbereichen und Einsatzgebieten unterscheiden.

IoT bezieht sich auf die Vernetzung und Kommunikation von Geräten und Objekten des täglichen Lebens, wie Haushaltsgeräte, Wearables, smarte Lautsprecher, Beleuchtungssysteme und viele mehr. Das Ziel von IoT besteht darin, das Leben der Menschen zu vereinfachen, Komfort zu bieten und Effizienz zu steigern.

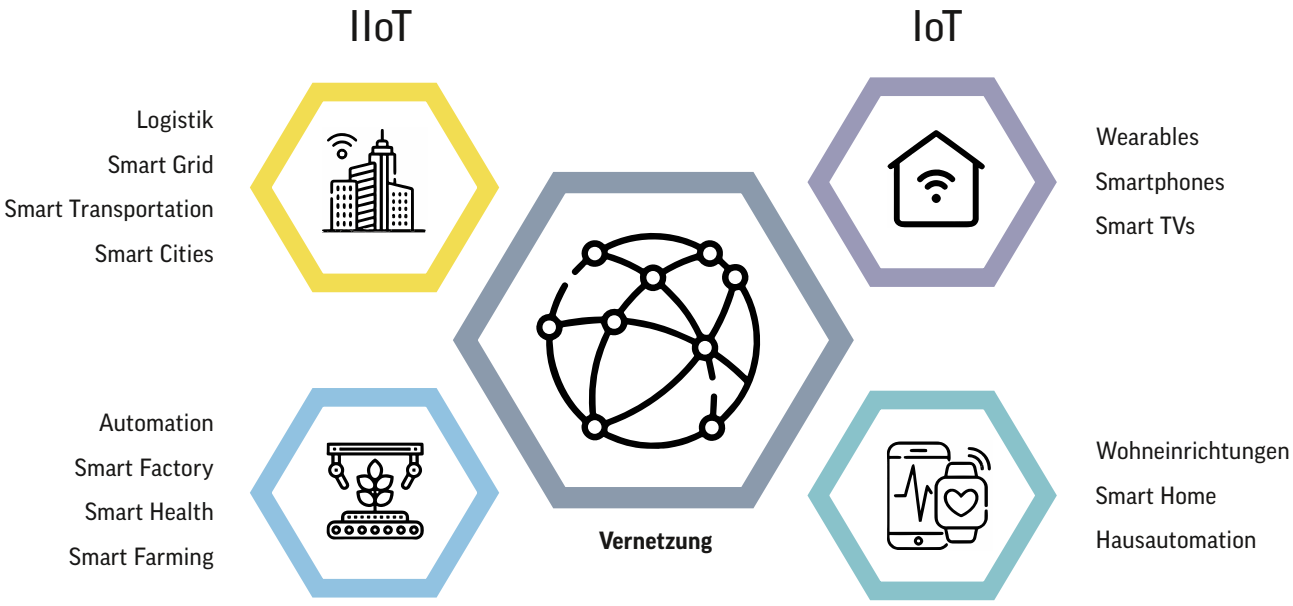
IIoT hingegen konzentriert sich speziell auf die Anwendung von IoT-Technologien in industriellen Umgebungen. IIoTs befasst sich mit der Vernetzung und Integration von Geräten, Maschinen und Sensoren in Produktionsanlagen, Fabriken, Logistikzentren sowie anderen industriellen Einrichtungen, um die betriebliche Effizienz zu verbessern, die Produktivität zu steigern und neue Geschäftsmöglichkeiten zu erschließen.

IIoT im Kontext der Anforderungen im OT/ICS-Bereich. Im Bereich des industriellen Internets der Dinge treffen die Anforderungen in der Operativen Technologie (OT) auf eine sich ständig weiterentwickelnde digitale Landschaft. Diese Schnittstelle zwischen traditionellen Betriebsabläufen und modernen Informationstechnologien stellt eine Vielzahl spezifischer Anforderungen an IIoT-Systeme dar.

Grundsätzlich ist es erforderlich, dass IIoT-Lösungen nahtlos in bestehende OT-Infrastrukturen integriert werden können. Basis hierfür ist die Kompatibilität einer breiten Palette von Geräten, Maschinen, Steuerungssystemen und den dazugehörigen Protokollen, die in Industrieanlagen eingesetzt werden. Nur so lässt sich eine reibungslose Kommunikation zwischen allen Systemen und Protokollen gewährleisten. Des

*/ IIoTs befasst sich mit der Vernetzung und Integration von Geräten, Maschinen und Sensoren in Produktionsanlagen

Einsatzgebiete



Quelle: Controlware

Weiteren müssen IIoT-Systeme robust und zuverlässig sein, um den hohen Anforderungen an die Betriebskontinuität in industriellen Umgebungen gerecht zu werden. IIoT-Systeme arbeiten in der Regel unter extremen Bedingungen, beispielsweise in Umgebungen mit starken Vibrationen, hohen Temperaturen oder feuchten Bedingungen. Besonderes Augenmerk sollte hier auf zuverlässige Datenverarbeitung und -übertragung gelegt werden, die Voraussetzung sind, Ausfallzeiten zu minimieren und die Produktionsleistung zu optimieren.

Insgesamt müssen IIoT-Systeme im Kontext der Operational Technology ein hohes Maß an Flexibilität, Zuverlässigkeit und Sicherheit bieten. Grundlage für die erfolgreiche Realisierung von Industrial IoT-Projekten ist eine vollumfängliche Strategie, die sowohl die Anforderungen der IT als auch der OT vereint. Nur so lässt sich eine erfolgreiche Planung, Implementierung und ein effektiver Betrieb garantieren. Nachfolgend zwei Beispiele für Einsatzgebiete des Industrial IoT.

IIoT-Asset-Tracking

IIoT-Asset-Tracking bezieht sich auf die Anwendung von IIoT-Technologien, um den Standort, den Zustand und andere relevante Informationen über verschiedene Arten von Assets in industriellen Umgebungen zu verfolgen und zu verwalten. Assets können dabei eine breite Palette physischer Objekte umfassen, unter anderem Maschinen, Fahrzeuge, Werkzeuge und Rohstoffe. IIoT-Asset-Tracking ermöglicht es Unternehmen, ihre Betriebsabläufe effizienter zu gestalten, die Produktivität zu steigern und die Betriebskosten zu senken. Die Echtzeitüberwachung von Assets erlaubt es Unternehmen, beispielsweise Engpässe und ineffiziente Nutzung zu identifizieren und entsprechende Maßnahmen zu ergreifen und so die Ressourcen-Auslastung zu optimieren.

Technologien, die im IIoT-Asset-Tracking eingesetzt werden, umfassen in der Regel eine Kombination drahtloser Sensoren, RFID-Tags (Radio Frequency Identification), GPS (Global Positioning System), drahtlose Netzwerke und Cloud Computing. Diese Sensoren und Systeme werden an den Assets angebracht oder integriert und erlauben es, wichtige Daten und relevante Parameter zu erfassen. Die erfassten Daten werden dann drahtlos an eine zentrale Datenplattform übertragen, wo sie analysiert und visualisiert werden. Unternehmen erhalten Echtzeiteinblicke in den Standort und den Zustand ihrer Assets und sind in der Lage, auf Basis dieser Informationen fundierte Entscheidungen zu treffen.

Predictive Maintenance

Predictive Maintenance, auf Deutsch vorausschauende Instandhaltung, ist ein entscheidender Ansatz in der industriellen Automatisierung, insbesondere in der OT. Diese fortschrittliche Methode revolutioniert die Art und Weise, wie Unternehmen ihre Anlagen und Maschinen verwalten und Wartungsarbeiten durchführen.

Im Kern basiert Predictive Maintenance auf der Nutzung von Daten und fortschrittlichen Analysemethoden, um den Zustand von Maschinen und Anlagen kontinuierlich zu überwachen. Diese Daten können aus dem vorher beschriebenen IIoT-Asset-Tracking stammen und werden in Echtzeit oder in regelmäßigen Intervallen gesammelt und analysiert. Durch die Analyse dieser Daten lassen sich Anomalien und Muster erkennen, die auf potenzielle Ausfälle oder Leistungsabfälle hinweisen könnten. Anstatt auf

zeitbasierte Wartungspläne zu setzen oder reaktiv auf Fehler zu reagieren, ermöglichen es diese Analysen, Wartungsarbeiten gezielt zu planen und durchzuführen – und zwar bevor ein Ausfall oder eine Störung auftritt. Dadurch können ungeplante Stillstandzeiten minimiert, die Produktivität gesteigert und die Lebensdauer der Anlagen verlängert werden.

»Triple A«: Autorisierung, Authentifizierung und Accounting sichern Produktionsumgebungen! Die Möglichkeiten und Chancen beim Einsatz von Industrial Internet of Things überwiegen klar gegenüber den Risiken – von der Optimierung der Anlagenleistung über die Vorhersage von Wartungsbedarf bis hin zur Implementierung intelligenter Logistiklösungen. Durch die Echtzeitüberwachung und -analyse können Unternehmen schnell auf Veränderungen reagieren, Sicherheitsvorfälle effektiv managen und mögliche Risiken und Schäden minimieren.

Die Einschränkung der Kommunikation auf Zonenebene, oder wenn möglich Systemebene, trägt ebenfalls zur Sicherheit bei, indem potenziell riskante Verbindungen minimiert werden. Durch eine restriktive Kommunikationspolitik lässt sich das Risiko von Angriffen und Datenlecks deutlich verringern.

Network Access Control (NAC) und Segmentierung als Teil eines Zonenkonzepts (unter anderem Ressourcen, Kommunikationsbeziehungen, Sicherheitsniveau und -kategorisierung) ermöglichen es, das Netzwerk zu schützen, indem der Zugriff auf autorisierte Benutzer und Geräte beschränkt wird. Durch die Segmentierung des Netzwerks in kleinere Einheiten können zudem potenzielle Bedrohungen isoliert und eingedämmt werden.

Insgesamt sind diese Sicherheitsmaßnahmen integraler Bestandteil einer umfassenden Sicherheitsstrategie, um sensible Daten und Systeme vor Cyberbedrohungen zu schützen und die Integrität der Unternehmensinfrastruktur zu gewährleisten.

Controlware, IT-Dienstleister und Managed Service Provider, ist ein kompetenter Partner, wenn es sich um die Realisierung von Projekten in den Bereichen Industrial Internet of Things (IIoT) und Operational Technology/Industrial Control Systems (OT/ICS) handelt. Durch eine maßgeschneiderte Architekturberatung analysieren die Controlware-Experten den aktuellen Stand der vorhandenen Infrastruktur und entwickeln individuelle Lösungen, die den heutigen und zukünftigen Anforderungen an intelligente Netzwerke gerecht werden – und die die Einhaltung der neuesten Normen, Regularien und Gesetze sicherstellen.

Christopher Gasteier,
Business Development Manager IT-Management
Controlware GmbH

www.controlware.de
blog.controlware.de