

# IUNO - Nationales Referenzprojekt zur IT-Sicherheit in Industrie 4.0

## ...auf einen Blick

### **IUNO- Leitbild**

Im Forschungsvorhaben IUNO, dem Nationalen Referenzprojekt zur IT-Sicherheit in Industrie 4.0, werden Bedrohungen und Risiken für die intelligente Fabrik identifiziert, Schutzmaßnahmen entwickelt und exemplarisch in vier Anwendungsfällen umgesetzt. Ziel ist es, möglichst allgemein verwendbare Lösungen für Herausforderungen der IT-Sicherheit im industriellen Anwendungsfeld zu entwickeln, um diese Unternehmen an die Hand zu geben. Die getesteten und übertragbaren IT-Sicherheitslösungen werden dann in einem Werkzeugkasten zusammengefasst und können als „Blaupause“ für die sichere Industrie 4.0 herangezogen werden. Besonders kleine und mittelständische Unternehmen, die sich bislang aus nicht abschätzbaren wirtschaftlichen Risiken gegen eine Digitalisierung der Produktion entschieden haben, können dadurch die Chancen des digitalen Wandels für sich nutzen.

### **21 Partner**

accesssec GmbH, Bosch Rexroth AG, Bosch Software Innovations GmbH, DFKI GmbH, Duravit AG, ESCRYPT GmbH, Fraunhofer AISEC, Fraunhofer IESE, Fraunhofer SIT, HOMAG, Infineon Technologies AG, Nobilis Werke, Phoenix Contact Electronics GmbH, Robert Bosch GmbH, Siemens AG, TRUMPF Werkzeugmaschinen GmbH + Co. KG, TU Darmstadt, TU München, Universität Kassel, Volkswagen AG, WIBU-SYSTEMS AG.

### **Förderer**

Gefördert vom Bundesministerium für Bildung und Forschung (BMBF), Projektkoordinator ist HOMAG.

## Projektdaten und -volumen

Laufzeit: 2015 - 2018

Projektvolumen: 33 Millionen Euro

## Die Themenschwerpunkte

Im Fokus von IUNO stehen vier Themen:

1. **Sichere Prozesse:** Eindeutige digitale Identitäten, Piraterieschutz, Sichere Einrichtung/Konfiguration von Produktionssystemen, Sicherheitsanalyse
2. **Sichere Daten:** Sicheres Speichern und Löschen von Daten, Datennutzungskontrolle, Sichere Anbindung an Cloud-Services, Schutz von Software sowie Produktions- und Maschinendaten
3. **Sichere Dienste:** Sicherung von Fernwartungszugängen, Trust Management und Trust Boundaries, Sichere Identifizierbarkeit des Dienstleisters, Datennutzungskontrolle, Sichere Anbindung an Cloud-Dienste
4. **Sichere Vernetzung:** Sichere Kommunikationsinfrastruktur, Sicherheit von Kommunikationssystemen, Vertraulichkeit und Verfügbarkeit der Funkkommunikation

## Vier Anwendungsfälle

Das vielfältige Themenfeld der Industrie 4.0 wird anhand von vier Anwendungsfällen betrachtet, die zusammen ein repräsentatives Bild der Herausforderungen des digitalen Wandels in der industriellen Produktion ergeben. Die Ergebnisse werden exemplarisch an Demonstratoren präsentiert, die reale und in der Industrie 4.0 relevante Szenarien aus der produzierenden und ausrüstenden Industrie widerspiegeln. Die Entwicklung der Demonstratoren wird dabei rechtswissenschaftlich begleitet und bewertet.

**Anwendungsfall 1: Kundenindividuelle Produktion**

Ziel des ersten Anwendungsfalls ist das Aufzeigen IT-sicherheitsbezogener Risiken und deren Bekämpfung in einer typischen Industrie 4.0-Produktionslandschaft. Das Szenario wird exemplarisch am Beispiel der Möbelindustrie umgesetzt, Im Anwendungsszenario werden zwei Demonstratoren umgesetzt: die Implementierung eines „Intelligenten Werkstücks“ sowie die Schaffung einer Simulations- und Testumgebung.

**Anwendungsfall 2: Technologiedatenmarktplatz**

Der Technologiedatenmarktplatz für industrielle Maschinen der Automatisierungstechnik orientiert sich im Wesentlichen an der Idee bereits existierender Marktplätze, über den Geräte mit zusätzlichen Funktionen ausgestattet werden können. Der Maschinenbetreiber kann Technologiedaten, die über den Grundumfang hinausgehen, über den Technologiedatenmarktplatz bedarfsgerecht und damit kostengünstig hinzulizenzieren. In der Vision von Industrie 4.0 werden die fehlenden Daten automatisiert über den Technologiedatenmarktplatz zur Verfügung gestellt. Die erforderlichen Technologiedaten sollen dabei über einen cloudbasierten Marktplatz gefunden, lizenziert und heruntergeladen werden können.

**Anwendungsfall 3: Fernwartung von Produktionsanlagen**

Ziel dieses Anwendungsfalls ist die Implementierung einer sicheren Möglichkeit, industrielle Anlagen aus der Ferne zu administrieren und zu warten. Hierbei wird ein Prozess abgebildet, bei dem ein externer Techniker über offene Netze einen temporären sowie gesicherten Zugang zu einem geschützten Fertigungsnetz erhält und sich mit einer Maschine vernetzen kann. Von einer zentralen cloudbasierten Plattform wird das Routing, das Ticketing sowie die Benutzer- und Zertifikatsverwaltung zentral gesteuert. Die Plattform übernimmt damit das komplette Management der Zugriffe auf die zu wartenden Maschinen und organisiert alle Verbindungen zwischen Maschinenbetreiber und Wartungsunternehmen.

**Anwendungsfall 4: Visueller Security-Leitstand**

Ziel im Anwendungsfall 4 ist die Entwicklung einer Visualisierungskomponente für die Darstellung und Bewertung des „Echtzeit“-Status der Informationssicherheit in der Produktion. Die Entwicklung eines Demonstrators soll die Möglichkeiten aufzeigen, bei einer akuten Bedrohung proaktiv, schnell und effizient das Risiko einzuschätzen und Schäden zu

verhindern. Eine kontinuierliche Sicherheitsüberwachung soll Spionage, Sabotage und Manipulationsversuche erkennen können, die Sicherheitsrisiken identifizieren und den Informationsfluss abbilden.

## **Weitere Informationen**

[www.iuno-projekt.de](http://www.iuno-projekt.de)

## **Pressekontakt**

Ute Fertig

Managerin Kommunikation IUNO

IUNO-Koordinierungsstelle

c/o TU Darmstadt

Otto-Berndt-Straße 2

64287 Darmstadt

Tel. +49 6151 16 27314

fertig@dik.tu-darmstadt.de