

IT-SICHERHEIT FÜR DIE INDUSTRIE



TRENDS

Produktions-Ökosystem

Die Unternehmen in der produzierenden Industrie möchten seit jeher die Maschinenauslastung optimieren, die eigenen Lagerbestände minimieren und die Energieeffizienz steigern, um ihre Produktivität zu maximieren und ihre Wettbewerbsfähigkeit zu erhalten. Durch die steigende Vernetzung werden die Produktionssysteme zu industriellen Umgebungen mit Anbindung an ERP-Systeme und andere Anwendungen der Büro-IT.

Maschinenkommunikation

Komponenten und Geräte werden verstärkt mit IuK Technologie ausgestattet. Aus ehemals isolierten Einheiten entstehen so Systeme von Systemen, den sog. Cyber Physical Systems, die in der Lage sind miteinander zu kommunizieren und mittels IT-Technik zum Beispiel auch Informationen über Produktionsabläufe, die Produkte selber und Logistikketten verarbeiten können.

Big Data

Durch den verstärkten Einsatz von Sensoren steigt die Informationsdichte in Produktionsumgebungen. Dadurch lässt sich nicht nur die Fertigung minutiös überwachen, sondern auch die Produkthistorie verlässlich nachvollziehen und rechtlich belastbar nachweisen – auch über Unternehmensgrenzen hinweg.

HERAUSFORDERUNGEN

Die wachsende Komplexität von industriellen Prozessen stellt nur eine der neuen Gefahren da, welche die Veränderungen im industriellen Sektor mit sich bringen. Die massive informationstechnische Vernetzung über das Internet macht produktionstechnische Anlagen und die dort hergestellten Produkte verstärkt zu einem attraktiven Ziel für Industriespione, Saboteure und organisierte Cyberkriminelle. Maschinenspezifische Angriffe mittels Trojanern wie Stuxnet, Duqu, Flame, Shamoon oder die jüngst bekannt gewordenen Aktivitäten diverser Nachrichtendienste wie Prism, Byzantine, ShadyRat oder Tempora haben bereits gezeigt, dass es sich hierbei um äußerst reale Bedrohungen handelt.

Schutz von Know-how und Fertigungswissen

Angesichts der Informationsmöglichkeiten in Produktionsumgebungen, wächst die Notwendigkeit wertvolles Know-how und Alleinstellungsmerkmale zu schützen, ohne Prozesse und Qualität zu beeinträchtigen. Die zu schützenden Güter, Prozesse und Daten sind dabei äußerst unterschiedlich: Maschinen- und Anlagenhersteller geht es teilweise um Patentschutz, teilweise geht es aber auch darum, Maschinenkonfigurationen und -Einstellungen zu schützen.



ANGEBOTE

Fraunhofer SIT besitzt langjährige Erfahrung in der Konzeption und Realisierung von kryptografischen Konzepten, die uns in die Lage versetzt Soft- und Hardware-Elemente so zu verzahnen, wie es für den jeweiligen Anwendungsfall erforderlich ist. Zur Durchführung von umfassenden Sicherheitsbewertungen in Anlehnung an nationale und internationale Standards betreibt das Institut ein Testlabor.

Für Unternehmen aus dem Produktionsumfeld bietet das Fraunhofer SIT folgende Service-Angebote:

- Erstellung von Bedrohungsanalysen und Mindestanforderungen
- IT-Sicherheitsbewertung von Anlagen und Komponenten
- Integration von IT-Sicherheitsmechanismen
- Entwicklung von Protokollen und IT-Sicherheitsfunktionen
- Entwicklung von Sicherheitsarchitekturen für industrielle Netze
- Produktschutz durch Einsatz kryptografischer Systeme
- Secure Engineering für Software-Entwicklungsprozesse
- Technische Beratung

KUNDENNUTZEN

Für Anlagenbetreiber:

- Schutz vor Produktionsausfällen und -störungen
- Schnelle und effiziente Unterstützung beim Risiko-Management

Für Anlagen- / Maschinen- / Komponentenhersteller:

- Wettbewerbsvorteile durch nachweisbare Sicherheitseigenschaften
- Schutz vor Produktpiraterie und Reverse Engineering

REFERENZEN

Piraterie-Schutz für Anlagen

Im Auftrag eines Industriekunden hat Fraunhofer SIT ein Konzept entwickelt, das Anlagen vor unerlaubter Manipulation und Reverse Engineering schützt. Implementiert wurde das System mit bewährten kryptografischen Verfahren. Selbst Insider können ohne Zugriff auf die geheimen Schlüssel weder einzelne Bauteile noch die zentrale Steuereinheit fälschen.

Trusted Core Network

Mit Partnern aus der Industrie hat Fraunhofer SIT das Trusted Core Network (TCN) entwickelt. Das TCN ist in der Lage, die Identität von Netzknoten zu prüfen und einen gewünschten Zustand der Netzknoten zu gewährleisten.

Pharmaceutical Identification & Compatibility Tool (PIC)

PIC ist eine Lösung zur Echtheitsverifikation von Produkten entlang pharmazeutischer Lieferketten auf Basis von Low-Cost-RFID-Tags. Mit dem Tool können alle Teilnehmer der Lieferkette die Echtheit eines Produkts via NFC-fähigem Handy prüfen und den nächsten Empfänger des Produkts innerhalb der Kette spezifizieren.

ContainIT – Sichere IT-Infrastruktur für die Logistik

Entwicklung einer IT-Infrastruktur, welche die Vielzahl an Teillösungen und Teilprozessen in der Container-Logistik integriert und die Effizienz und Sicherheit steigert. Fraunhofer SIT untersuchte die Telemetriesysteme sowie die Sensortechnologien zur Überwachung des Containerstatus.

DAS INSTITUT

Die Informationstechnologie hat bereits weite Teile unseres Alltags durchdrungen: Ob Auto, Telefon oder Heizung – ohne IT-Einsatz sind die meisten Geräte und Anlagen heute nicht mehr denkbar. Insbesondere Unternehmen nutzen IT-Systeme zur effektiven Gestaltung ihrer Arbeitsprozesse. Fraunhofer SIT beschäftigt sich mit dem Schutz dieser Systeme vor Ausfällen, Angriffen und Manipulationen.

Fraunhofer SIT ist für Unternehmen aller Branchen tätig. Viele erfolgreiche Projekte mit internationalen Partnern sind eindrucksvoller Beweis für eine vertrauensvolle Zusammenarbeit. Zu unseren Kunden zählen unter anderem HP, die Software AG, SAP, Lufthansa und das Bundesamt für Sicherheit in der Informationstechnik.

KONTAKT

Dr. Thorsten Henkel

Telefon 06151 869-4271

Fax 06151 869-224

thorsten.henkel@sit.fraunhofer.de

Fraunhofer-Institut für Sichere Informationstechnologie

Rheinstraße 75

64295 Darmstadt

www.sit.fraunhofer.de