Sicherheitshardware schafft Mehrwert für Industrie 4.0

Mit der Vernetzung von Firmen- und Produktionsnetzwerken werden Tür und Tor zur virtuellen Fabrik geöffnet. Bei Schutzmechanismen vertrauen viele Anlagenbetreiber auf rein softwarebasierte Lösungen. Effektiv höheren Schutz vor Hackern und Spionen bieten hardwarebasierte Sicherheitslösungen für vernetzte Maschinen und Kommunikationsknoten.

TEXT: Jürgen Spänkuch, Infineon **BILDER:** Infineon

Industrie 4.0 verspricht effizientere Produktionsprozesse, ermöglicht kundenindividuelle Produktionsvorgänge und eröffnet den Unternehmen neue Geschäfts- und Servicemodelle. Durch die zunehmende Vernetzung steigen jedoch auch die Sicherheitsrisiken. Denn die automatisierte Kommunikation zwischen cyber-physischen Systemen schafft neue Einfallstore für Angriffe aus dem Netz. Allein der Datentransfer über das Internet erhöht das Risiko von Datendiebstahl und Manipulation an Firmennetzwerken, Geräten oder Informationen. Stillstand von Maschinen und Produktion, aber auch Diebstahl von geistigem Eigentum und Know-how sind unter Umständen die Folge. Wer also die Türen zu seinen Fabriken öffnet, muss sein besonderes Augenmerk auf die Identität, Authentizität und Integrität der vernetzten Maschinen und Anlagen legen.

Sicherheit im System verankern

Ob in der Industrieautomatisierung oder dem vernetzten Zuhause – bisher werden zur Authentifizierung von Geräten in einem Netzwerk oftmals rein Software-basierte Lösungen

Herausforderungen für Smart Factories mit Blick auf Datensicherheit

eingesetzt. Software besteht jedoch aus geschriebenem Code und kann meist recht einfach gelesen, analysiert und kopiert werden. Und sobald Code analysiert ist, kann er von einem Angreifer abgeändert werden, etwa um Zugang zu sensiblen Informationen zu bekommen oder die teilweise bis komplette Kontrolle über eine industrielle Anlage zu erlangen. Soft- oder Firmware allein bieten damit nicht ausreichend Schutz vor Angriffen.

Sicherheitschips können nicht nur als Daten-Tresor eingesetzt werden, sondern erlauben auch aktive Authentifizierung und bilden damit einen Vertrauensanker in der virtuellen Welt. In einem Sicherheitschip kann individueller Datencode gesichert und verschlüsselt abgelegt werden. Fehler und Manipulationen am Datencode können so frühzeitig erkannt und unerlaubte Veränderungen am System verhindert werden. Durch die Verbindung mit gesicherter Hardware wird Software also vertrauenswürdig. Das belegen umfangreiche Erfahrungen aus dem Bereichen Trusted Computing oder der Einsatz von Sicherheitselementen in Smartphones.

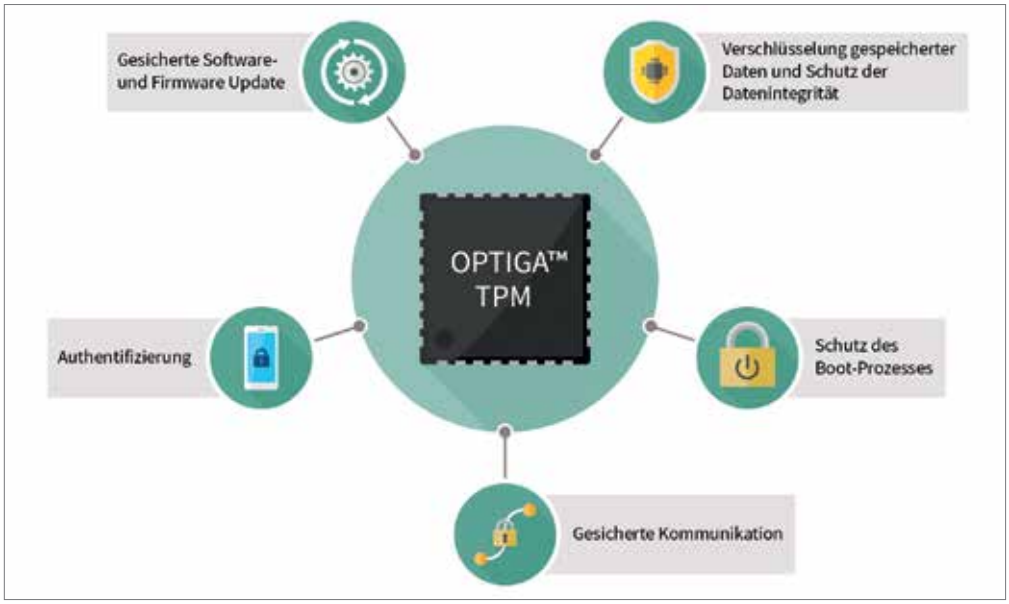
TPM-Chips – der Allrounder für Embedded-Systeme

Das breiteste und am stärksten standardisierte Spektrum an Sicherheitsfunktionen decken TPM-Chips (Trusted Platform Module) ab. Diese speziellen Sicherheitscontroller basieren auf dem internationalen, offenen Standard der Trusted Computing Group (TCG), einem Herstellerverbund aus der IT-Industrie. Nachdem sich TPM-Chips bereits seit Jahren in Computeranwendungen bewährt haben, findet diese Technologie auf Grund des gestiegenen Sicherheitsbedarfs auch Eingang in vernetzte industrielle Systeme. Um vernetzte Betriebsabläufe und Anlagen zu schützen, werden Kommunikationsknoten wie Router, Industrie-PCs und komplexe Steuereinheiten um TPM-Chips erweitert. Die entsprechenden Embedded-Systeme profitieren so ebenfalls von den Sicherheitsfunktionen der TPM-Spezifikation sowie den vielfältigen Vorteilen der Standardisierung.

Im Vergleich zu proprietären Lösungen ist das TPM mit einem Funktionsumfang ausgestattet, der durch den internationalen Standard ISO/IEC 11889 definiert ist. Kunden und Anwender können daher auf eine höchst standardisierte Sicherheitslösung bauen. Das erhöht zugleich Flexibilität und Planungssicherheit.

Sichere Identitäten für Maschinen und Geräte

TPM-Chips können als ein Ausweis für Geräte dienen, die Teil eines komplexen Netzwerkes sind. Gesicherte Identitäten für Maschinen bilden die Grundlage für die Implementierung von nachhaltigen Sicherheitskonzepten in Smart Factories. Auf der Basis gesicherter Hardware lässt sich eine Kette an Sicherheitsmaßnahmen aufbauen, die ein Industrieautomatisierungssystem schützen. Hierfür werden ein individuelles kryptographisches (Endorsement-) Zertifikat sowie ein dazugehöriger privater Schlüssel in den Chip eingebracht und



Typische Anwendungsfälle im Überblick

geschützt abgelegt. Darüber hinaus finden TPM-Chips ihre Anwendung in einer Vielzahl von weiteren sicherheitsrelevanten Anwendungen.

Besonderheiten der Industrie-Automatisierung

In Industriesteuerungen können TPMs zur gesicherten Datenübertragung oder -speicherung oder Integritätsüberprüfung eingesetzt werden. Auch beim gesicherten Fernzugriff, zum Beispiel zur Wartung der Systeme oder Softwareaktualisierung, schützt das TPM mittels Authentifizierung der Geräte die Zugänge zum System. Hierbei kommt es vor allem auf die Kombination von gesicherter Hardware und Software-basierten Sicherheitsmechanismen an.

Das TPM dient bei den Anwendungen als gesicherter Speicher für geheime Schlüssel und schützt die Durchführung von kryptographischen Operationen. Für typische Anwendungen wie das SSL/TLS-Protokoll werden Schlüssel statt auf dem Speicher des Hauptprozessors im gesicherten Speicher des TPMs abgelegt und ausschließlich intern verarbeitet, so dass sie vor Angriffen geschützt sind.

In Verbindung von TPM und Sicherheitsmechanismen wie Verschlüsselung werden Geräte vor Manipulation geschützt. Aufgrund der Standardisierung sowie einer Vielzahl an verfügbaren Interfaces wie SPI, I^2C oder LPC ist eine einfache Integration möglich. Darüber hinaus sind OPTIGA TPM-Chips von Infineon auf die Anwendung in rauen Umgebungen vorbereitet, beispielsweise durch Auslegung auf einen erweiterten Temperaturbereich.

Vor dem Hintergrund steigender Komplexität durch Sicherheitsanforderungen bietet das Infineon Security Partner Network (ISPN) Lösungen, die auf die spezifischen Bedürfnisse unterschiedlicher Branchen und Unternehmen zugeschnitten sind. Das Angebot der Netzwerkpartner deckt dafür die gesamte Wertschöpfungskette ab, von Beratung und Design bis zu Systemintegration und Servicemanagement. Eine Auswahl bestehender Fallbeispiele, und Lösungsansätze sind im virtuellen Showroom *www.infineon.com/ispn* zu finden.

Sicherheit schafft Mehrwert für Industrie 4.0

Mit dem Internet der Dinge nimmt die Vernetzung von Mensch und Maschine stetig zu. Die vielfältigen Anwendungsfälle zeigen eines: Sicherheit in Embedded-Systemen schafft Mehrwert. Sie bietet Differenzierungspotenzial, ermöglicht neue Geschäfts- und Servicemodelle und schützt sensible Daten von Herstellern und Nutzern. Letztendlich muss Sicherheit aber einfach zu integrieren und zu verwalten sein. Die Realisierung von intelligenten Fertigungen und geschützten globalen Produktionsprozessen im Rahmen von Industrie 4.0 setzt zudem voraus, dass die Implementierung zuverlässig und kosteneffektiv ist – eine der wesentlichen Vorteile der OPTIGA-Sicherheitslösungen von Infineon. ❐