Cybersicherheit für Industrial Ethernet

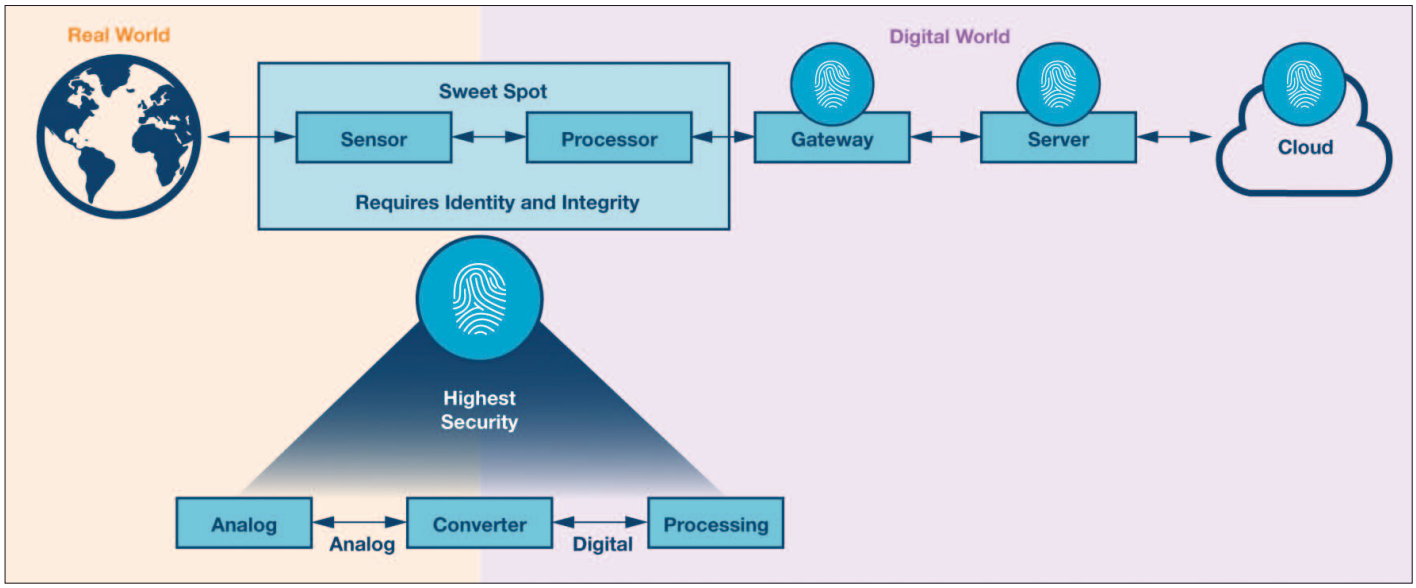

Bild 1: Der „Sweet Spot" - Höchste Sicherheit am Übergang von der analogen zur digitalen Welt

Der Wandel hin zur Digitalisierung ist kaum an anderer Stelle so spürbar wie im industriellen Bereich. Die Produktionslandschaft verändert sich, sie wird vernetzt, sie kommuniziert untereinander, zwischen unterschiedlichen Unternehmensbereichen oder gar über Unternehmensgrenzen hinweg. Es findet ein reger Austausch von unzähligen, unterschiedlichsten Daten zwischen allen Beteiligten statt, egal ob Mensch oder Maschine. Waren früher einzelne Maschinen miteinander verbunden, wird künftig die Vernetzung allgegenwärtig sein – angefangen bei einzelnen Sensoren und Aktuatoren, über Maschinen bis hin zu kompletten Systemen. Alle Teilnehmer der Produktion werden durch den von Industrie 4.0 bzw. (Industrial) Internet of Things (IoT) getriebenen Wandel zur Digitalisierung mit intelligenten Netzwerken verbunden. Als wesentlicher Kommunikationsstandard kristallisiert sich das industrielle Ethernet heraus, da es gegenüber bisherigen Feldbussen entscheidende Vorteile wie größere Übertragungsraten und eine höhere Zuverlässigkeit bietet. Außerdem kann so die gesamte Kommunikation auf eine einheitliche Basis gebracht werden, die das klassische Ethernet um Echtzeitfunktionen und Determinismus ergänzt. Man spricht von Time Sensitive Networking (TSN), einem Zusammenschluss mehrerer Substandards, die im Rahmen der Standardisierungsgruppe IEEE 802 (Time Sensitive Networking Task Group) erarbeitet werden und u. a. Mechanismen zur Datenübertragung mit möglichst geringen Latenzzeiten bzw. hoher Verfügbarkeit definieren.

Autor:
Thomas Brand
Analog Devices Inc.
www.analog.com

Die Basis dieser TSN-Netzwerke

bilden unzählige Sensoren, Geräte und Systeme, die immer mehr mit künstlicher Intelligenz ausgestattet werden und künftig in der Lage sind, eigenständig Entscheidungen zu treffen. Derartig autonome Systeme und das erhöhte Datenaufkommen stellt Hersteller von Automatisierungsanlagen, gerade im Bereich der IT- bzw. Cybersicherheit vor extreme Herausforderungen. Bislang gut abgeschottete Maschinenbereiche müssen künftig für die Kommunikation nach außen hin offen und zugreifbar sein. Cybersicherheit gewinnt im Vergleich zur reinen Prozesssicherheit bzw. Produktionsverfügbarkeit immer mehr an Bedeutung. Auch Vorfälle wie Stuxnet, Wanna Cry oder der Angriff auf den deutschen Bundestag steigern deren Bedeutung.

Cybersicherheit

ist eine komplexe Angelegenheit mit den Schutzzielen Vertraulichkeit, Integrität, Verfügbarkeit. Von Vertraulichkeit spricht man, wenn keine unautorisierte Informationsgewinnung möglich ist. Integrität umfasst sowohl die Korrektheit der Daten (Datenintegrität) als auch die korrekte Funktionsweise des Systems (Systemintegrität). Unter Verfügbarkeit fällt der Grad der Funktionalität der informationstechnischen Systeme, d. h. ob die Systeme jederzeit betriebsbereit sind und ob die Datenverarbeitung auch korrekt abläuft. Bei Authentifizierung und Autorisierung wird die Identität des Benutzers und dessen Zugriffsrechte bzw. die sichere Herkunft der Daten geklärt. Durch Verbindlichkeit / Nichtabstreitbarkeit wird sichergestellt, dass die Kommunikationsteilnehmer Nachrichten nicht ablehnen.

Cybersicherheit behandelt somit ein sich ständig wandelndes Problem, welches über den gesamten Lebenszyklus von Geräten, Systemen, aber auch Netzwerken ein Thema ist. Da ständig neue Schwachstellen aufgedeckt und neue Methoden zum Hacken gefunden werden, gilt es die Geräte und Systeme immer wieder zu aktualisieren und die Schwachstellen zu beseitigen. Systeme müssen daher so konzipiert sein, dass sie sichere Updates für wichtige Funktionen zulassen, um dauerhaft geschützt zu sein. Hierbei handelt es sich um

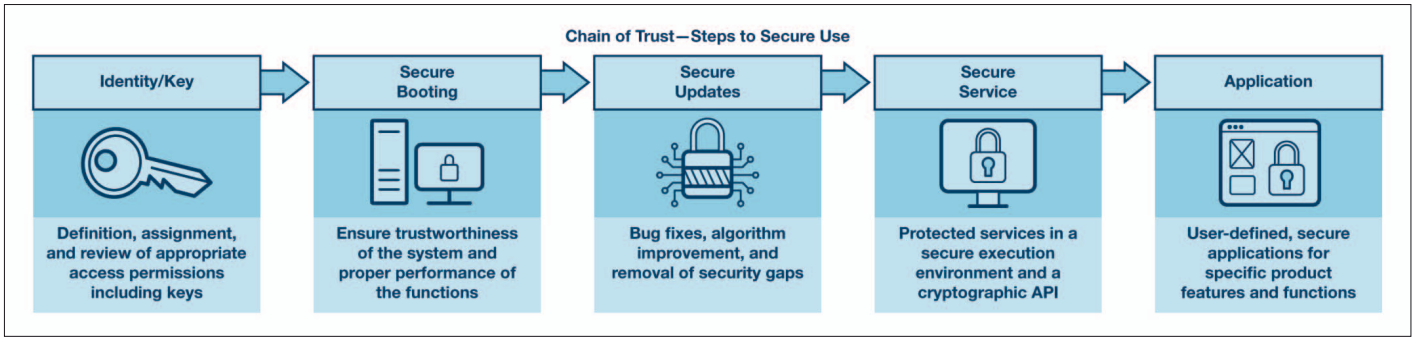

Bild 2: „Root of Trust" – Die Schritte des Vertrauensaufbaus für eine sichere Anwendung

ein sehr umfangreiches Themengebiet. Daher ist es sinnvoll, bereits im frühen Entwicklungsstadium mit entsprechenden IT- und Sicherheits-Experten zusammenzuarbeiten. Ansonsten besteht die Gefahr, dass durch unbemerkte Sicherheitslücken Schäden auf die Unternehmen zukommen.

Sicherheit bei höherem Datenaufkommen

Traditionell wurde Cybersicherheit als ein IT-Problem angesehen, das die Implementierung sicherer Betriebssysteme, Netzwerk- und Anwendungsprotokolle, Firewalls und anderer Lösungen zum Schutz vor Netzwerkangriffen, erforderte. Bedingt durch den Wandel zur Digitalisierung müssen Maschinen künftig jedoch möglichst intelligent und selbstständig arbeiten, was zu mehr Funktionalitäten, mehr Konnektivität und gleichzeitig zu einem höheren Datenaufkommen führt. Folglich nimmt auch die Bedeutung der Risikobewertung der Systeme enorm zu. Wo Sicherheit bzw. der Schutz der Systeme bisher nicht erforderlich war, kann sich nun eine entscheidende Schwachstelle auftun. Für die Hersteller gilt es daher, die Schwachstellen äußerst sorgfältig zu überprüfen, zu bewerten und entsprechende Schutzmaßnahmen zu ergreifen.

Geeignete Sicherheitsfunktionen einbauen

Die Implementierung von geeigneten Sicherheitsfunktionen so früh wie möglich, am besten direkt am Anfang der Signalkette von Systemen, d. h. am Übergang von der realen, physikalischen Welt zur digitalen Welt, am sogenannten „Sweet Spot", scheint hierbei die vielversprechendste Stelle der Signalkette zu sein. Diese Stelle bildet für gewöhnlich der Sensor bzw. Aktuator. Hier ist die Komplexität bei der Kodierung von vertrauenswürdigen Daten in der Regel noch relativ gering.

Sweet Spot

Wie in Bild 1 dargestellt, erfordert der Sweet Spot dabei allerdings ein hohes Maß an Identität und Integrität, um höchste Datensicherheit und damit auch Vertrauen der Betriebssysteme in sichere Daten zu erlangen. Die Umsetzung von Identitäten und Integrität bereits auf Hardwareebene, d. h. bereits in Silizium eingebettete Schutzfunktionen, bieten dabei den vielversprechendsten Ansatz. Hier beginnt auch die sogenannte „Root of Trust" (Vertrauenskette).

Root of Trust – die Vertrauenskette

bildet eine Reihe von zusammengehörenden sicheren Funktionen, die als weitestgehend separate Recheneinheit den kryptografischen Prozess in den Geräten steuert. Dabei wird eine sichere Datenübertragung i.d.R. dadurch erzeugt, indem Hard- und Softwarekomponenten in sequentiell verknüpften Schritten kontrolliert werden. Durch die sequentielle Abfolge der einzelnen Schritte, wie diese in Bild 2 zu sehen sind, wird sichergestellt, dass die Datenkommunikation wie gewünscht und unbeschadet abläuft. Demzufolge kann von einer gut geschützten Anwendung ausgegangen werden.

Die Sicherstellung einer nicht angreifbaren Anwendung erfolgt durch die Nutzung einer eigenen Identität bzw. eines eigenen Schlüssels. Hier werden die Zugriffsberechtigungen der Geräte oder Personen vergeben und überprüft. Identitäten und Schlüssel sind zwar etabliert, stellen in diesem ersten Schritt der Vertrauenskette dennoch das kritischste Element dar, denn das Gerät ist nur so sicher, wie der Schutz des Schlüssels. Aus diesem Grund gilt es weitere Schutzfunktionen zu implementieren, die für eine sichere Aufbewahrung des Schlüssels und Weiterleitung an die richtigen Empfänger sorgen.

Sicherer Bootvorgang

Um die eigentlichen Funktionen der Geräte vor unerlaubten Zugriffen zu schützen, bedarf es beim Start der Geräte eines sicheren Bootvorgangs. Durch Authentifizierung und anschließender Dechiffrierung der Software wird gewährleistet, dass die Geräte vor Angriffen und Manipulation geschützt sind. Ohne einen sicheren Bootvorgang ist es für potentielle Angreifer relativ einfach, sich in die Systeme einzuschalten, sie zu manipulieren und fehlerbehafteten Code auszuführen.

Sichere Updates

sind ein wichtiger Schritt, um der sich ständig ändernden Anwendungsumgebung und den sich auftuenden Sicherheitslücken gerecht zu werden. Sobald neue Schwachstellen in Hardware oder Software entdeckt werden, sind diese schnellst möglichst durch Aktualisierungen der Geräte zu beheben, noch bevor größerer Schaden durch Angriffe entstehen kann. Sichere Updates werden auch durchgeführt, um etwaige Produktfehler zu beheben oder Produktverbesserungen vorzunehmen.

Damit eine vertrauenswürdige Umgebung zur Ausführung der gesamten Funktionen entsteht, sind zusätzlich sichere Services, beispielsweise eine kryptografische Programmierschnittstelle (API), gefordert. Auch sie beinhaltet Schutzfunktionen wie Verschlüsselung, Authentifizierung und Integrität.

All diese sicheren Funktionen sollten in einer von den eigentlichen Anwendungen der Geräte separierten und geschützten Ausführungsumgebung platziert sein, damit gewährleistet werden kann, dass sich keine Fehler in den Codes befinden, die zu Folgeschäden der Geräte führen könnten.

Cybersicherheit, ein wachsendes Thema für Halbleiterhersteller

Halbleiterhersteller beschäftigen sich bereits seit geraumer Zeit mit dem Thema Cybersicherheit. Um den zunehmenden Sicherheitsanforderungen gerecht zu werden, kann man beispielsweise das Konzept der Root of Trust in die Produkte und Entwicklungen einfließen lassen. Das Ziel ist es, entsprechend angriffssichere Produkte anbieten zu können. Dies bedeutet Sicherheit dort einzuführen, wo eine Verbindung zu einem Netzwerk besteht. Hauptsächlich sind hier Halbleiterprodukte für den Kommunikationsbereich gemeint, allen voran Industrial Ethernet- und TSN-Komponenten. Ferner ist Sicherheit auch überall dort unausweichlich, wo ein integriertes System auf einem Chip vorhanden ist, d. h. wo ein Mikroprozessor sich mit essenziellen Funktionalität beschäftigt.

Durch eine frühzeitige Zusammenarbeit mit dem Kunden können die grundlegendsten Sicherheitsanforderungen mit in die Designs aufgenommen und somit die gesamte Signalkette geschützt werden. So lassen sich Identitäten bereits auf physikalischer Ebene, direkt am Sensorknoten der Signalkette einbetten

Durch sichere Schlüsselgenerierung/ -verwaltung, sicheres Booten, sichere Updates, einen sicheren Speicherzugriff sowie sicheres Debuggen reichen diese soge-

nannten CSS-Sicherheitslösungen über die klassischen Verschlüsselungstechnologien hinaus. Sie bieten einen vollintegrierten Ersatz für klassische kryptografische Lösungen und ermöglichen künftig ohne viel Aufwand die Realisierung äußerst sicherer Hardware-Plattformen. Die CSS-Cybersicherheitstechnologie, bzw. all deren Sicherheitsfunktionen werden für gewöhnlich auf einem separaten FPGA-basierten Subsystem umgesetzt, das parallel neben den eigentlichen Anwendungsfunktionen des Chips läuft. Man spricht hierbei von einer „Trusted Execution Environment" (TEE), wie in Bild 3 dargestellt.

Die FPGA-basierte Umsetzung

ermöglicht problemlos Software-Upgrades von Feldgeräten zum Beheben etwaiger Sicherheitslücken. Im Gegensatz zu softwarebasierten Verschlüsselungstechnologien wird bei dieser hardware-basierten Lösung ein dedizierter Prozessor für die Berechnung der Verschlüsselungsalgorithmen sowie ein dedizierter Speicher für das Hosting des sicheren Schlüssels verwendet. Der dedizierte Speicher ist dabei nur über den dedizierten Prozessor zugänglich. Durch die Verwendung der dedizierten Komponenten kann die TEE und alle sensiblen Operationen vom Rest des Systems isoliert werden, was die Ausführungsgeschwindigkeit der Verschlüsselungsfunktionen erhöht und gleichzeitig die potenzielle Angriffsfläche für Hacker deutlich reduziert. Es verhindert jeden unbefugten Zugriff auf den restlichen Chip, während der Zugriff auf die kryptographische Funktionalität über die API-Schnittstelle stattfindet.

Zusammenfassung

Cybersicherheit und der dabei stattfindende Schutz der technischen Systeme vor etwaigen Angriffen ist ein zentrales Element beim Wandel hin zur Digitalisierung, insbesondere in der Automatisierungsbranche. Aufgrund fehlender Regularien und Kenntnisse im Bereich der Cybersicherheit, besteht derzeit noch bei vielen Unternehmen große Unsicherheit, wie sie dieses wichtige Thema angehen sollen. Die Bewertung von Risiken ihrer Prozesse, ist dabei nur der Anfang, jedoch ein zentraler Punkt. Allerdings sollte die Cybersicherheit weiter in den Unternehmen und deren Produkte verankert werden. Hierbei ist die Unterstützung von Experten empfehlenswert.

Es sind bereits Produkte auf dem Markt verfügbar, die das Einführen der Sicherheitslösungen erleichtern.

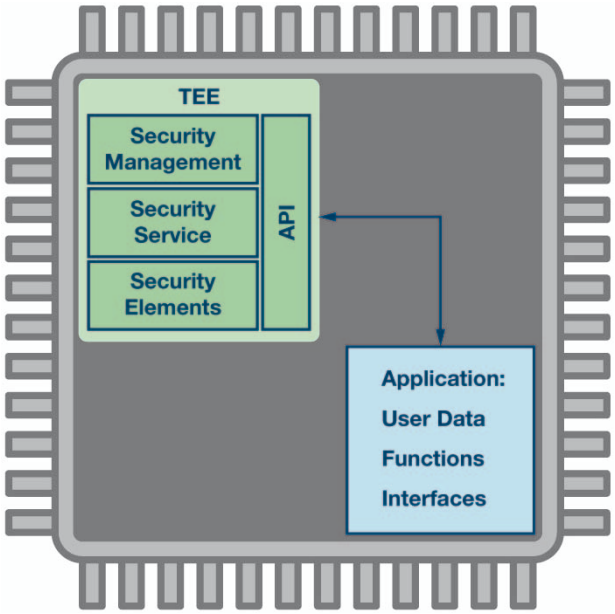

Bild 3: FPGA-Plattform mit integrierter hardwarebasierter Verschlüsselungstechnologie in Form einer separaten TEE

Dazu zählen Entwicklungen von bereits schlüsselfertige, hardwarebasierte Lösungen, die den Kunden die Einbindung von Datensicherheit problemlos ermöglichen. Aufgrund zahlreicher Vorteile gegenüber softwarebasierten Verschlüsselungstechnologien, konzentrieren sich Halbleiterhersteller mehr und mehr auf hardwarebasierte, kryptografische Lösungen, um vor unerwünschten Angriffen zu schützen. Sensiblen Anwendungen, in denen Sicherheit und hohe Zuverlässigkeit von entscheidend sind, wie zum Beispiel in den Märkten für Industrieautomation, Automobil, Energie bzw. kritische Infrastrukturen, können somit ein Höchstmaß an Sicherheit geboten werden. ◄