

Sicherheit für die vernetzte Industrie

OPC UA-fähige RFID-Lesegeräte mit Secure Elements schützen Kommunikation

RFID in der Industrie 4.0

Radio Frequency Identification (RFID) zählt seit langem zu den wichtigen Bausteinen der modernen industriellen Welt. Klein, unauffällig und fast überall vertreten sind RFID-Etiketten heutzutage der Fahrtschein, mit dem sich Daten und Güter durch die industriellen Abläufe bewegen. Ihr ursprünglicher Einsatzbereich in der internen und externen Warenlogistik, in der die kleinen Etiketten die Bewegung der Waren von A nach B transparent und immer nachvollziehbar machen, haben sie lange hinter sich gelassen und sind heute unerlässliche Helfer, beispielsweise für Zugangskontrollsysteme oder Produktionssteuerungen. In der Industrie 4.0 wird die industrielle Produktion noch abhängiger von der genauen und automatisierten Nachverfolgung und Identifikation von Material und Daten. RFID ist eine wichtige Technologie, um die immer komplexeren und heterogenen, engmaschig vernetzten industriellen Anlagen flexibel zu halten. Als kostengünstiges und fast universell genutztes System passt RFID perfekt für die neuen industriellen Anwendungen. Die Technologie organisiert Lieferketten und ermöglicht nun die kundenspezifische, individuelle Produktion von Kleinserien oder sogar Einzelprodukten. Die Zukunftsaussichten industrieller Anwendungen hängen dabei von Sicherheit in der Kommunikation und vom Austausch der Daten und Identitäten ab. Winzige RFID-Tags ermöglichen diese Szenarien, wobei RFID-Lesegeräte als Augen und Ohren der Lieferkette, der automatisierten Fabrikumgebung und dem späteren Versand und der Verteilung der fertigen Produkte an Kunden dienen.

Herausforderungen

Traditionelle RFID-Systeme bedeuten eine mögliche Schwachstelle in den neuen IIoT-Umgebungen. Ohne weitere Schutzvorkehrungen bleibt die Verbindung zwischen RFID-Etiketten und Lesegeräten ein leichtes Ziel für Klonen, Nachbauten, Snooping-, Replay-, Man-in-the-Middle- oder Denial-of-Service-Angriffe oder andere Versuche, Daten abzugreifen oder zu manipulieren, um unrechtmäßig Informationen zu gewinnen oder dem Unternehmen zu schaden. Bei einer etablierten Technologie, die so allgegenwärtig ist wie RFID, müsste jeder Versuch, diese Lücken zu schließen, innerhalb der vorgegebenen Parameter und innerhalb der begrenzten Möglichkeiten der Technologie funktionieren. Die Ablösung des



gesamten Konzepts scheint eine kommerziell unhaltbare Option zu sein. Die neuen Schutzfunktionen müssen daher nahtlos in die etablierten Standards passen und gleichzeitig so robust und flexibel wie möglich sein.

Lösung

Balluff, einer der führenden Sensorhersteller der Welt, und Wibu-Systems, Experte zu Lizenzierungs- und IT-Sicherheitslösungen, haben ihre Kompetenzen unter der Leitung des führenden Herstellers von Holzverarbeitungsmaschinen Homag im IUNO-Projekt zur IT-Sicherheit in Industrie 4.0 zusammengebracht, um eine Lösung zu finden, die all diese Herausforderungen gleichermaßen löst. Ihre Vision: Ein „OPC UA RFID-Lesegerät mit integriertem Secure Element“, basierend auf Balluffs intelligenter UHF-Lesegeräteplattform und dem CmASIC von Wibu-Systems als der robusten Sicherheitslösung mit Infineons SLE97 Cryptocontroller. Das System nutzt die auf OpenSSL aufbauenden Schutzfunktionen der OPC UA-Implementierung von Unified Automation, um sichere Maschinenkommunikationen auf beiden Seiten zu garantieren: zwischen dem RFID-Lesegerät und dem datenverarbeitenden Computer auf der einen Seite und der digitalisierten Produktionssteuerung auf der anderen Seite.

Sicherheit in der Industrie 4.0

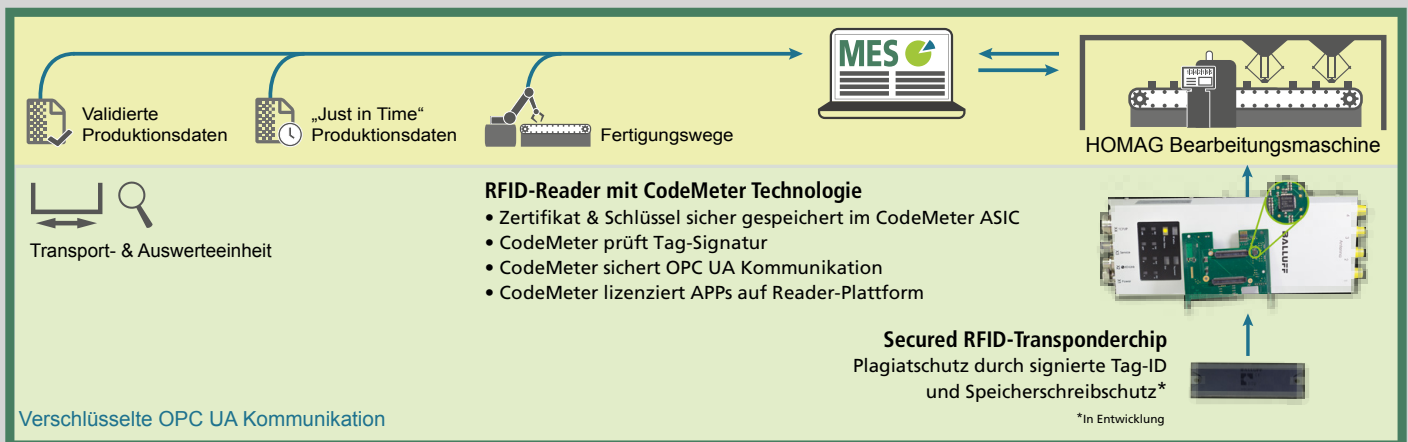
RFID-Lesegerät mit Secure Element:

- Geschützter Schlüssel- und Zertifikatsspeicher
- Sichere RFID-Identitäten
- OPC UA-Kommunikationsstandard
- Besserer Schutz mit CodeMeter

OPC UA Hintergrund

In der Lösung von Wibu-Systems und Balluff zeigen die Schutzfunktionen von OPC UA ihre Flexibilität und ihr Potenzial, um die nötige Sicherheit in der RFID-Kommunikationskette zu erweitern: Mit dem CmASIC als Secure Element können die nötigen kryptographischen Schlüssel sicher aufbewahrt werden und so den starken Schutz, den das OPC UA-Protokoll in der Maschinenkommunikation ermöglicht, voll ausnutzen. Die bisher wenig sichere RFID-Kommunikation wird um drei wesentliche Eigenschaften erweitert: sichere Identitäten für die beteiligten Geräte, Integrität für den Tag-Leseprozess und eine vor Diebstahl und Manipulation geschützte Datenkommunikation. Speziell gesicherte Speicherbereiche sind vorhanden, um neue Software mit umfangreichen Lizenzierungs- und sicheren Updatefunktionen

für RFID-Lesegerät wurden mit der AutoID-Spezifikation des AIM-D e.V. standardisiert. Mit den Entwicklertools und dem Codegenerator von Unified Automation kann das Standardsystem leicht für jede RFID-Lesegerät-Anwendung implementiert werden. Die von Wibu-Systems entworfenen Erweiterungen für OPC UA bringen dabei den Schutz und die Sicherheit des Systems auf den nächsthöheren Schutzlevel. Die auf OpenSSL basierenden Schutzfunktionen von OPC UA sind perfekt in das CmASIC als Secure Element integriert. Als weiterer wichtiger Baustein überwacht CodeMeter den Zugriff auf das Secure Element und die Kommunikation zwischen OpenSSL und dem gesicherten Schlüsselspeicher. Alle diese Komponenten greifen ineinander, um die Kommunikationskette sicher, integer und vertrauenswürdig zu machen.



hinzuzufügen und damit den Funktionsumfang der RFID-Lesegeräte im Feld zu erweitern. Gleichzeitig kann die gesamte Kommunikation von Ende zu Ende verschlüsselt werden, was das bisher schwächste Glied in der Kette – die Funkverbindung zwischen Etikett und Lesegerät – sichert.

Produkte von Unified Automation

Das OPC UA-Kommunikationsprotokoll und Datenmodell wurde wegen der Vielseitigkeit des Unified Automation Software-Development-Kits (SDK) für die Kommunikation zwischen RFID-Lesegerät und Maschinen ausgewählt. Die OPC UA-Funktionen zur Informationsmodellierung sind in den SDKs vollumfänglich verfügbar und für den Anwender leicht einsetzbar. Die semantische Beschreibung und die Daten-, Kommando- und Diagnostikmodelle

Über IUNO

Im IUNO-Projekt, das nationale Referenzprojekt zur IT-Sicherheit in Industrie 4.0, arbeiten Balluff und Wibu-Systems unter der Leitung von Homag zusammen, um die bekannte RFID-Welt mit sicheren Identitäten und abgesicherter Kommunikation zu schützen. Zusammen haben die drei Partner eine praktische Demonstration des neuen Systems als Grundlage für individuelle Produktionsabläufe entworfen – also für eine der wichtigsten Zukunftsperspektiven der Industrie 4.0, die ohne verlässliche Identitäten und sichere Kommunikation in den immer komplexeren und heterogeneren Welten intelligenter Fabriken und vernetzter Industrien unmöglich wäre.

Über Wibu-Systems:

WIBU-SYSTEMS AG, 1989 von Oliver Winzenried und Marcellus Buchheit gegründet und eigentümergeführt, ist Weltmarktführer im Bereich Schutz und Lizenzierung von Software und Dokumenten. Die breite und vielfach ausgezeichnete Palette von Wibu-Systems-Lösungen ist einzigartig und bietet patentierte Lösungen zu Kopier- und Knowhow-Schutz, Lizenzierung und Security, also Manipulationsschutz. Die Anwendungen reichen von Embedded- und Steuerungssystemen über PC-basierte Lösungen bis in die Cloud.

Wibu-Systems®, CodeMeter®, SmartShelter®, SmartBind® und Blurry Box® sind eingetragene Markenzeichen der WIBU-SYSTEMS AG.