



RFID und Sicherheit

Sicherer Einsatz von RFID in der Produktion

Einsatz von RFID

Die Vorteile einer einfachen eindeutigen Identifikation unterschiedlicher Objekte scheinen auf der Hand zu liegen: Die für Entscheidungen notwendigen Informationen „Was ist wann an welchem Ort?“ können mit Hilfe von RFID-Systemen in deutlich feinerer Granularität gewonnen werden und helfen dabei, bestehende Prozesse zu optimieren.

Durch den Einsatz der RFID-Technologie kann jedoch weitaus mehr erreicht werden, als nur dem alt eingesessenen Barcode ein neues Gewand zu geben. Schlagworte wie Fälschungssicherheit, Pulk-Erfassungen oder selbststeuernde Logistik geben einen Einblick in das Spektrum der Möglichkeiten, und es wird schnell klar, dass es mit bestehenden und künftigen RFID-Systemen möglich sein wird, wirklich neuartige Prozesse bereitzustellen.

Ebenso vielschichtig wie das Potential und die aktuellen Möglichkeiten des RFID-Einsatzes gestalten sich jedoch auf der anderen Seite auch die Einstiegsschwellen. Die Kosten von RFID-Transpondern sinken, liegen jedoch noch nicht in jedem Bereich in einem Rahmen, der einen geplanten Einsatz rechtfertigen könnte. Gerade das von vielen Befürwortern inzwischen belächelte Negativbeispiel des Joghurtbechers mit RFID-Transponder zeigt eine unverhältnismäßige Skalierung auf, bei der Nutzen und Kosten – insbesondere unter Berücksichtigung des Wertes des einzelnen zu identifizierenden Objekts – außer Relation geraten. Es bleibt die Frage, in welcher Situation ein solcher Einsatz sinnvoll ist, wenn Paletten oder Ladungsträger schon heute (kosten-)effizient über RFID-Transponder identifiziert werden können.

Im Zuge dieser Fragestellung ist es wichtig, einen weiteren Faktor zu betrachten, der Kosten verursacht: die Sicherheit der eingesetzten RFID-Systeme bzw. die Kosten, die durch mangelnde Sicherheit entstehen können. RFID-Komponenten sind nicht nur immer an IT-Systeme gekoppelt, sie sind in sich IT-Systeme und unterliegen einem eigenen Gefährdungs- und Bedrohungspotential.

Gegenwärtige Situation

Betrachtet man die sich heutzutage im Einsatz befindlichen RFID-Systeme, stellt man fest, dass Funktionssicherheit – im Speziellen Prozesssicherheit – als das wesentliche Sicherheitsziel erachtet wird: Ein Prozess muss unter Verwendung von RFID-Systemen zuverlässig und effizient gesteuert bzw. begleitet werden. Diese Anforderungen werden häufig direkt aus dem Umfeld abgeleitet, in dem eine RFID-Technologie zum Einsatz kommt.

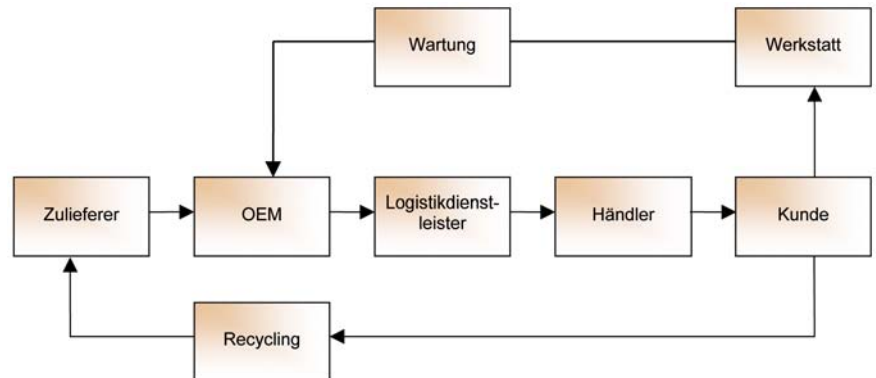


Abb.1 Lieferketten-übergreifender RFID-Einsatz

Gerade im Sektor Produktion und Logistik stehen diese Sicherheitsziele historisch an erster Stelle.

Bei vielen RFID-Installationen in Deutschland handelt es sich um Insellösungen und Prototypen, mit denen der Einsatz von RFID-Transpondern erprobt werden soll [waldmann07]. In diesen abgekoppelten Systemen gibt es kaum Schnittstellen nach außen, die Menge und Güte der verarbeiteten Informationen ist überschaubar, und die Interoperabilität mit anderen RFID-Systemen ist vernachlässigbar. Da zudem viele dieser Anwendungsszenarien dem Einsatz von 1-D oder 2-D Barcodes ähneln, werden auch die entsprechenden Sicherheitsanforderungen daraus abgeleitet. Als Konsequenz treten in der Praxis Datenschutz und Datensicherheit in den Hintergrund.

Mit der zunehmenden Verbreitung der RFID-Technologie ist jedoch die Einführung neuer Funktionalität verbunden. So verfügen moderne RFID-Transponder auch über die Möglichkeit, Daten auf dem Transponder selbst zu speichern. Wo zunächst nur IDs über die Luftschnittstelle ausgetauscht wurden, können nun auch prozesskritische Daten übertragen werden. Gerade in der Automobilindustrie – und in dem eng damit verbundenen Logistik-Sektor – ist eine starke Tendenz zu erkennen, prozessbegleitende Informationen und Produktdaten direkt auf dem Transponder zu speichern, statt in einem korrespondierenden Backend, in dem sie über die IDs referenziert werden [vda5501].

Trends und Konsequenzen

Es zeichnen sich zwei wesentliche Trends beim Einsatz von RFID-Systemen ab. Erstens werden RFID-Systeme immer tiefer in vorhandene ERP- (Enterprise Resource Planning) und Produktionssysteme integriert werden. Ein Beispiel dafür ist eine Ablösung der papiergebundenen Produktionsdokumentation (z. B. Baukarte) durch ein Pendant auf RFID-Basis.

Damit wird auch die Abhängigkeit von RFID-Systemen steigen, was einen gesteigerten Bedarf an Verfügbarkeit und Integrität nach sich zieht. Besonders angreifbar ist dabei die Luftschnittstelle, aber auch die Authentizität der einzelnen Komponenten wie RFID-Transponder und RFID-Reader (oder auch Writer) muss sicher festgestellt und gewährleistet sein. Unbefugt ausgelesene Informationen, eingeschleuste Fehlinformationen, fremde Lese- und Schreibgeräte oder auch unbefugte RFID-Transponder können den Produktionsprozess stören. In speziellen Bereichen müssen RFID-Transponder darüber hinaus an Umgebungsbedingungen wie Temperatur oder mechanische Belastung angepasst sein. Die physische Verbindung zum Objekt spielt dabei eine wesentliche Rolle, da auch die Wahl zwischen einem abtrennbaren oder untrennbaren RFID-Transponder Konsequenzen für den gesamten Prozess oder das Produkt haben kann.

Als Zweites steht das langfristige Ziel des transparenten RFID-Einsatzes über die gesamte Liefer- bzw. Wertschöpfungskette hinweg im Vordergrund. Dabei ist es wünschenswert, dass Güter in der Lieferkette einmal zu Beginn mit einem RFID-Transponder verbunden werden und dieser über die gesamte Lieferkette hinweg eingesetzt wird (Abbildung 1). Für dieses Ziel sind schon heute die besonderen Anforderungen, die sich durch den Einsatz von RFID-Hardware ergeben, vor auszuplanen und beim Einsatz und der Entwicklung von RFID-Hardware zu berücksichtigen. Wird die Schwelle zwischen isolierten Insellösungen und einem lieferketten-übergreifenden Einsatz überschritten, so gewinnen die Sicherheitsziele Datensicherheit und Datenschutz an Bedeutung [eckert04]. Gerade wenn Prozessinformationen für die Partner in einer Lieferkette auf dem RFID-Transponder selbst gespeichert werden, beginnen Daten auf einem physischen Datenträger das Produktionsgelände zu verlassen.

Sichten auf die Daten werden für die einzelnen Partner der Lieferkette notwendig, und eine effiziente Verschlüsselung muss die Daten vor unbefugtem Zugriff schützen. Wie mit jedem System, das einen weit verbreiteten Einsatz findet, erhöht sich auch mit gebräuchlich eingesetzten RFID-Systemen die Wahrscheinlichkeit eines Angriffs auf eine RFID-Infrastruktur. Mögliche Angriffsarten werden in Abbildung 2 aufgezeigt.

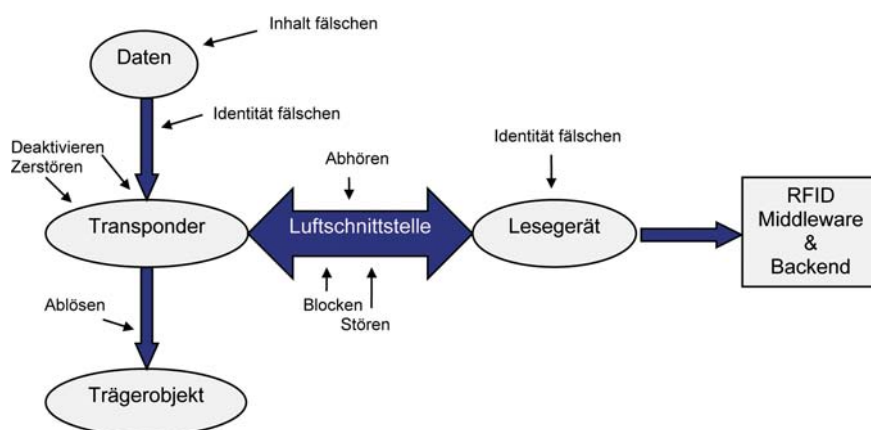


Abb. 2 Angriffsarten (nach [bsi04])

Spezifische Maßnahmen

Um eine vor Abhören gesicherte Übertragung auf der Luftschnittstelle zu gewährleisten, muss ein RFID-Transponder integrierte Kryptographie-Hardware bereitstellen. Je mehr Gatter für die Implementierung dieser Verschlüsselung notwendig sind, desto komplexer wird das Design eines RFID-Transponders, und desto kostenaufwendiger ist die Herstellung. Aus diesem Grund werden zurzeit immer effizientere „leichte“ Verschlüsselungsalgorithmen entwickelt, die die Anforderung an die Sicherheit erfüllen aber weniger Gatter benötigen. Damit die Verfügbarkeit eines RFID-Transponders sichergestellt werden kann, muss er sicher an das Trägerobjekt gebunden werden. Teilweise kann das Ablösen eines RFID-Transponders im Verlauf der Lieferkette gewünscht sein. Andererseits kann ein direkt in das Objekt eingearbeiteter RFID-Transponder bei einem Defekt nur schwierig oder gar nicht ersetzt werden. Es gilt abzuwägen welche Lösungen für einen spezifischen Prozessschritt und welche Lösungen für einen lieferketten-übergreifenden Einsatz notwendig sind. Beide Seiten müssen schließlich miteinander in Einklang gebracht werden.

Die Wahl eines speziellen RFID-Transponder Typs wird auch durch die Oberflächenbeschaffenheit des Objekts beeinflusst. Abhängig vom Material des Trägerobjekts (z. B. Metall) haben sich spezielle Frequenzbereiche für die Übertragung als günstig erwiesen. Die Wahl eines Frequenzbandes beein-

flusst schließlich die Reichweite des RFID-Transponders, die Gefahr von Reflektionen und damit False-Reads (das ungewollte Erfassen von RFID-Transpondern durch Lesegeräte) und so den Aufbau des gesamten Prozesses. Ein angepasster Prozessaufbau kann jedoch auch die Funktionssicherheit durch implizite Qualitätssicherung begünstigen und sollte generell beim Einsatz von RFID bedacht werden.

[bsi04] Bundesamt für Sicherheit in der Informationstechnik – BSI: Risiken und Chancen des Einsatzes von RFID-Systemen, 2004.

[eckert04] C. Eckert: IT-Sicherheit – Konzepte, Verfahren, Protokolle, Oldenbourg Verlag München Wien, 3. Auflage, 2004

[waldmann07] U. Waldmann, T. Hollstein, K. Sohr, Technologieintegrierte Datensicherheit bei RFID-Systemen, Februar 2007

[vda5501] Verband der Automobilindustrie: VDA-5501 RFID im Behältermanagement der Supply-Chain, November 2006

Henk Birkholz

TZI Technologie-Zentrum Informatik
Universität Bremen

Fazit

Um eine sichere RFID-Infrastruktur gewährleisten zu können, müssen frühzeitig die Sicherheitsanforderungen des Einsatzes von RFID-Hardware bei großen Skalierungen berücksichtigt werden. Je höher die Sicherheitsanforderungen an RFID-Transponder (wie z.B. Kryptographie, Schutz vor Umwelteinflüssen, Verbindung zum Objekt), desto höher sind die Kosten für die Transponder und deren Betrieb. Die Kosten werden sich aber schon in naher Zukunft mit wachsender Verbreitung deutlich relativieren. Offene Standards können dabei helfen, die Interoperabilität zwischen den Partnern einer Lieferkette sicherzustellen. Zum Beispiel erhöht ein konsequent eingehaltenes Authentisierungsmodell für alle RFID-Komponenten nicht nur die Datensicherheit, sondern auch die Funktionssicherheit. Möglichkeiten zur Verschlüsselung auf der Luftschnittstelle und auf dem RFID-Transponder selbst stehen schon zur Verfügung, und die Möglichkeiten, RFID-Transponder den Umgebungsbedingungen entsprechend an ein Objekt zu binden, werden immer vielfältiger. So können sanfte Migrationen unter Berücksichtigung der zukünftigen Anforderungen den Einsatz der RFID-Technologie profitabel werden lassen.