



e**BUSINESS**LOTSE

INFOBÜRO FÜR UNTERNEHMEN

SÜDBRANDENBURG



# AutoID TECHNOLOGIEN

W IST GEMEINT?  
 A IST MÖGLICH?  
 S IST DER BESTE WEG?

### **Redaktion**

Sebastian Krautz  
Hochschulring 1  
15745 Wildau  
sebastian.krautz@th-wildau.de  
www.ebusinesslotse-suedbrandenburg.de

### **Autoren:**

Prof. Dr.-Ing. Frank Gillert  
Sebastian Krautz  
Stephan Flatow

### **Bildnachweis**

www.fotolia.de

### **Grafische Konzeption und Gestaltung**

Mare Media  
www.mare-media.de

# IMPRESSUM

### **Herausgeber**

eBusiness-Lotse Südbrandenburg  
TH Wildau [FH]  
Forschungsgruppe Sichere Objektidentität  
Hochschulring 1  
15745 Wildau  
www.ebusinesslotse-suedbrandenburg.de

### **Stand**

März 2015

## **Inhalt**

Einleitung – Was ist AutoID?	4
Wo wird AutoID angewandt?	5
Welche Ziele lassen sich mit AutoID erreichen und wie?	6
Für wen eignet sich der Einsatz von AutoID Technologien?	7
Welche Hard- und Software kommt zum Einsatz?	8
Barcode	8
RFID	8
RTLS	9
Software	10
Welche Rahmenbedingungen gibt es?	11
Zulassungen	11
Standardisierung	11
Datenschutz	12
Was ist bei der Einführung und dem Einsatz von AutoID zu beachten?	13
Welches Vorgehen empfiehlt sich für eine Einführung?	15
Entwicklungen AutoID	17
Wer unterstützt bei Fragestellungen?	18
eBusiness-Lotse Südbrandenburg	20

## Einleitung - Was ist AutoID?

Technologie ist in fast allen Lebensbereichen ein ständiger Begleiter, gerade Tablets und Smartphones haben in den letzten Jahren viele Innovationen durch neue Anwendungsmöglichkeiten in allen Lebensbereichen geschaffen. AutoID ist ein integraler Bestandteil von vielen dieser Anwendungsmöglichkeiten, als Begriff bisher aber zumeist nur Fachleuten bekannt. AutoID steht als Kurzform für „auto-matische Identifikation“ und bezeichnet alle Vorgänge, mit denen Personen oder Gegenstände automatisch und ohne zusätzliche Handlungen identifiziert werden können. Je nach Anwendungszweck können dabei unterschiedliche Verfahren und Arbeitsweisen eingesetzt werden, z.B. Erkennung auf der Basis von akustischen, optischen, mechanischen oder elektromagnetischen Eigenschaften oder Signalen. Die verschiedenen Vertreter der AutoID-Technologien (einige Beispiele finden Sie auf dem Deckblatt dieses Dokuments) lassen sich jeweils unterschiedlichen Wirkweisen zuordnen. Barcodes, welche auf nahezu jedem käuflich erwerbbaaren Produkt aufgebracht und daher weit verbreitet sind, gehören beispielsweise zu den optischen Technologien. Darüber hinaus finden gerade Technologievertreter der Elektromagnetik, wie Radio Frequenz Identifikation (RFID) und Near Field Communication (NFC), durch die nahezu flächendeckende Verfügbarkeit und Anwendung mobiler Geräte und Zukunftsthemen wie dem neuen Personalausweis zunehmende Präsenz in der Öffentlichkeitswahrnehmung und in der täglichen Praxis. Die vorliegende Broschüre soll daher erläutern, welche Möglichkeiten sich aus dem Einsatz unterschiedlicher AutoID-Lösungen für Unternehmen ergeben, was bei ihrem Einsatz zu beachten ist und an welchen Stellen man Informationen und Hilfestellungen erhalten kann.

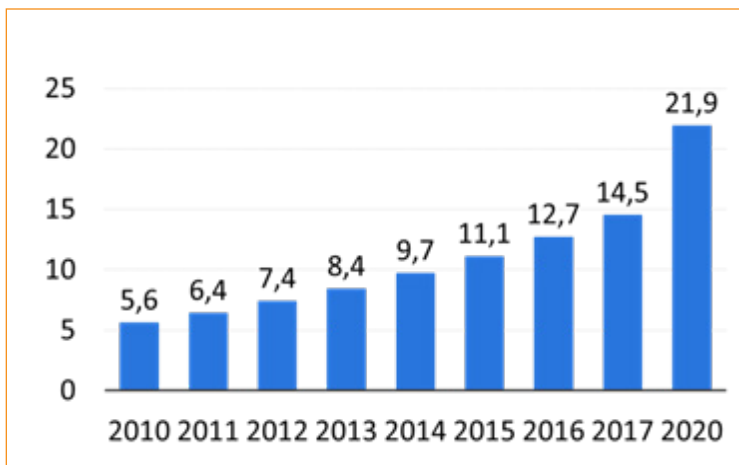


## Wo wird AutoID angewandt?

Die erwähnten Barcodes sind eine der bekanntesten und verbreitetsten AutoID-Anwendungen weltweit und aus der täglichen Praxis kaum wegzudenken. Diese ursprünglich eindimensionalen Codes – mit den bekannten schwarzen und weißen Strichen – gibt es inzwischen auch immer häufiger zweidimensional. Der QR-Code, wie einer der am häufigsten verwendeten Codes heißt, ist insbesondere für die Verwendung durch mobile Endgeräte optimiert. Wie beschrieben werden unter AutoID aber sehr unterschiedliche Technologien zusammengefasst, sodass eine Vielzahl an möglichen Einsatzbereichen und Anwendungsbeispielen entsteht. Neben dem Einsatz in klassischen TUL<sup>1</sup>-Prozessen finden sich moderne AutoID-Systeme, z.B. RFID, heute

- im Krankenhausbereich,
- in Wäschereien,
- im Kundendienst (bspw. für Hotels),
- als Markenschutz,
- zur Warenverfolgung und Diebstahl-schutz im Retail-Geschäft und
- für die Personenidentifikation

wieder. Das Spektrum ist daher groß und die Absatzzahlen der Technologieanbieter nehmen entsprechend zu.



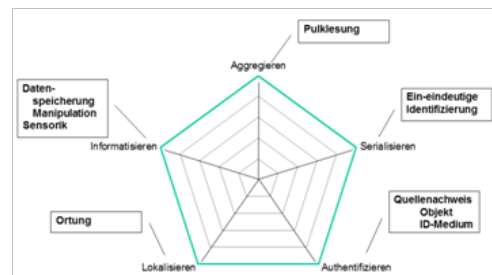
Prognose zum weltweiten Umsatz mit RFID-Transpondern bis zum Jahr 2020 (in Milliarden US-Dollar) ;  
Quelle: Uni Jyväskylä;  
© Statista 2015

Dies wiederum ermöglicht ein moderates Preislevel und bedeutet auch eine stetig verbesserte Systemstabilität: ID-Systeme wie Barcode und RFID sind seit Jahren in der Praxis erprobt und bewährt. Doch für das Unternehmen muss der Einsatz wirtschaftlich bleiben!

## Welche Ziele lassen sich mit AutoID erreichen?

Welche Ziele lassen sich mit AutoID erreichen?

Auf der Grundebene verfügen alle AutoID-Technologien über die notwendigen Funktionen zur Erledigung der Aufgaben Aggregation, Serialisierung, Authentifizierung, Informatisierung und Lokalisierung (siehe Abbildung).



Quelle: eigene Darstellung

Aus den verschiedenen Funktionen ergeben sich unterschiedliche Einsatzbereiche, innerhalb denen spezifische Ziele abgeleitet und verfolgt werden, z.B.:

### Funktionale Ziele

- Zeitersparnis / Aufwandsreduktion (Pulk-Lesung, Lesung ohne Sichtkontakt)
- Vermeidung von unproduktiven Arbeitsschritten
- Optimierung von produktiven Arbeitsschritten
- Eindeutige Identifikation von Subjekten und / oder Objekten
- Steuerung von Materialflüssen

### Qualitative Ziele

- Qualitätsverbesserung (Fehlerreduzierung, Nachverfolgbarkeit)
- Synchronisation von Material- und Informationsfluss
- Steigerung der Sicherheit
- Rückverfolgbarkeit
- Steigerung des Komfort

### Wirtschaftliche Ziele

- Steigerung des Umsatzes
- Steigerung der Produktivität
- Zukunftssichere Aufstellung in der Prozesswelt

Jeder Einsatz einer AutoID-Technologie zur Verfolgung spezifischer Ziele verän-

dert dabei die betroffenen Prozesse selbst: Stellt man beispielsweise auf Scannen per RFID um, so verändert sich der Zähl-/ Identifikationsprozess, da eine Lesung von mehreren Objekten gleichzeitig möglich ist und sich der dafür erforderliche Zeitbedarf verändert. Dieser veränderte Prozess kann wiederum Auswirkungen auf alle anderen Prozesse in der Kette haben, sodass die Einführung von AutoID immer ein gründlich geplanter und durchgeführter Schritt sein muss.

### **Für wen eignet sich der Einsatz von AutoID-Technologien?**

Diese Frage kann nicht pauschal beantwortet werden, da es zu heterogene Anwendungsfelder gibt, die selbst oft einer großen Dynamik unterliegen. Die Anforderungen durch die Umsetzungsziele (z.B. Produktivitätssteigerung) und die Rahmenbedingungen der Prozesse (z.B. besondere Qualitätsanforderungen) müssen dem Potenzial der verschiedenen AutoID-Technologien gegenübergestellt werden, da nicht jede Technologie für jedes Anwendungsfeld gleich gut geeignet ist. Zusätzlich ist jede Technologieeinführung mit Aufwand verbunden: Die Investitionen müssen den zu erwartenden Ersparnissen gegenübergestellt werden, denn der Einsatz von AutoID kann in Einzelfällen auch Mehrkosten verursachen. In diese Kosten- / Nutzenrechnung müssen auch weiche Faktoren einbezogen werden, z.B.:

- Stabilität des Absatzes und damit Reife / Kontinuität der Prozessauslegung
- Entwicklungen in der Versorgungskette und hieraus entstehende neue Anforderungen
- Branchen-/ Produkt-/ Marktcharakteristika  
(Beispiel: Wird ein Chip zur Identifikation in den Produkten geduldet?)

## Welche Hard- und Software kann zum Einsatz kommen?

Im Folgenden werden die gängigsten AutoID-Systeme sowie deren Anbindung beschrieben.

### Barcode

Zu einem Barcode-System gehören der Barcode selbst und ein Lesegerät, welches diesen verarbeiten kann. Ein Barcode kann in verschiedenen Formen vorliegen. Die einfachste Möglichkeit ist, den Code auf Papier aufzudrucken. Darüber hinaus können aber auch Codes direkt auf Objekte gedruckt, gepresst, geätzt oder eingebrannt werden. Zum Auslesen eines solchen Codes werden entweder ein Lesegerät (Entschlüsselung der Daten per Lichtreflexion) oder eine Kamera (Entschlüsselung der Daten mittels zugehöriger Bildverarbeitungssoftware) benötigt.

Lesegeräte sind - abhängig vom konkreten Einsatzzweck und Anwendungsfall - in verschiedenen Formen anzutreffen: Eine sehr bekannte Variante ist das stationäre Lesegerät, wie es z.B. im Kassensbereich von Supermärkten eingesetzt wird. Dem gegenüber steht die Anwendung in der Industrie, da hier Handlesegeräte weit verbreitet sind. Eine besondere Ausprägung sind Tunnelsysteme, bei denen ein Objekt von fast allen Seiten gescannt werden kann und somit nicht extra ausgerichtet werden muss.

Alle Varianten sind in der Regel an ein entsprechendes verarbeitendes System angebunden, während die Anbindung selbst drahtlos (z.B. per Bluetooth) oder kabelgebunden erfolgen kann.

### RFID

RFID-Systeme bestehen aus drei Komponenten: dem Reader (Schreib- / Lesegerät), dem Transponder (Kunstwort aus „Transmitter“ und „Responder“, als eine kombinierte Empfangs- und Sendeeinheit) und der Middleware (ein verarbeitendes IT-System).

Neben der Erfassung und Versendung von Daten dienen Reader der Energieübertragung zu den Transpondern, um die Kommunikation zwischen den beiden Elementen überhaupt erst zu ermöglichen. Sie können in sehr unterschiedlichen Bauformen und Designs, z.B. als Handgerät oder als stationäre Einheit, vorkom-



men.

Ebenfalls in sehr unterschiedlichen Varianten existieren die Transponder (oft einfach „Tag“ genannt), auf denen Informationen gespeichert werden können. Je nach Konstruktion, Speichergröße und Art der Energieversorgung (passiv, semi-aktiv oder aktiv) ergeben sich unterschiedliche mögliche Systemparameter, z.B. ist die Übertragungreichweite bei aktiven Transpondern sehr viel größer als bei passiven.

Zur Verarbeitung der empfangenen Informationen sind die Reader in der Regel an ein verarbeitendes IT-System angeschlossen, wobei die Anbindung über sehr unterschiedliche Schnittstellen (z.B. COM, RJ45, WLAN) erfolgen kann.

RFID-Systeme, sowie die in diesen Systemen eingesetzten Komponenten, unterscheiden sich sehr in Abhängigkeit von den verwendeten Frequenzen. Hierbei werden drei Frequenzen bzw. Frequenzbereiche unterschieden: Niederfrequenz (Low Frequency, LF), Hochfrequenz (High Frequency, HF) und Ultrahochfrequenz (Ultra High Frequency, UHF), welche teils unterschiedliche technische Lösungen verlangen und sich auch in anderen Parametern (z.B. Einführungskosten und Störanfälligkeit) unterscheiden.

## RTLS

Real-Time-Location-Systeme können sich in ihrer Arbeitsweise teils stark voneinander unterscheiden, da die verwendete Hardware sehr vielfältig ist. Eine der bekanntesten RTLS-Anwendungen ist das Global Positioning System, kurz GPS, welches ursprünglich vom US-Militär aufgebaut wurde und heute den weltweiten Standard für Navigationssysteme darstellt. Beim GPS wird die Position über die Auswertung von Satellitensignalen bestimmt, sodass Positionsdaten im Freien bis auf wenige Meter genau, bei speziellen Varianten (z.B. Differential GPS) sogar noch genauer bestimmt werden können. Innerhalb von Gebäuden ist die Anwendung von GPS durch den fehlenden „Sichtkontakt“ zu Satelliten jedoch nicht möglich, weshalb hier andere Systeme zum Einsatz kommen. Weit verbreitete Lösungen sind der Einsatz von Mikrowellenfunksystemen mit einer Frequenz von mehreren GHz und RFID.

## Software

Die reinen technischen Komponenten von AutoID-Lösungen, z.B. Reader und Transponder, erzeugen für sich genommen in der Regel keine direkt verwertbaren Informationen. Sie werden daher mit nachgelagerten Softwarelösungen gekoppelt, welche die erhaltenen Daten in für den Prozess verwertbare Informationen umwandeln. Die verschiedenen AutoID-Lösungen dienen vorrangig der Identifikation, der Scan eines Barcodes z.B. liefert also zunächst nur die in diesem Code hinterlegte Identifikationsnummer. Erst die Verknüpfung dieser Nummer mit weiteren Daten (z.B. Produktdetails oder Prozessanweisungen) durch die Software ermöglicht den tatsächlichen Praxiseinsatz. Je nach Aufbau des Gesamtsystems kann es sich bei der Software um verteilte (z.B. Einzelplatz) oder übergreifende (z.B. Zentralserver) Lösungen handeln. Ebenfalls können die Aufgaben variieren, von der reinen Umwandlung von Daten in Informationen bis hin zu komplexen Verwaltungs- und Verteilungstätigkeiten. Je nach Softwarestruktur kann die Middleware auch direkt mit weiteren Softwaresystemen (z.B. Materialflusssteuerung, ERP-System oder Lagerverwaltungssystem) verbunden werden.

## Welche Rahmenbedingungen gibt es?

### Zulassungen

Der beeinträchtigungsfreie Betrieb eines Funksystems erfordert die Erfüllung verschiedener Kriterien. Hier ist zunächst die Einhaltung der gewählten Funkfrequenz zu nennen. Heutzutage gibt es eine Vielzahl an Funkübertragungen, sodass die Wahl der Frequenz nicht beliebig ist. Stattdessen werden Anwendern in der Regel eine oder mehrere Frequenzen zugeteilt, damit sich unterschiedlich Systeme nicht gegenseitig überlagern und so unbrauchbar werden können. Zusätzlich gibt es bestimmte Frequenzbereiche, in denen unterschiedliche Frequenzen frei genutzt werden können. Ein bekannter Vertreter ist der Frequenzbereich um 2,4 GHz, welcher u.a. von WLAN und Bluetooth genutzt wird. Zu beachten ist, dass Frequenzen und Frequenzbereiche teilweise länderspezifisch sind. So werden für UHF-RFID-Systeme in Deutschland 868 MHz, in den USA 915 MHz genutzt. Eine einheitliche Frequenz besitzt hingegen der HF-Bereich bei RFID, da hier alle Systeme weltweit bei einer Frequenz von 13,56 MHz arbeiten.

Weiterhin ist die Einhaltung von Leistungsgrenzen (Festlegungen zur elektromagnetischen Verträglichkeit) essenziell. Sendeleistungen sind üblicherweise auf wenige Watt begrenzt, z.B. 2 Watt als maximale Sendeleistung für UHF. Bei derart geringen Sendeleistungen ist der Einfluss des RFID-Systems auf Personen vernachlässigbar.

Entsprechende Zulassungen werden durch den Gerätehersteller meist selbst initiiert und von einer dafür autorisierten Prüfstelle erteilt. Der potentielle Anwender sollte Störeinflüsse jedoch vorab prüfen lassen, hierzu mehr im Abschnitt „Investitionssicherheit“.

### Standardisierung

Bei der Vielzahl an möglichen Technologien und Einsatzgebieten sind Standards im Bereich AutoID zwingend erforderlich, da sie die Interoperabilität von Geräten über Herstellergrenzen hinweg sichern. Nutzer sind somit nicht auf einen einzelnen Hersteller festgelegt, sodass sich in der Regel Hardwarekomponenten von verschiedenen Herstellern in einem System kombinieren lassen.

In den AutoID-Standards werden verschiedene Bereiche des Aufbaus und der Verwendung klar definiert. Bei vielen Funksystemen sind so zum Beispiel die Protokolle, die für die Datenübertragung zwischen den einzelnen Komponenten genutzt werden, geregelt. Für optische Systeme (z.B. Barcode) werden in solchen Standards vor allem die Strukturen der Codes festgelegt, u.a. werden also die Kodierung der Daten und Prüfziffern sowie der Wechsel zwischen Strichen und Freiräumen festgelegt. Ein weiterer Aspekt ist die Nutzung der Technologien über Ländergrenzen hinweg. Um dies zu gewährleisten, gibt es neben nationalen (z.B. DIN) auch internationale (z.B. EN, ISO) Standardisierungsorganisationen. Derzeit existieren u.a. folgende Standards:

Standard	Inhalt
ISO 18000-3	Beschreibung der Luftschnittstelle von RFID bei 13,56MHz
ISO 18000-6	Beschreibung der Luftschnittstelle von RFID bei 868MHz
ISO 14443	Beschreibung von RFID Transpondern für den Nahbereich (proximity)
ISO 15693	Beschreibung von RFID Transpondern für mittlere Reichweite (vicinity)
ISO 18092 / 21481	Beschreibung für Near Field Communication (NFC)
ISO 15416 / 15426	Beschreibung für Barcodes

## Datenschutz

Mittels automatischer Identifikation können Daten teilweise ohne die aktive Beteiligung von Personen erhoben und gespeichert werden. Dieser Umstand rückt Fragen des Datenschutzes in den Mittelpunkt, sodass die frühzeitige Sensibilisierung der durch das (neue) AutoID-System betroffenen Personengruppen sehr wichtig ist. Hier sollten dringend Datenschutzbeauftragte und Vertreter der Mitarbeiter in die Planungen mit einbezogen werden, um Transparenz zu schaffen. Selbst bei kleinen Anwendungsgebieten, wie der Einsatz von Zugangsberechtigungen oder der Zeiterfassung mittels RFID, können Mitarbeiter durch die Verknüpfung von Daten über verschiedene Systeme hinweg theoretisch wesentlich umfassender überwacht werden, als durch das einzelne AutoID-System selbst möglich wäre. Entsprechende Implementierungen müssen daher so aufgebaut sein, dass die Verknüpfung der generierten Daten mit Daten aus anderen Quellen nicht möglich ist, indem bspw. Anonymisierung eingesetzt wird oder die System-

grenzen die Datenverknüpfung verhindern.

Auf Grund der besonderen Bedeutung von personenbezogenen oder personenbeziehbaren Daten für die Wahrnehmung und die Praxis der Menschen gibt es auch von öffentlicher Seite Unterstützung für den Datenschutz in AutoID-Systemen. Speziell für den Einsatz von RFID wurden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) sogenannte Technische Richtlinien erarbeitet, die vorgeben, welche Aspekte zur Gewährleistung des Datenschutzes einzuhalten sind. Diese Richtlinien sind seit 2009 Teil eines europäischen Rahmenwerks, der Europäischen Datenschutzfolgeabschätzung (engl. „Privacy Impact Assessment“, PIA). Dieses Rahmenwerk bietet Richtlinien für den datenschutzkonformen Einsatz von RFID-Systemen auf dem Grundsatz von „Privacy by Design“, was so viel bedeutet wie „Datenschutz durch Konzeption“. Damit soll zum Ausdruck gebracht werden, dass nur eine sorgfältige Konzeption unter Einbeziehung aller Betroffenen von vornherein den Datenschutz innerhalb einer Anwendung gewährleisten kann.

## **Was ist bei der Einführung und dem Einsatz von AutoID zu beachten?**

### **Investitionssicherheit**

Ein entscheidender Faktor für die Investitionssicherheit bei AutoID-Systemen ist die uneingeschränkte Funktionsweise innerhalb des eigenen Betriebes. Dieser Umstand wird in der Regel als selbstverständlich vorausgesetzt, ist aber in der Praxis teilweise aufwändig umzusetzen.

AutoID-Systeme stellen verschiedene Anforderungen an die Arbeitsumgebung: Optische Systeme setzen beispielsweise bestimmte Lichtverhältnisse oder Sichtlinien und Winkel voraus, während bei Funksystemen Metalle und ggf. Flüssigkeiten mögliche Störquellen sind. Die konkrete Beschaffenheit der Einsatzumgebung kann sich daher auf die in der Realität erbrachte Leistungsfähigkeit auswirken. Es ist daher wichtig, alle Parameter des Systems und mögliche Einflüsse vorab zu prüfen, da viele der möglichen Einschränkungen der Systemleistung durch entsprechende Planung und Installation in der Regel behoben werden können.

Dazu empfiehlt es sich, Unterstützung bei einer neutralen Kompetenzstelle zu suchen, da so Experten die Machbarkeit und Funktionsparameter genau beurteilen können und die Funktionsweise, und damit die Sicherheit der Investition, von technischer Seite gewährleistet werden kann.

Über die Hardware hinaus ist natürlich auch ein Augenmerk auf die Softwarekomponente zu legen. Besonders wichtig ist hier, dass die Anbindung der AutoID-Software / Middleware an die eigenen Systeme gewährleistet ist.

### Unabhängigkeit / Integrationsfähigkeit

Beim Einsatz von AutoID-Systemen empfiehlt sich stets die Verwendung von standardisierten Komponenten für Hard- und Software. Somit kann die Unabhängigkeit von einzelnen Herstellern und Preisen erreicht werden, ohne dass die Funktionsfähigkeit des Gesamtsystems negativ beeinflusst wird. Darüber hinaus bieten Standardlösungen meist eine Anzahl vordefinierter Schnittstellen, welche die Einbindung in bestehende Prozesse, Anwendungen und hauseigene Lösungen erleichtern.

### Skalierbarkeit

Mit der Zeit können sich der Funktionsumfang, das Anwendungsgebiet und die Leistungsanforderungen an ein AutoID-System ändern. Es sollte daher ein besonderes Augenmerk auf die Skalierbarkeit des Systems gelegt werden, da so z.B. neue Firmenbereiche problemlos in das bestehende System integriert werden können. In diesem Zusammenhang ist ein ganzheitlicher Ansatz wichtig! Dazu gehört z.B. auch die kritische Prüfung von Wartungsverträgen, welche ggf. durch flexible Abrechnungsmodelle ersetzt werden sollten.

### Sicherheit

Wie jedes andere IT-System müssen auch AutoID-Anwendungen mit in die IT-Sicherheit des Unternehmens integriert werden. Dies ist ein enorm wichtiger Faktor, da Angreifern sonst nicht nur eine Möglichkeit geboten wird, Daten zu stehlen, sondern im schlimmsten Fall auch Sabotage. Fragen der IT-Sicherheit müssen daher bereits bei der Planung des neuen AutoID-Systems berücksich-

tigt werden. Ebenso muss die physische Sicherheit gewährleistet werden. Sind Komponenten nicht ausreichend gegen äußere Einflüsse geschützt, können diese von Fehlfunktionen betroffen werden oder ausfallen, was im schlimmsten Fall bis zum Ausfall des gesamten Systems führen kann.

Auch bei sehr guten Sicherheitsvorkehrungen kann ein Systemausfall auftreten, vor allem wenn unvorhersehbare Kaskadeneffekte auftreten. Daher ist hier wie bei allen anderen betrieblichen Prozessen zu definieren, wer was im Notfall zu tun hat. Auch hier können unabhängige Stellen oder die Anbieter selbst aufgrund der Erfahrungen unterstützen.

### Zukunftsfähigkeit

Das Gesamtsystem muss dahingehend soweit wie möglich vorbereitet sein, dass in der Zukunft eine Integration neuer Identifikations-technologien möglich ist und somit sowohl nützliche Hard-, als auch Softwareinnovationen möglichst unterbrechungsfrei den Weg in den Betriebsalltag finden können.

## Welches Vorgehen empfiehlt sich für eine Einführung?

### 1. Fallbeschreibung

Zuerst muss der Anwendungsfall definiert und die Erwartungen gestellt werden. Hierzu gehören auch die Auflistung von erwarteten Vor- und Nachteilen der angestrebten Lösung.

### 2. Prozessanalyse IST

Eine Prozessbeschreibung muss erstellt oder auf Aktualität geprüft werden. Die Unterprozesse sind zu bewerten, um sie später mit dem Soll-Szenario vergleichen zu können. Dieser wichtige Schritt hat absoluten Grundlagencharakter, so dass eine Unterstützung durch (externe) Experten sinnvoll ist.

### 3. Aufstellung von Identifikationspunkten und Machbarkeit

Wo soll das Subjekt / Objekt wie erfasst werden und welche Technologiekompo-

nenten sind dafür nötig? Hierbei ist kritisch zu hinterfragen, wer Information an welcher Stelle wirklich benötigt und wie diese zu erheben sind. Das Ziel muss es hier sein, so wenig wie möglich, so viel wie nötig Technologie einzusetzen. Implementierungsexperten sollten prüfen, ob die Identifikationspunkte technisch sowie organisatorisch machbar sind und keine Störumgebung vorliegt.

#### 4. Prozessdefinition SOLL

Dem Nachweis der generellen Machbarkeit folgt die Ableitung von Soll-Prozessen, welche ggf. bestehende Prozesse mit den neuen Technologien verknüpfen und somit die Blaupause für die neuen Prozesse und Strukturen im Unternehmen legen.

#### 5. Kostenanalyse

Zur Kostenanalyse zählen neben dem Investment für Hardware und IT auch die Planungskosten, laufende Kosten, Instandhaltung, Systemanpassungen sowie Schulungen und mögliche Produktionsausfälle durch Implementierung und Betrieb der Lösung. Diese werden den Prozessersparnissen gegenübergestellt, welche sich als Delta aus dem Ist- und dem Soll-Zustand ergeben.

#### 6. Umsetzung

Je nach Ergebnis der Kostenanalyse herrscht Klarheit darüber, ob das angestrebte Projekt wirtschaftlich tragbar und sinnvoll ist. Je nach Bedarf und Verbesserungspotenzial können einzelne Schritte wiederholt (z.B. Anpassung der angestrebten Identifikationspunkte) und das Projekt so verändert bzw. angepasst werden. Auf diesem iterativen Weg lassen sich viele Projekte in der Realität noch gewinnbringend umsetzen. Dennoch gilt, dass nicht jeder potenzielle Anwendungsfall tatsächlich vom Einsatz von AutoID in der Praxis profitiert. Nach der Entscheidung für die Projektumsetzung sollte die Umsetzungsplanung auf Grundlage der Differenz zwischen Ist-Zustand und Soll-Planung erstellt und die Umsetzung sorgfältig vorgenommen werden.



## Entwicklungen in der AutoID

Zukunft der AutoID ist stark beeinflusst von Themen wie „Industrie 4.0“ und dem „Internet der Dinge“. Das Fraunhofer IML formuliert dazu:

„Industrie 4.0 steht für die intelligente Vernetzung von Produktentwicklung, Produktion, Logistik und Kunden.“

Hiermit wird eine komplette Vernetzung und damit hochautomatisierte Prozesssteuerung als Wettbewerbsvorteil im wirtschaftlichen Umfeld postuliert. Das Einsatzgebiet erweitert sich von der Logistik in Richtung Montageband, aber auch in Richtung Kunde / Nutzer. So ist das Abscannen von Codes aus Ersatzteilkatalogen oder der Kühlschranksinhalte zur Beschaffung derer heute schon möglich. „Im Internet der Dinge werden Objekte intelligent und können über das Internet untereinander Informationen austauschen. Ziel des Internet der Dinge ist es, die virtuelle mit der realen Welt zu vereinen.“

Die Sensorik dringt tiefer in das Alltagsleben, beruflich wie privat. Auf Verbraucher-Bedürfnisse zugeschnittene AutoID-Lösungen als Komponente einer vernetzten Welt sind heute schon in vielen Bereichen in der Entwicklung (Smart Home-Lösungen; autonome Fahrzeuge) und werden die Branche wachsen lassen. Derartige Entwicklungen bieten erhebliche Chancen und Risiken für Unternehmen, eine aktive Beobachtung des Marktes und der Forschung kann sich daher langfristig als wettbewerbsentscheidend zeigen.

## **Ist nun der Einsatz von AutoID etwas für Ihr Unternehmen? - Checkliste**

Die folgende Checkliste kann als Schnellindikator dienen, ob die Einführung von AutoID für Ihr Unternehmen sinnvoll ist.

- Wo ist der Identifikations-/ Erfassungsaufwand besonders hoch und lässt sich dieser durch AutoID signifikant reduzieren?
- War die Identifikation bisher mangelhaft?
- Sind Lösungen bei Konkurrenzunternehmen zu finden, die sich als wirtschaftlich bewiesen haben?
- Wurden AutoID-Prozesse in der vor- oder nachgelagerten Versorgungskette des eigenen Unternehmens eingeführt, welche den eigenen Einsatz von AutoID voraussetzen, um im Markt stabil zu agieren?
- Ist genug finanzieller Spielraum vorhanden, um mögliche Projektrisiken auffangen zu können, bzw. sind Partner verfügbar, mit denen zunächst eine Testumgebung realisiert werden kann?

## **Wer unterstützt bei Fragestellungen?**

Die verschiedenen Fragestellungen zu Machbarkeit, Wirtschaftlichkeit und dem richtigen Einsatz von AutoID machen das Thema für Einsteiger schwer greifbar. Für Unternehmen ergeben sich dadurch häufig Hemmnisse, welche gegen eine Investition in RFID-Technologie sprechen. Abhilfe können hier Institutionen schaffen, die Informationen, Schulungen oder auch praktische Unterstützungen bieten. Eine erste Anlaufstelle für Informationen Vereine und Verbände, die sich bereits seit Jahren mit der Thematik beschäftigen. Zu diesen zählt unter anderem der Industrieverband für Automatische Identifikation, Datenerfassung und Mobile Datenkommunikation (AIM-D). Dieser besteht aus Technologie- und Beratungsunternehmen sowie ausgewiesenen AutoID-Herstellern und -Beratern. Er widmet sich der Entwicklung von weltweiten Standards im Bereich AutoID und der Verbreitung von AutoID-Technologien. Über den AIM-D werden unter ande-

rem richtungsgebene White Paper erstellt oder Schulungen zu speziellen Themen organisiert. Ein weiterer Verband, der in diesem Gebiet Informationen und Handlungsempfehlungen bereitstellt, ist der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM). Dieser befasst sich gleichzeitig auch mit weiteren Themenfeldern von Industrie 4.0.

Neben Verbänden gibt es auch Fachzeitschriften, die über aktuelle Entwicklungen und auch Anwendungen berichten. Vertreter sind hier unter anderem die „RFID im Blick“ sowie die „ident“.

Eine weitere Möglichkeit sind Informationsnetzwerke, wie das eBusiness-Lotsen-Netzwerk. Im Rahmen der eBusiness-Lotsen werden verschiedene Workshops und Informationsmaterialien zu diversen Themen (unter anderem auch AutoID) angeboten.

Als letzte hier vorgestellte Anlaufstelle sind Universitäten und Hochschulen zu nennen, welche sich mit diesem Gebiet beschäftigen. Die Technische Hochschule Wildau [FH] ist dabei ein Vertreter aus Brandenburg. Hier sind Erfahrungen und Kompetenzen im Bereich AutoID aus Forschung und Praxis gebündelt: Die Hochschule betreibt u.a. spezielle Labore, in denen die Grundlagen von AutoID-Technologien allgemein sowie anwendungsspezifisch erforscht und getestet werden können. Dazu gehören ein besonderes AutoID Testcenter und ein Intralogistiklabor, in dem eine vollständige Logistikumgebung abgebildet und mit entsprechenden Industrie-4.0-Technologien ergänzt wurde.

## eBusiness-Lotse Südbrandenburg

Der eBusiness-Lotse Südbrandenburg ist Teil der Förderinitiative „eKompetenz-Netzwerk für Unternehmen“, die im Rahmen des Förderschwerpunkts „Mittelstand-Digital – IKT-Anwendungen in der Wirtschaft“ vom Bundesministerium für Wirtschaft und Technologie (BMWi) gefördert wird.

Mit 38 bundesweit verteilten Kompetenzzentren informiert der eBusiness Lotse kostenlos, neutral und praxisorientiert. Er unterstützt gezielt kleine und mittlere Unternehmen (KMU) sowie das Handwerk bei der Entwicklung und Nutzung moderner Informations- und Kommunikationstechnologien (IKT). Schwerpunktthemen des eBusiness-Lotsen Südbrandenburg sind dabei insbesondere der Online-Handel, das Online-Marketing sowie Anwendungen der AutoID und RFID Technologien.





**eBUSINESSLOTSE**

INFOBÜRO FÜR UNTERNEHMEN

SÜDBRANDENBURG

Fragen? Wir helfen Ihnen weiter!

eBusiness-Lotse Südbrandenburg  
Industrie- und Handelskammer Cottbus  
Goethestraße 1 | 03046 Cottbus

Tel. 0355 365-1551  
Fax. 0355 365-261551  
Mail [info@ebusinesslotse-suedbrandenburg.de](mailto:info@ebusinesslotse-suedbrandenburg.de)

[www.ebusinesslotse-suedbrandenburg.de](http://www.ebusinesslotse-suedbrandenburg.de)