Foundations and Trends® in
Technology, Information and Operations Management
Vol. 4, No. 2 (2010) 105–185

DOI: 10.1561/0200000020

RFID and the Internet of Things: Technology, Applications, and Security Challenges

By Sergei Evdokimov, Benjamin Fabian,
Oliver Günther, Lenka Ivantysynova
and Holger Ziekow

Contents

Foundations and Trends® in
Technology, Information and Operations Management
Vol. 4, No. 2 (2010) 105–185

DOI: 10.1561/0200000020

RFID and the Internet of Things: Technology, Applications, and Security Challenges

Sergei Evdokimov[1], Benjamin Fabian[2], Oliver Günther[3], Lenka Ivantysynova[4] and Holger Ziekow[5]

[1] *gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Friedrich Str. 136, 10117 Berlin, Germany, sergei.evdokimov@gematik.de*
[2] *Institute of Information Systems, Humboldt-Universität zu Berlin, Spandauer Str. 1, 10178 Berlin, Germany, bfabian@wiwi.hu-berlin.de*
[3] *Institute of Information Systems, Humboldt-Universität zu Berlin, Spandauer Str. 1, 10178 Berlin, Germany, guenther@wiwi.hu-berlin.de*
[4] *Universität Potsdam, August-Bebel-Strasse 89, 14482 Potsdam, Germany, ivantysynova@cs.uni-potsdam.de*
[5] *Institute of Information Systems, Humboldt-Universität zu Berlin, Spandauer Str. 1, 10178 Berlin, Germany, ziekow@wiwi.hu-berlin.de*

Abstract

Radio Frequency Identification (RFID) has started to exert a major influence on modern supply chain management. In manufacturing, RFID changes the way objects are tracked on the shop floor and how manufactured goods interact with the production environment. In logistics, RFID is used to track and trace pallets or individual objects on a global scale. In retail, RFID is used to identify objects, retrieve related information, and prevent theft. Sometimes the tags remain attached

to the objects post-sale, thus facilitating additional services. Overall, enterprises have much more detailed information about the objects: the use and produce, their location, their trajectories, and their physical state.

In this survey paper, we show how RFID has transformed the supply chain over the past decade, discussing manufacturing, logistics, and retail and related cost/benefit considerations. We also describe the vision of an "Internet of Things," where each participating object has a digital shadow with related information stored in cyberspace. We conclude with an extensive discussion of related privacy and security risks, including some of our own proposals to mitigate them.

1

Introduction

Radio Frequency Identification (RFID) is likely to join the ranks of those information technologies that are called disruptive. Its adoption by an enterprise and subsequent integration into the local IT infrastructure typically triggers considerable changes to existing architectures and business processes. The cost of the following reengineering tasks may well exceed the cost of the required hardware and software.

On the other hand, RFID and related sensor technologies have the potential to change the way we control business processes in a fundamental manner. RFID allows us to track objects throughout their production and subsequent life cycle, spanning enterprise boundaries as well as spatial and temporal limits. A consequent application of the technology leads to a detailed and accurate digital shadow of the objects and processes being surveyed. Using appropriate aggregation and reporting techniques, this information can be used by decision makers at different layers of the organizational hierarchy. This may lead to considerable operational and strategic benefits. Prototypical installations confirm this positive outlook; some of them already led to impressive productivity gains throughout the various functional areas of an enterprise.

We believe that RFID is likely to have a significant impact on a broad variety of business functions, in particular manufacturing, logistics, and marketing and sales. In this survey paper, we present some insights how the technology can be applied in a variety of industries. We also offer operational and strategic guidelines for organizations to improve their expected return on investment.

By now there are a great number of applications and industries using RFID in an effective manner. We will not be able to cover all of those in this paper and therefore refer the reader to some related work. The growing importance of RFID is reflected by its inclusion into the main categories of e-business as presented by Gupta et al. [55]. A general meta study and framework for RFID-related research issues is presented by Irani et al. [59]. Identification and tracking of people have been covered in [2, 40, 41, 45]. General tracking in operations management is covered by Holmstrom et al. [58], whereas Camdereli and Swaminathan [18] focus on the tracing of inventory. Applications in healthcare have been analyzed in [4, 65, 75, 82, 102, 111]. Ngai et al. [83] give a framework and guidelines for RFID systems implementation. Ferrer et al. [39] study RFID applications in service delivery and operations.

Our own practical insights are based on a number of case studies, focusing on the concrete benefits of RFID technology in manufacturing. All of the companies we surveyed see considerable potential for RFID. RFID is expected to lead to increased automation, especially in data capture, and therefore to a reduction in labor costs. Improved tracking and tracing may lead to a more stable manufacturing process with interruptions in the production process becoming less frequent. This should help to reduce downtimes, to lower error rates, and to cut down on production waste. Tracing faulty parts and processes in the wake of a complaint or an accident is becoming much easier. Given the increasing demands on product liability, this is likely to create major competitive advantages for early adopters. In container management, RFID can optimize the scheduling and help to reduce shrinkage. Using RFID for the uniform labeling of shipments may lead to considerable savings in labor and hardware. RFID on the shop floor will help to cut down theft and allow more sophisticated presentations of the merchandise to the customer.

In order for these positive potentials to come true, it is crucial that RFID does not form a technology island but is tightly integrated into existing IT infrastructures. Enterprise software systems need to be adapted to take advantage of the richness of data becoming available through RFID. Appropriate filtering techniques need to be put into place to make sure that other system components receive the relevant information in the appropriate granularity. Moreover, companies must consider carefully how to distribute storage and processing in the resulting multi-tier IT architecture that ranges from RFID tags and sensors, on the one hand, to data warehouses and business intelligence tools, on the other hand.

During our case studies, we found that most of today's RFID applications focus on issues that are operational and local, i.e., intra-enterprise. In many cases, this is most likely to guarantee a short-term return of the required investment. Use cases where RFID is used as a strategic enabler, on the other hand, are found much less frequently. The same holds for inter-enterprise applications, where supply chain partners cooperate to maximize the positive impact of the new technology. This may be done, for example, by leaving RFID tags on the objects being produced as they move through the supply chain and by integrating the related business processes. Cooperating partners can use the technology to provide fine-grained product traceability and quality assurances across the whole supply chain. This may translate into significant and tangible competitive advantages.

The paper is structured as follows. We first introduce the reader to the relevant hardware and software as well as to standards and architectures. We then present several case studies and use cases how RFID can be used in manufacturing and retail. Here, the focus is on intra-enterprise applications and local benefits. Subsequently, we move further down the supply chain, discussing RFID applications in logistics and the perspectives for an Internet of Things. This is followed by a discussion of cost/benefit analyses of RFID implementations. The paper then discusses possible security and privacy risks of RFID and presents several architecture proposals for a less centralized Internet of Things. We conclude with a summary and outlook.

2

RFID Technology

Radio Frequency Identification (RFID) is a generic term for technologies that use transponders to identify an object. The technology has its origins in the first part of the twentieth century and was initially used to identify military aircrafts as friend or foe. Today, RFID technology has found various applications in security, logistics, and maintenance, to name just a few. In the following, we briefly introduce RFID hardware and middleware technologies for business applications.

2.1 RFID Tags and Readers

RFID hardware includes RFID tags (see Figure 2.1) and RFID readers. RFID readers are devices for reading out RFID tags via radio signals. Different versions of readers exist that are tailored to the targeted application. Examples are mobile readers for manual reads or RFID gates for monitoring items that pass through a door. Figure 2.2 illustrates a typical handheld device that can be used for manual reads.

RFID tags consist of a chip for storage and computation and an antenna for communication. We categorize RFID tags

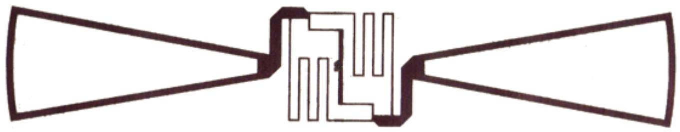

Fig. 2.1 Gen 2 RFID tag.

Fig. 2.2 RFID handheld reader.

Table 2.1. Exemplary tags with their attributes: *energy supply* (battery), *data storage capabilities* (memory and access to memory), and *frequency*.

Tag	Bat.	Data storage Mem.	Data storage Access	Freq.
VOLCANO TAG 231 (Assion Electronic)	No	64 Bit	Read-only	125 kHz
BIS L (Balluff)	No	192 Byte	Read/write	125 kHz
TFM 05 2205.210 (Leuze electronic)	No	44 Byte	Read/write	13.56 MHz
Short Dipole Label (Intermec)	No	96 Bit	Read-only	868 or 915 MHz
AD-220 9 (avery dennison)	No	96 Bit	Read/write	902–928 MHz
Beacon Tag 137001 (Gao RFID Inc.)	Yes	9 Byte	Read-only	868 or 915 MHz

according to their (i) energy supply, (ii) data storage capabilities, and (iii) communication frequency. Finkenzeller [40] gives a detailed description of each of these attributes. Table 2.1 shows some exemplary tags and their corresponding attributes.

Tags without batteries are referred to as passive tags. These tags harvest energy from the communication signal sent by the RFID reader to run their operations. By contrast, active tags use a battery for energy supply.

RFID tags can have diverse storage capabilities starting at a few bits and going up to several megabytes. Furthermore, one can distinguish between read-only and rewritable tags, according to the properties of their memory. In addition, tags vary in their type of construction. That is, they can be built to be reusable, designed for single use, shielded against heat, manufactured for application on certain surfaces, or tailored to other application-specific conditions.

Regarding the communication frequency, RFID tags are usually categorized into low-frequency (LF), high-frequency (HF) or ultra-high-frequency (UHF) transponders. LF tags typically operate on frequencies around 125 kHz and have communication ranges that are commonly below 0.5 m. HF tags operate on the frequency of 13.56 MHz and typically reach communication ranges of 0.5 m to approximately 1 m. Both, LF and HF tags use inductive coupling for communication. By contrast, UHF tags operate using backscattering and reach ranges of up to approximately 7 m. UHF tags operate in a frequency range between 860 and 960 MHz. For more details, see [40].

RFID solutions that use LF have low read ranges that are usually about 0.5 m. The communication with the reader is facilitated via inductive coupling in the near field of the reader antenna. Typical applications for this frequency are access control and animal tracking [21].

RFID solutions based on HF use inductive coupling for communication. Given the wavelength of the HF frequency, the tags' theoretical maximal read range is about 3.5 m. This is because of the limits of the near field. However, typically achieved read ranges are about 0.5–1.0 m. Examples for RFID applications with HF technology can be found, for instance, in logistics or for access control (e.g., in ski lifts).

RFID solutions that use UHF communicate on the basis of backscattering technology. That is, RFID tags and readers are not coupled in an electromagnetic field as in inductive coupling. In UHF-based systems, the tag interacts with the reader by modulating the received signal and radiating it back to the reader. Thus, the range is not limited by the near field of the reader's antenna. Typically, UHF-based applications achieve read ranges of 3–6 m. An important property of UHF is that the achievable read ranges enable bulk reads of pallets. Consequently, the most prominent applications of this frequency can be found in logistics.

The industry association EPCglobal defines four classes of RFID tags along the tags' capabilities [28]. Class-1 RFID tags are passive tags that hold an identification number and optional user memory. The prominent Gen 2 standard for UHF tags falls into this category [29]. This standard is only specified for UHF tags and ratified as the ISO standard 18000-6c [60]. It is commonly used for logistics applications. Class-2 RFID tags provide extensions to the features of Class-1 tags such as extended user memory and authenticated access control. Class-3 RFID tags are semi-passive tags that are equipped with sensors and optionally with functionality for sensor data logging. Class-4 tags are active tags that can be equipped with sensors. Unlike the other tag classes, Class-4 RFID tags can actively initiate communication. They can also directly communicate with other RFID tags, i.e., they can form sensor networks.

Today, a large number of companies offer RFID hardware, specializing in reader technology, RFID tags, or aligned solutions for both. Many known manufacturers in the readers market are small- and medium-sized. This includes companies such as deister electronic GmbH, FEIG ELECTRONIC GmbH, and Nordic ID GmbH. However, large companies such as Siemens offer RFID readers as well.

The market for RFID tags shows similar diversity. A large number of small- and medium-sized companies such as FERROXCUBE, Dynamic Systems GmbH, and many others offer specialized solutions for RFID tags. However, large companies such as Avery Dennison include RFID tags in their product portfolio as well.

Cost for RFID hardware decreased over the past years, due to increased production volumes and technological advancements. Within the past decade, prices for typical reader gates (one reader device and four connected antennas) dropped from about 5000 EUR to less than 2000 EUR per gate. However, the price depends heavily on specifics of the solution. Similarly, cost for RFID tags decreased. For instance, within the past 10 years, the price for Gen 2 inlays (chip plus antenna) dropped below 5 Euro Cent. Today, a total price of 5–10 EUR Cent per label (inlay plus casing) can be achieved for quantities of millions. However, as for readers, the concrete price depends heavily on specifics of the solution.

2.2 RFID Middleware

A range of software systems use RFID technology for data capturing. Examples include software solutions for warehouse management, asset tracking, or supply chain management. Typically, these software solutions do not directly access RFID readers but use RFID middleware as an intermediate layer [11, 42].

RFID middleware is software for integrating RFID data with higher-level applications. Middleware abstracts the access to RFID readers from different vendors and pre-processes RFID data before passing them on the other applications. Commonly, a system architecture with RFID middleware is structured in four layers [11]. We refer to these layers as device layer, edge layer, enrichment layer, and application layer. Figure 2.3 provides an overview.

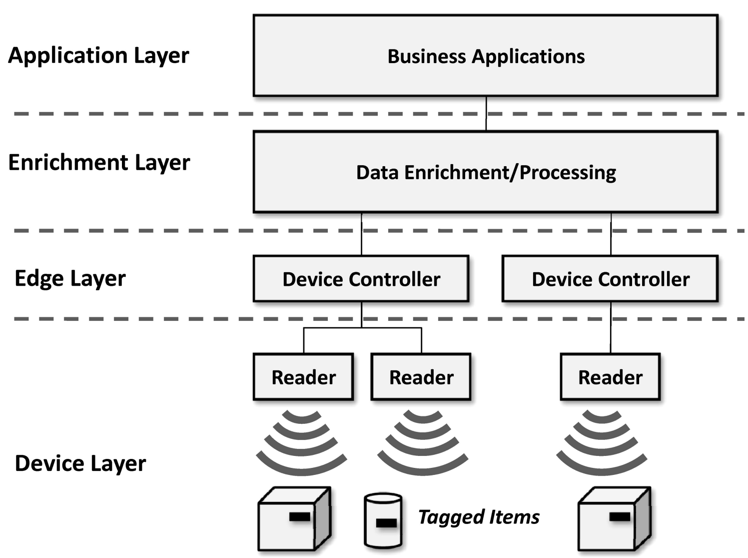

Fig. 2.3 System layers for RFID integration.

The lowest layer — the device layer — includes the RFID hardware with tags and readers. The layer above is the edge layer. It can be considered part of the middleware. This layer holds components for device control and abstraction. Following the terminology of Bornhövd et al. [11], we refer to these components as device controllers. Device controllers can be part of the reader software or run on edge PCs that control the readers. Typical low-level filter logic and aggregation functionalities are implemented in device controllers. That is, the controllers apply filters to cancel out double reads and read errors in the RFID data stream [17]. Furthermore, device controllers can integrate multiple readers. For instance, the controller may suppress redundant reads from several readers in an RFID gate and provide an interface that abstracts the gate to a logical read point [62].

The enrichment layer (called "business process integration layer" in [11]) prepares RFID data from the device controllers for use in higher-level application. Here, a central task is enriching the data with process semantics. For instance, association of read points with the corresponding process steps is done in this layer. Further functionalities such as message buffering and complex event processing may be realized in this layer as well.

On top of the described architecture is the application layer with the applications that use RFID data.

2.3 Numbering Standards and Electronic Product Code

Storing data directly on an RFID tag (*data-on-tag*) requires memory capabilities that constitute a major proportion of the tag price. To keep tag costs low, one may often merely store an identifier and use it as a key to access databases containing the actual object information. This data management paradigm is known as *data-on-network*. The Electronic Product Code (EPC) is the most popular standard for such an identifier approach. The EPC standard [31] represents a numbering framework that is independent of specific hardware features, such as tag generations or specific radio frequencies. This numbering system has the potential to enhance and finally replace traditional barcodes. It aims to assign a globally unique number to nearly every object equipped with an RFID tag. The EPC is serving as an identifier for the physical object carrying the tag, which can now be recognized, identified, and tracked by an IT infrastructure. It can be used as a key to retrieve information from the EPCglobal Network, a widely distributed system of databases [32].

EPCs are potentially the most important coding standard for RFID tags. Through RFID tags, EPCs can be attached or integrated into supply chain pallets and transporting cases, and possibly to all applicable manufactured single goods of the future. Though the EPC standard is actually a meta-framework for several encoding schemes and name spaces, most EPCs have a structure similar to the one shown in Figure 2.4, which depicts an example EPC for one of the most popular standards, the Serialized Global Trade Identication Number (SGTIN).

In this SGTIN-96 variant, the EPC includes a Header to denote its EPC identity type (here: SGTIN-96), a Filter Value for fast logistic decisions, a Partition Value that indicates the boundary of the next two fields, and a Company Prefix (also referred to as EPC Manager) that is a unique identifier of the item manufacturer. Furthermore, manufacturers can assign Item Reference Numbers (also called Object Classes) to classes of objects they produce. Within the same class, similar objects can be distinguished by their Serial Number, this is a fundamental extension compared with the conventional barcode. Standards for further EPC numbering systems besides GTIN-96 are given in [31].

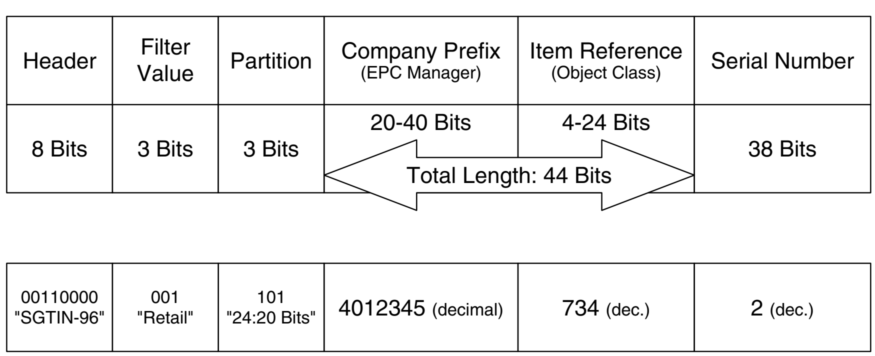

Fig. 2.4 SGTIN-96 EPC.

2.4 Summary

In this section, we provided an overview of RFID technology from various perspectives. We covered (1) RFID hardware, (2) RFID middleware, and (3) RFID-related numbering standards. With regards to hardware, we elaborated on the technological variety of different tags and reader versions along with their physical properties. Concerning middleware, we discussed typical functionalities and architectural properties. Regarding numbering schemes, we provided a detailed discussion about the prominent EPC.

In the following section, we focus on applications of RFID in the manufacturing domain and discuss use cases along with their technical implementation.

3

RFID in Manufacturing

This section shows how manufacturing companies can benefit from Radio Frequency Identification (RFID) technology. Related work on RFID benefits in manufacturing includes [16, 76], and Thiesse and Fleisch [100] focus on real-time RFID location systems in complex manufacturing processes. We present seven diverse RFID-application scenarios. We derived these application scenarios from six case studies, evaluating the introduction or extension of RFID applications in production processes. All RFID scenarios analyzed are either meant as an improvement over an existing barcode implementation or they support scenarios that are not feasible using barcode technology, e.g., due to physical conditions on the plant floor. In this section, we also derive a number of challenges to consider when applying RFID in shop-floor scenarios.

3.1 RFID-application Scenarios

In order to truly examine the potential of RFID in manufacturing, we conducted six case studies at diverse manufacturers. With this qualitative research method, we aimed at acquiring an in-depth understanding of the situation present in the manufacturing domain. As a result, we evaluate RFID potentials that are specific for the manufacturing domain. We specifically choose the case-study approach as a qualitative-empirical method [115]. Case studies have the disadvantage of leading to smaller samples compared with questionnaires. However, the fact of having a much greater depth of analysis often outweighs this disadvantage [43]. In our case studies, we apply an interpretative research approach. In each case study, we analyze the production processes of one specific plant. All case studies are from large- and medium-sized manufacturing companies — mostly automotive suppliers but also companies from the electronics and packaging industries. Their size ranges from several hundred to 18,000 employees. The companies produce airbags (case 1), sliding clutches (case 2), engine-cooling modules (case 3), cast parts (case 4), electronic connectors (case 5), and packaging materials (case 6). For the full case studies, we refer the interested reader to [53].

From our case studies, we have derived the following common RFID-application scenarios. Our findings are in line with [20] and show the practical relevance of RFID in manufacturing.

(1) *Accelerating scan processes*: Manufacturers monitor production processes by scanning barcodes or manually registering objects at certain check points. The registration can often be sped up or automated by using RFID, e.g., by exploiting the ability to read without line of sight. This does not only save labor costs but also increases production throughput.
(2) *Extending scan processes for quality and efficiency*: Manufacturers analyze information about production activities. Thus, they aim to identify causes of quality problems and to point out potentials for improvements. With RFID technology, new scan points can be introduced, in particular, in hostile conditions, allowing extracting more information from the shop floor.
(3) *Extending scan processes for narrowing recalls*: Narrowing the scope of recalls is a concern for many of the plants

investigated. RFID facilitates additional scan points in the production process and helps determining the scope of an error more accurately.

(4) *Reducing paper-based data management*: A common method for recording and maintaining data throughout the production process is by paper documents, which accompany the products. The paper-based data management can be reduced by using RFID tags with writable memory that store data from accompanying documents right with the corresponding object.

(5) *Automating asset tracking*: Accurate tracking of asset location can be crucial for ensuring seamless production processes. RFID technology can facilitate the recording of assets' positions. For instance, assets can be equipped with RFID tags and registered at check points. This can spare costly idle times of machines.

(6) *Reducing back-end interactions*: Some manufacturers demand to reduce the interactions between the back-end system and shop floor software. With RFID, the workload of the back-end system as well as the communication with back-end databases can be reduced (because RFID tags can store up to several megabytes of data). Thereby, RFID facilitates new ways of distributing data and business logic.

(7) *Unifying labels*: Manufacturers face challenges in handling labels for outbound shipments. Different customers typically demand different barcode solutions for labeling transportation units and packages. With RFID, it is possible to abstract from the physical representations of data. Labels could be unified despite differences regarding the information on the label, see Section 2.3.

3.2 Six Case Studies

Table 3.1 shows in which case studies we identified our RFID-application scenarios. The results clearly demonstrate the heterogeneity of application scenarios for RFID in the manufacturing domain. It is

Table 3.1. Identified application scenarios for RFID in manufacturing.

	The seven RFID-application scenarios						
Case study	1	2	3	4	5	6	7
Case 1: Airbags	√	√				√	√
Case 2: Sliding cluthes	√	√	√				
Case 3: Engine cooling module						√	
Case 4: Cast parts		√			√		
Case 5: Connectors	√	√		√			√
Case 6: Packaging materials		√	√	√	√	√	

important to note that RFID-application scenarios go beyond mere barcode replacement. Manufacturers must consider a range of application scenarios to unravel the full potential that RFID technology holds for them. In the following, we shortly describe each case study.

3.2.1 Case 1: Production of Airbags

The company's main motivation to consider RFID is to automate and accelerate manual barcode scan processes by applying a tag to each airbag being produced. Manual scanning accounts for a significant proportion of the employees' work time. The application of RFID would save up to 4 s at each manual scan point. Applied to all production lines, this would amount to approximately 26,000 h of work per year (i.e., 24 s/airbag total saving through the process, times 4 Mio. airbags per year). Yet, only a few cents could be saved per airbag. Since in this scenario RFID tags remain on the product, the tag cost must be weighed against the savings per airbag. Furthermore, the manufacturer could accelerate its production by reducing the back-end interactions during each scan.

Currently, the infrastructure is at its limits for processing plausibility checks in the process control system. A planned expansion in the number of scan points would therefore require additional investments into the server infrastructure. If tags with extended writable memory are used, consistency checks could be processed independently of the back-end system. Here, the cost for additional servers has to be traded against the running costs for RFID tags with sufficient memory as well as the effort for implementing plausibility checks on local terminal PCs.

Further savings may result from avoiding penalties for unreadable barcodes. Currently, the manufacturer pays a few thousand Euros to the customer for each unreadable barcode. Such penalties could be avoided if RFID is applied. Yet, this requires that the customers agree to switch from barcodes to an RFID-based solution.

In addition to these quantifiable effects, the manufacturer may also gain intangible improvements due to RFID adoption. Strategic benefits of RFID may include improvements in customer service, reputation, and inter-organizational collaboration. With RFID tags on the products, the manufacturer enables its clients to benefit from the technology as well, thereby providing an additional service. The company's reputation may be positively affected because of the manufacturer's positioning as an innovative company that quickly adapts new technologies. With regards to inter-organizational collaboration, RFID may strengthen the manufacturer's position as well. Labeling each product with RFID tag readies the manufacturer for RFID-based supply chain management and collaboration. In addition to strategic effects, the manufacturer may encounter other non-quantifiable benefits, e.g., by taking away workload from the back-end system.

3.2.2 Case 2: Production of Sliding Clutches

Here, the manufacturer plans to narrow recalls with the help of RFID technology. RFID would improve the current traceability of sliding clutches by applying tags on carriers during the production process. If a production error is detected today, all sliding clutches potentially affected must be checked manually. For parts that are faulty and already shipped, checks take place at the customers' plants. This results in additional cost for sending engineers to the customers. Costs for recalls are even higher for sliding clutches already used in a customer's production because the manufacturer has to pay penalties in such a case. These penalties add up to about 7.5% of the total revenue. Thus, improving traceability and thereby narrowing recalls can account for significant savings.

The costs for realizing this application scenario with RFID depend on the desired level of tracing granularity. The basic application could be implemented with only one reader gate at the plant floor and reusable tags on the transport units. Yet, the tracing would still be relatively coarse-grained. To achieve tracing on the level of individual operations, additional readers on the plant floor would be needed. Furthermore, the software of the machines would need to be updated as the machines move sliding clutches within and between transportation units. However, once the manufacturer decides to apply RFID technology for expanding traceability, then the technology could also be used for improving other processes in production as well. One example is the warehouse management and a speedup of the processes for loading and unloading shipments.

In addition to these quantifiable aspects of applying RFID, we also have to consider intangible aspects. Here, we would improve the quality of the manufacturer's services due to more precise recalls. Additionally, a more detailed data capturing may enable data analysts to reveal unexpected potentials for production improvements. With regards to interorganizational collaboration, RFID adoption would strengthen the manufacturer's strategic positioning. The planned application would make the manufacturer ready for RFID-based supply chain management and RFID-based information exchange with its partners.

3.2.3 Case 3: Production of Engine-Cooling Modules

This manufacturer applies RFID for storing and communicating routing data on parts in a production line. Thereby, the manufacturer reduces back-end interactions. As the RFID tags are reused, costs for this application scenario are mostly fixed. Thus, the number of RFID tags remains small and tags with extended storage are affordable despite their relatively high costs. In a barcode-based solution, more functionality in the back-end system would be needed. By using the RFID-based solution, investments in the back-end system can be reduced.

In addition to this monetary aspect, the manufacturer may achieve positive intangible effects as well. This is because RFID enables an architecture that can positively impact IT management. Storing data on the tag allows pushing most data management tasks to the production line and reduces the complexity of managing back-end operations. Further intangible benefits are improvements in customer service, in the company's reputation, and in inter-organizational collaboration.

3.2.4 Case 4: Tracking of Cast Parts

This manufacturer needs to keep track of several thousand casts stored in numerous different places. The use of RFID could enable automated tracking and thereby increase tracking accuracy. Quick retrieval of model parts is a challenge, especially when the manufacturer switches from weekly planning to daily planning in the near future. Thus, the manufacturer must trade the cost of an improved tracking system against the higher search effort. To determine the hardware cost, two different scenarios must be considered. In the first scenario, the forms should only be tracked between different production floors and the diverse storage rooms.

For this scenario, about 10 reader gates would be required at waypoints on the transportation routes. Several tens of thousands RFID tags would be needed to label all the model parts. In a second scenario, one uses mobile readers and position tags on the plant floor. Two mobile readers would be sufficient to equip each of the two warehouse workers. Compared with the first scenario, the second scenario needs fewer investments in hardware, although additional RFID tags for marking positions on the plant floor are needed. In addition to being cheaper in terms of hardware cost, the second scenario allows for tracking at a finer granularity. However, evaluating the reader data is more complex in the mobile reader scenario. Thus, more complex and more expensive software would be required. One of the main drivers for RFID was in fact an intangible benefit: the reduced search times would allow the manufacturer to optimize production planning by switching from weekly to daily planning.

3.2.5 Case 5: Production of Electronic Connectors

This manufacturer expects to automate manual bookings using RFID technology. Currently, employees on the plant floor spend about 5%

of their time for copying data from and to accompanying tickets. This time could be saved if the materials used were equipped with RFID tags. Then, the data could be transferred automatically via RFID. If all carriers of materials have tags, false machine settings could be avoided, thereby reducing waste (carriers and material stay together throughout the production process). This would greatly improve process quality.

More importantly, employees also forget to conduct the booking process. Fixing missing bookings can take up to 30 min of employee time. Furthermore, missing bookings can interrupt the production process. With an automated booking process, the time for reconstructing data for missing bookings could be reduced. Additionally, the manufacturer tries to reduce the effort for printing customer-specific labels. This scenario is highly interlinked with other RFID applications. If RFID readers are in place, they could be used to write customer-specific information on tags in the outbound. In this case, expensive, specialized printers for labels would no longer be necessary. This would result in saving hardware cost and increased productivity. In addition to these quantifiable aspects, RFID may lead to intangible gains, in particular, by improving the tracking of production processes.

3.2.6 Case 6: Production of Packaging

The main reason for this manufacturer to investigate in RFID is the decentralization of the IT system. The manufacturer suffered from breakdowns of the back-end system in the past. This resulted in production downtimes lasting several days, causing a loss of revenue and reputation. A fail-over solution for the central database has been discussed; however, decentralized data management via RFID is currently favored by the company's production supervisor. RFID would provide a simple solution for managing production data in an emergency. This would require writable RFID tags with a few kilobytes of memory as well as one reader per workstation.

Additionally, RFID may help to reduce production errors and improve product quality. This could be achieved by automating the data management and thereby avoiding errors in manual data maintenance. The frequency of errors and the related cost determine the potential savings for this application scenario. Furthermore, improvements in the data accuracy may help to better analyze and streamline the processes. Altogether, applying RFID would enable more reliable production planning, ease IT management, improve production reliability, and the manufacturers' reputation. Yet, the monetary effects of these use cases are difficult to estimate.

3.3 Challenges for Shop-Floor Applications

As the case studies show, plant floors are often hostile environments with extreme conditions. Challenging factors include dirt, heat, presence of metal, limited space, and others. In many of the companies studied, products are exposed to extreme conditions, e.g., heat, oil. Special casings or foils can protect RFID tags from external influences. Furthermore, numerous metal objects can be present: transportation units, machines, or the products themselves. The presence of metal can influence communication with RFID tags due to signal attenuation, reflection, detuning, and eddy currents. Moreover, on some plant floors different production steps take place in close physical proximity. In one of the investigated plants, different assembly steps have been conducted within a 1-m distance. Associating an RFID read event with the correct process step may be challenging if several steps are performed within the range of a reader.

RFID solutions for manufacturing must be able to cope with such hostile physical conditions. IT infrastructures supporting RFID need the following functional components: filtering and enriching RFID data, storing RFID data, exchanging RFID data (sharing information along the supply chain), and detecting events in RFID data. They are all generic building blocks that are typically required in RFID infrastructures. This applies to RFID setups in logistics as well as in manufacturing, or in other applications.

Particular requirements of RFID applications on the plant floor cover aspects of integration with other systems, paradigms for data processing, and architectural and functional requirements. In particular, we derived the following six issues for IT systems: distributing business logic and data, supporting heterogeneous data sources, dealing with noise and uncertainty, supporting process analysis, supporting asset tracking, and providing RFID data to overlying software components.

3.4 Conclusion

The case studies show that RFID technology holds many promises for improving manufacturing processes while also exhibiting new challenges. The automation of object identification processes through RFID can help to increase the efficiency by reducing scan times and manual work, reduce errors due to manual data entry and analysis, and improve product tracking and tracing. Detailed data tracks can help increasing product quality and narrowing the extent of necessary product recalls.

In comparison with barcode technology, RFID does not require a line of sight for scanning, enables simultaneous batch scanning, does not require the technological effort for high-quality printing, and is more resistant to physical influences such as dirt or scratches. Avoiding problems related to unreadable barcodes may help to reduce the number returns and penalties and increase customer satisfaction, especially in supply chains operating according to the just-in-sequence paradigm.

Five out of six companies' motives for an RFID adoption are purely operational and intra-enterprise. That is, they would like to use this technology to improve processes and productivity on the plant floor. Motivations to use RFID as a strategic enabler of data exchange between enterprises along the supply chain were found much less frequently.

We explore these issues further in Section 5. Beforehand, however, let us look at the potential of RFID in retail.

4

RFID in Retail

Retail became a well-known application domain for Radio Frequency Identification (RFID) due to frontrunners such as Metro and Wal-Mart. Strong drivers for applying RFID are benefits that stem from improved supply chain management and in-store logistics [101]. Already in 2003, Metro and Wal-Mart started integrating RFID into their value chains. However, RFID also enables use cases specifically for retail stores. In this section, we focus on such use cases and resulting challenges.

4.1 RFID Applications in Retail

Future retail stores will use RFID technology to enhance services and operations directly on the sales floor. The Metro Future Store is an example where these applications are undergoing continuous tests [80]. In this shopping environment, products are tagged with RFID tags. This setup enables applications that retailers can use for improving (1) inventory management, (2) store operations, and (3) customer services.

4.1.1 Improved Inventory Management

RFID tags on products reduce the manual labor involved in inventory taking. For instance, smart shelves can automatically report their contents and workers can quickly take stock with the help of mobile handheld readers. Improvements in the stock taking process allow analysis of the inventory more frequently and with higher accuracy. With more detailed information at hand, store managers can make better decisions about orders and prevent out-of-stock situations [48, 56]. It is possible to detect shrinkage and misplacements [85] earlier and incorporate the information in order management.

Furthermore, improved visibility can yield additional insights into the store operations and help detecting potentials for improvements. Detailed cases are discussed in [78, 98]. The authors describe the use of RFID-based information for evaluation of candidate policies for inventory levels and product presentation. In such cases, RFID acts as a measure instrument to observe the effects of process changes. Taking fine-grained inventory allows a fine-grained analysis of product flows within a store facilities. This in turn enables the evaluation of performance metrics for store processes, improve the store layout, and reason about factors that impact sales quota. For instance, Thiesse et al. illustrate how to analyze the positioning of fitting rooms at a retailer [98].

4.1.2 Improved Store Operations

Using RFID on the sales floor improves checkout operations. Here, RFID can replace barcode technology and significantly accelerate scanning processes or facilitate self-serve checkouts [91]. This does not only reduce waiting times but also provides detailed sales data on an item-level basis. Further scenarios are based on "smart shelves" equipped with RFID readers (see Figure 4.1). This technological setup enables fine-grained monitoring of products on the sales floor and triggering actions that contribute to efficient sales floor operations [77]. For instance, smart shelves can detect when they run low on certain products and automatically call for replenishment. This drastically reduces out-of-shelf situations where products are in stock but not available on the sales floor in the shelf. Furthermore, smart shelves can automatically detect misplaced products and direct a worker to correct the placement. They can also detect when a perishable product is about to reach its date of expiry. It can then initiate measures such as giving

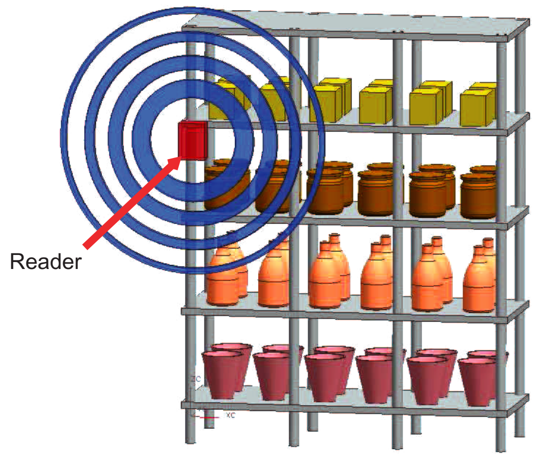

Fig. 4.1 Smart shelves.

discounts on the product or demanding a worker to place the product at a more prominent position in the shelf. If the expiry date has passed, the shelf can trigger an alert to have the product removed, thus preventing it from being sold.

In addition to these operational benefits, smart shelves can enable informational benefits by providing additional insights on shopping behavior. The collected RFID data reveal details such as which products were taken from the shelf and put back later or which products were selected in which order. These insights can help in optimizing product display and operations on the sales floor. An example for such analysis is discussed in [98]. The authors describe how to use information from RFID-equipped fitting rooms and checkouts to observe customer behavior over time. The results allowed to pinpoint situations where customer support appears insufficient and enabled more efficient staff planning.

4.1.3 Improved Customer Services

In addition to improving store operations, RFID technology can be an enabler for new customer-facing services [72], in particular services offered by retailers. These services can target the shopping experience itself or be part of after-sale services. Applications on the sales floor use RFID to provide the consumer with additional product information. Examples include electronic shopping assistants [94] or "smart mirrors" [96]. An electronic shopping assistant can be, for instance, a device that is mounted to a push cart and equipped with an RFID reader. Consumers can use the shopping assistant to get detailed information about products. They can track down the origin of individual food items and thereby get assurance about the quality. The shopping assistant can further use the product information to make suggestions about purchases that go along well with already selected items or help the consumer choose food in accordance to certain diets. Similarly, smart mirrors in changing rooms can recognize the chosen items and make suggestions about fashionable combinations.

After-sale services yield another wide spectrum of possible RFID applications. An often cited example is the smart fridge. Such a fridge uses RFID tags to provide functionalities such as keeping track of the purchased items, warning about expiration dates, and possibly creating shopping lists. Other services are possible in handling warranty issues and returns. The unique identifier on RFID tags can make it unnecessary to provide the original receipt.

4.2 Challenges on the Sales Floor

The examples illustrate that RFID holds the potential for a broad range of applications at retail stores. However, these applications hold various challenges. They fall into the two main categories of (1) technical challenges and (2) concerns regarding consumer privacy.

Technical challenges are often related to automatic data capturing on the sales floor. Some challenges are related to the application of RFID to different product types. Certain products (especially those containing metal and liquids) can pose serious obstacles for automatic read outs. This can limit the feasibility of some sales floor applications to certain product types. Further challenges can arise when multiple readers are operated in close proximity. This is especially the case for smart shelves. Close physical proximity can result in false reads where a shelf captures RFID tags in the adjacent shelf. Furthermore, simultaneously operated readers can distort each other. Addressing these challenges requires an advanced middleware to coordinate reads [93] and to associate reads with the correct shelf [62].

Concerns regarding consumer privacy have sparked fierce discussion in research, media, and politics [54]. The Metro AG received a "Big Brother Award" for its future store initiative, a prize that is awarded by civil rights activists to criticize privacy threats. Benetton was subject to a boycott campaign as response to its RFID project. These examples stress the necessity for retailers to carefully address privacy concerns of consumers. Many demand to automatically deactivate (kill) RFID tags by default at checkout in order to protect privacy. However, this limits after-sale applications.

Privacy issues can also arise before the point of sale, i.e., in applications that track consumer behavior on the sales floor. Retailers must therefore carefully evaluate and address privacy concerns in dependence on the specific application. For a more detailed discussion of privacy issues, see Section 7.

4.3 Conclusion

This section gave a short overview of RFID use cases in retail. So far we focused on operational, intra-enterprise applications a focus that fails to exploit the full potential of RFID technology. In the following section, we turn our focus on inter-company scenarios, as epitomized by the vision of an "Internet of Things."

5

RFID in the Supply Chain — Towards an "Internet of Things"

In the previous sections, we have identified benefits that Radio Frequency Identification (RFID) may provide when used by manufacturers or retailers without any data exchange with other supply chain partners. However, the true potential of RFID is only revealed in open loop scenarios in which stakeholders gather and exchange data as tagged items move along the supply chain. By providing an efficient mechanism for tracking physical objects, RFID can greatly improve the transparency and efficiency of supply chain processes.

Numerous works predict the potential of RFID for increasing supply chain efficiency, including use cases and benefit frameworks for logistics. A literature survey is provided by Sarac et al. [87]. A further literature review and study of empirical evidence of RFID impacts on the performance of supply chains is presented in [106]. Lee [69] discusses benefits of RFID in the supply chain along the dimensions of substitution, scale, and structural effects. A framework for identifying and assessing benefits is given in [8]. Timing strategies of RFID adoption are analyzed by Whang [113], while Cannon et al. [19] discuss perspectives on its benefits and risks.

In [81], Miragliotta et al. present a quantitative model in supply chains for fast moving consumer goods, whereas an economical assessment or RFID for such supply chains on the basis of a questionnaire survey is given in [12]. Analytic models of the benefits of item-level RFID are presented in [49]. Item-level information visibility is analytically analyzed by Zhou [117]. Inventory-record inaccuracy in a supply chain model is discussed by Heese [57]. A simulation-based framework for evaluating the effect of inventory error on the performance of complex distribution systems was developed by Goebel and Günther [51], which allows one for comparing the profitability of RFID for inventory tracking with other managerial measures. Another simulation model to calculate the expected benefits of an integrated RFID system on a three-echelon supply chain is given in [103]. In [88], a further simulation model and adoption-decision framework are presented.

The life cycle of RFID data in supply chains is the focus of [84]. Architectures for information management for supply chain quality management are discussed in [116]. A case study on RFID Data Warehouses is given by Wang et al. [110], while the advantages of sharing such data in the EPCglobal Network (EPCN) are presented in [99] and, based on a case study in the retail industry, in [108]. Supply chain performance metrics and time savings by adopting RFID are presented in [25]. Benefits on the consumer-facing end of the supply chain are the topic of [72], whereas Veronneau and Roy [105] focus on the cruise-ship supply chain, and Swartz et al. [95] focus on medical supply chains.

Cost pressure and transparency demands are main drivers for the adoption of RFID in the supply chain [41]. At the current time, many RFID pilot projects focus on intra-organizational use, that is, optimizing manufacturing processes within one company. However, there are indicators of strategic advantages of item information flow between companies, which could optimize the whole supply network, not only its nodes. The term Internet of Things, as it is established within RFID and supply chain communities today, describes the collective global information service architecture for RFID-tagged items; that is, networked services that speak about things, rather than services that reside inside the objects themselves. This information sharing between companies could be enabled by the EPCN [32, 99, 107, 109].

While an RFID-equipped item travels through a supply chain, at every station — manufacturer, suppliers, shop — the Electronic Product Code (EPC) is read by RFID readers and stored in local databases together with context information — time, location, physical environment conditions, or business process steps [27]. By subsequently retrieving these data, the items path through the chain becomes transparent, inventorying becomes easier, bottlenecks could be identified, and handling processes be optimized. Currently, RFID tagging is mostly used at the container and pallet level; however, in part due to massive investments of major companies, future tagging of most consumer items is to be expected.

In this section, we consider scenarios in which RFID technology is used to facilitate data exchange between different stakeholders. The term stakeholders may refer to both companies (suppliers, retailers) and individuals (in particular customers). We describe the IT architecture that can provide a standardized way to exchange such data, examine the benefits of such architecture, and discuss possible challenges.

5.1 The EPCglobal Network

EPCglobal, originating from the Auto-ID labs of MIT, the former EAN International and Uniform Code Council (both now GS1), is a consortium that places its focus on developing and establishing global standards for RFID, EPC, and the EPCN. In their view, information about an object should in general not be stored on its RFID tag itself, but instead be supplied by distributed servers on the Internet. By using name services such as the Object Naming Service (ONS) or EPC Discovery Services, it will be possible to locate EPC Information Services (EPCIS), which are remotely accessible data collections about the particular object.

The main components, i.e., functional roles, services, and interfaces, in the EPCN are depicted in Figure 5.1 [32].

Users of the EPCN are called EPCglobal Subscribers. They capture EPCs and data from RFID tags on objects they receive via standardized Tag Air Interfaces by using their RFID reader infrastructure. The data and EPCs are passed to the internal Intranet and EPC

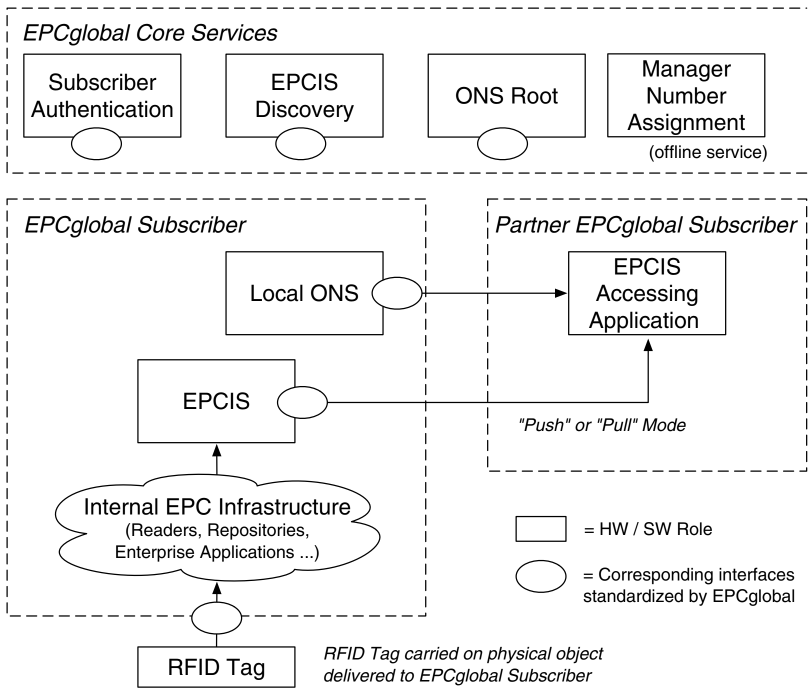

Fig. 5.1 EPCglobal Network — Roles and services [32].

infrastructure, which besides RFID readers includes higher layer collection and aggregation software, repositories, and enterprise applications. This EPC infrastructure can itself offer and query EPCIS, both locally and remotely to partner EPCglobal Subscribers, enabling the exchange of object and event data.

In order to locate dynamically registered EPCIS globally, a static list or a single server would lead to out-of-date information and scalability problems. The EPCN therefore includes central name or look-up services called EPCIS Discovery Services and ONS. Each time someone requests information about a particular object — information not already present in local caches, or "stale," that is, marked as out of date — these services are queried for a recent list of relevant EPCIS. After retrieving this list, the requestor directly contacts the EPCIS in which she is interested. While Discovery Services are still in the development phase (see [34] for a current overview on designs), the

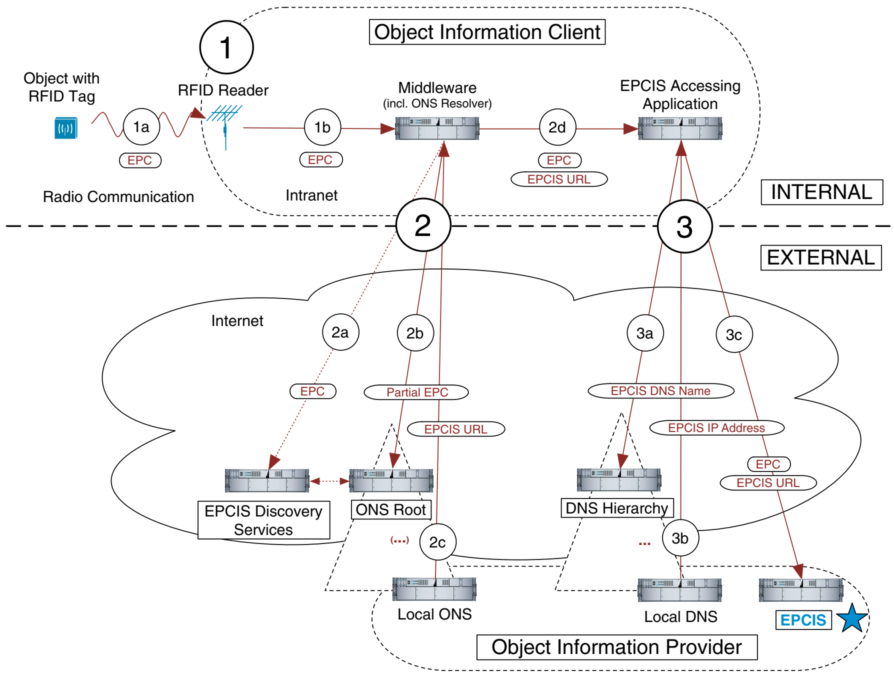

Fig. 5.2 Communication flow in the EPCglobal Network [37].

ONS standard has been published and ratified [30]. According to the standard, the ONS is organized as a distributed hierarchical database, very much resembling the architecture of the Domain Naming Services (DNS). The ONS hierarchy has two levels: On the top level resides the ONS root, the second level consists of local ONS servers.

In the EPCN, retrieval of information about an object that is identified by an EPC number generally involves three main phases (Figure 5.2):

(1) *RFID Tag-to-Reader and Intranet Communication*: An RFID reader reads an EPC from an RFID tag via wireless communication (1a). This EPC is transmitted to a middleware layer for further processing (1b).
(2) *EPCIS Discovery and ONS*: This phase will involve EPCIS Discovery Services that are not specified yet (2a). The middleware uses the EPC number to query the ONS for

Uniform Resource Locators (URLs) of corresponding information sources (mostly EPCIS) (2b). The final answer (2c) from the Local ONS of an information provider is handed over to the application (2d).

(3) *EPCIS Access*: The application needs to resolve the EPCIS DNS names (3a, b) delivered by ONS, and finally contacts the relevant EPCIS directly to retrieve the object information (3c). This procedure will in most cases not be conducted manually, but in an automated fashion, e.g., by the use of Web services.

One of the advantages the EPCN promises is to let many parties — manufacturers, suppliers, shops, or after-sale service providers — dynamically register any kind of EPCIS for the objects they are concerned with, thereby creating an open way to exchange product-related information. By improving the information flow, as objects pass from suppliers to manufacturers, distributors, retail stores, and customers, the EPCN aims to facilitate cooperation within supply chains and thus to make them more efficient.

EPCglobal itself offers Core Services, such as the offline Manager Number Assignment for assigning and managing the EPC Manager part of EPCs, and online Subscriber Authentication, and EPCIS Discovery. In addition, EPCglobal is responsible for the ONS Root, whose practical operation has been outsourced to the company VeriSign.

5.2 Challenges of the EPCglobal Network

The main task of the EPCN is to provide supply chain stakeholders with a standardized way for exchanging high volumes of data that describe status and movement of products and their components. Above we described how it can increase the transparency of logistic processes and extend planning and optimization capabilities, thus, allowing for significant improvements in the supply chain efficiency. However, while providing numerous benefits, the EPCN also poses several challenges, which we examine below.

5.2.1 Normative Issues: Who has the Right to Access which Data?

First off, it is not always clear who should have access to what kind of data at what time, even if all related security challenges (discussed in Section 7) could be solved. If one buys a steak, for example, does one also acquire the right to know its producer? Maybe even the animal it came from? If one buys a shirt, should that enable the buyer to find out who sawed it? Or where the cotton came from? *Vice versa*, should producers be able to know who exactly owns their products? And what they do with the merchandise? — These are questions that different societies and cultures will answer differently and it will represent a major challenge to accommodate the different preferences and legislations in what will doubtlessly be a global information system.

5.2.2 Misalignment of Costs and Benefits

Section 6 presents a detailed discussion about costs and benefits of RFID. Here we focus on one particular issue that is relevant to the EPCN and presents a serious challenge towards its proliferation. Namely, the EPCN architecture and the structure of membership fees introduce a misbalance between its costs and benefits. Stakeholders that are required to make high investments in the EPCN infrastructure do not necessarily enjoy high benefits from using it (and vice versa). Manufacturing, in particular, is the area that benefits least from the participation in the EPCN. On the other hand, manufacturers usually have to carry the costs for RFID tags, maintenance of EPCIS, and EPCglobal fees. Additionally, while manufacturers and logistics service providers prefer to track the flow of cases or pallets, retailers typically aim at tracking individual items [47]. Such misalignment of incentives makes their participation in the EPCN not very attractive.

In scenarios where a manufacturer is using RFID in its production processes, the costs of RFID tags do not play significant role anymore. Maintenance of the EPCIS can be provided by those stakeholders that benefit most from their use. Those stakeholders could also take over the

EPCglobal fees. However, in cases of large OEMs or large distributors that receive products from hundreds of suppliers, this may result in significant costs.

5.2.3 Organizational Power Structures

The ONS, one of the core services of the EPCN, serves to identify those EPCIS that correspond to a given EPC identifier. It is implemented as a hierarchically organized distributed database with its root hosted by VeriSign, a US-based company also hosting several DNS roots and providing a variety of security and telecom services (Figure 5.3). Such unipolarity of control became a source of political controversy, with opponents pointing out that being an international structure, the EPCN should not have its key components being dependent on legislation of a single country [33].

In addition, the need to rely on such centrally managed services may result in lock-in situations in which participants of EPCN will become dependent of business strategies of EPCglobal and its partners. As one of the consequences, GS1 France is currently deploying a European ONS Root hosted by the French telecom company Orange [1]. As no agreement describing the interoperability of the ONS nodes between GS1 France and EPCglobal has been concluded, GS1 initiated a work group to develop a new ONS architecture supporting multiple independent roots.

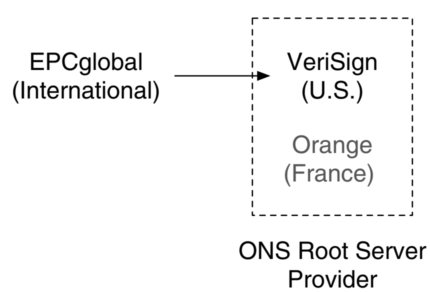

Fig. 5.3 ONS power structure.

5.3 Conclusion

In this section, we presented the application of RFID in supply chains and the corresponding global information infrastructure, the EPCN. Further, we gave an overview on some of the major challenges involved. The privacy and security challenges of this infrastructure will be discussed in detail in Section 7: *Security and Privacy*. In the following section, we focus on cost/benefit issues concerning such complex business infrastructures.

6

Cost and Benefit Analysis

This section addresses the assessment of cost and benefits of Radio Frequency Identification (RFID) applications. We review research that has already been conducted in this field. The majority of works focus mainly on logistic applications, which we shortly describe. We then go into detail about what factors are to consider regarding assessing cost and benefits of RFID with a focus on manufacturing, because there exist very few literature on this topic. We discuss quantifiable costs and benefits resulting from the seven typical RFID-application scenarios evaluated in Section 3. We also describe non-quantifiable aspects of an RFID investment and address the question of how to combine tangible and intangible costs and benefits.

6.1 RFID-specific Methods

Dimensions of the value proposition of RFID are discussed in [26], whereas Whitaker et al. [114] and Tzeng et al. [102] present frameworks for RFID value and benefits. During the past years, some RFID-specific cost and benefit evaluation methods have been developed in order to close the so-called “credibility gap” of the value of RFID [70].

One recent stream of research addresses the issues of imprecise and uncertain information by applying fuzzy logic to solve the underlying investment decision problems. In [13], the authors, for example, propose a fuzzy analytic hierarchy process with a hierarchy of four main criteria: scientific and technological merit, potential benefits, project execution a project risk, and 11 sub-criteria. However, AHP-based approaches are impractical if a large number of decision criteria need to be covered, as usually is the case, e.g., in the manufacturing domain. A second approach by Ustundag and Tanyas [104] focuses on fuzzy cognitive maps to model causal relationships in a non-hierarchical manner for an RFID investment evaluation. The whole approach is for applications in distribution logistics.

However, in order to apply Ustundag and Tanyas' [104] method, relationships between causes and effects and their impact on costs and benefits have to be clearly known, which is not always the case beforehand. Additionally, fuzzy-logic approaches like the ones discussed here include complex mathematical computations and therefore do not meet simplicity and clarity criteria. Although being very valuable for specialists, they are not ideally suited for applications in small- and medium-sized enterprises where the management often has little decision-modeling experience.

The same needs to be said about proposals to apply option models from financial theory [23] to IT and RFID investment decisions [24, 79]. In order to be applicable to a wide range of companies, less sophisticated approaches are needed, such as value benefit analyses (VBAs), as discussed by Tellkamp [97].

Other methods take a more fine-granular approach and focus on the effect that RFID has on atomic activities. In [68], Laubacher et al., for example, conduct an activity-based performance measurement. GS1 [52] shows the impact of RFID on logistic processes with an Excel-based calculation tool for cost–benefit analysis of RFID roll-outs in supply chains. The tool takes various steps in the supply chain into account and calculates the payback period of the investment. The steps considered range from the packaging supplier to the point of sale. Ustundag [103], Veronneau and Roy [105], and Smart et al. [90] investigate RFID adoption costs in supply networks.

The Auto-ID Center developed a web-based tool for estimating the impact of RFID [97]. However, only the Electronic Product Code Value Model [71] focuses more on the role of manufacturers. The tool uses a cause-and-effect analysis to assess the impact of RFID on various business goals. Unlike our work, this MS EXCEL-based tool targets mainly benefits in the manufacturers supply chain rather than on the shop floor. In several survey sheets, it captures basic business information about the company, information on the implementation cost, and information about the impact of RFID on expected improvements. A summary sheet presents the overall results of the cost and benefit calculations.

Still, all these methods strongly focus on financial issues, omitting to a large extent the unquantifiable benefits and risks that RFID may have. In the remainder of this section, we provide some guidance for assessing both the quantifiable and the non-quantifiable aspects of RFID rollouts in manufacturing. We explicitly address the main obstacle that leads to decisions against RFID — the inability to foresee concrete benefits [89].

As we will discuss later, the taxonomy along the terms quantifiable *versus* non-quantifiable is independent of the taxonomy classifying certain measures into being operational *versus* strategic. Figure 6.1 gives examples of all four possible cases. The boundaries between operational and strategic are somewhat fuzzy, as are the boundaries between quantifiable and non-quantifiable. Especially the latter classification should not be seen as a discrete differentiation but as a spectrum.

6.2 Quantifiable Costs and Benefits

The implementation of RFID has a lot in common with any generic IT project: the IT project's costs for integration, support, training, and maintenance are much higher than the actual purchase price of the required hardware and software. Therefore, the costs should be calculated with a Total Cost of Ownership (TCO) analysis. A complete TCO analysis spans over a specific period of time (such as 5 years) and includes expectation values for all costs to be encountered by the company in question. Therefore, a TCO analysis cannot be done at a

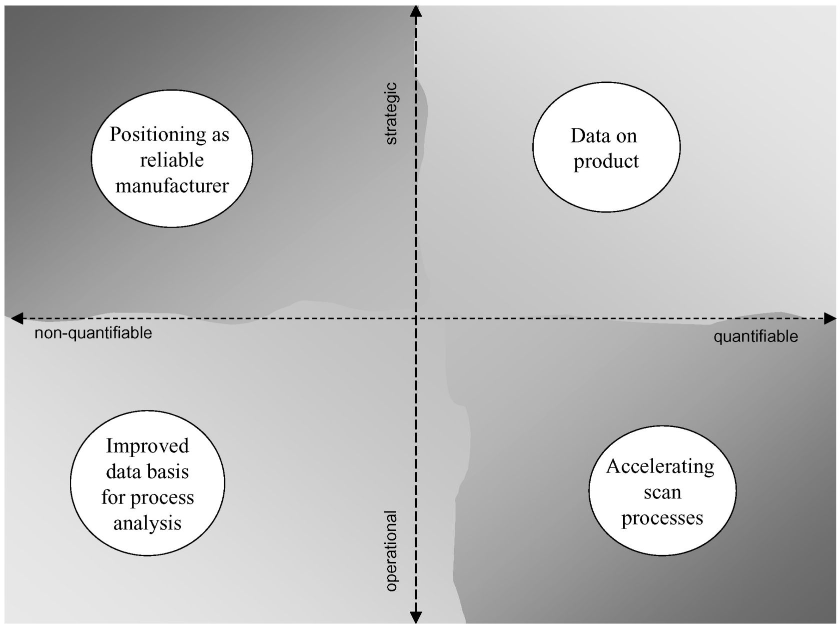

Fig. 6.1 Aspects of an RFID rollout in manufacturing.

general level, it has to be case-specific. In this section, we restrict the discussion to general aspects. We first discuss quantifiable costs and benefits of RFID investments.

6.2.1 Fixed Costs

Some fixed costs are common to practically all RFID applications. These are costs for software (including middleware), hardware (including, e.g., readers, network components, reusable RFID tags, and terminal computers), training of staff, maintenance, and system integration costs. Note that part of the fixed cost is up-front, e.g., costs for RFID readers. Assuming constant equipment utilization over time, another part of the fixed costs is uniformly distributed over the application lifetime. These are, in particular, maintenance costs. If RFID is used as a replacement for an existing barcode solution, the fixed costs need to include write-offs for any existing solution, which is prematurely phased out.

6.2.2 Variable Costs

Variable costs are uniformly distributed over the application lifetime. For variable cost, we have to distinguish between closed-loop and open-loop scenarios. In closed-loop applications, RFID tags do not remain on the product post-sale. They may be recycled and reused in future production cycles. In closed-loop applications, the number of labeled items per time unit and the cost for applying and later recycling RFID tags determine the variable cost.

In open-loop applications, the RFID tags are used throughout several phases of the supply chain and subsequently discarded or left with the customer. In such scenarios, we consider the costs per non-reusable RFID tag attached to an item. Note that discounts due to cost-sharing models or discounts for high quantities are possible. Cost-sharing models are typical of complex supply chains where RFID tags are used by several supply chain partners at once, which then share the related expenses.

In many use cases, RFID tags could be applied to transportation units that cycle on the plant floor (e.g., material carriers). In such cases, tags are applied only once. However, the data written on the tag (or associated with the tag) must be changed in each cycle. Depending on the particular setup, this task may require manual intervention which results in variable labor costs. Removing tags accounts for additional labor costs. However, no removal is necessary if tags cycle on transportation units on the plant floor. Additional cost can occur for transporting reusable RFID tags between the points of application and removal. Tags may just be transported within the plant floor in applications that are restricted to one plant. Yet, advanced RFID applications may span several production steps in the supply chain and tags may need to be transported between different plants.

6.2.3 Benefits

Accelerating scan processes: One reason for applying RFID is to accelerate or to completely automate the scanning of identifiers. This allows reducing labor costs. Resulting total benefits can be quantified via the RFID-enabled time savings and the relevant labor cost. In total, the saved time is the product of the expected application lifetime, the number of identifiers scanned per hour, and the RFID-enabled time saving per scan.

Extending scan processes for narrowing recalls: The monetary benefits can be estimated, for instance, when RFID reduces the batch size for tracking. The expected application lifetime, the error frequency, and the reduction of the batch sizes determine how many items can be spared in a recall. Together with the cost for recalling an item, this yields the monetary benefits for narrowing recalls.

Reducing paper-based data management: As described above, improving data maintenance by RFID may reduce costs that result from errors in collected production data. This is because RFID can help to automate data maintenance in some applications and thereby reduce the impact of human mistakes. Related errors may include wrongly configured machines that may produce waste, forgotten bookings of finished steps that may delay production, or manual data entries that can be error prone. Preventing these errors also avoids resulting expenses due to penalties or production errors. Furthermore, RFID may accelerate or automate data maintenance tasks, thus saving labor costs.

Automating asset tracking: Having the right assets available at the right time is crucial for seamless operations of a production plant. The expected RFID-enabled benefits can be quantified as the product of the expected application lifetime, the frequency that assets are missing, and the related costs per missing asset. Cost per missing item can be derived from penalties due to production delays or opportunity costs resulting from production downtimes.

Reducing back-end interactions: RFID allows storing data with the corresponding object rather than in back-end databases. Applications that work on data from RFID tags are less vulnerable to system failures than centralized solutions (no single point of failure). Using data from RFID tags, the production can continue in the case of a back-end failure at least temporarily. The monetary value of this effect stems from the reduction of production downtimes and resulting expenses for penalties and opportunity costs. For quantifying the savings, one must consider the application lifetime, the expected improvement regarding system failures downtimes, and the cost per downtime.

Unifying labels: The main cost driver when printing labels concerns specialized multi-format printers. Another cost factor that is related to label handling concerns the penalties for labels that cannot be read by the customers. To quantify the savings, one must factor in the application lifetime, the improvement regarding unreadable labels, and the saved costs for managing print labels on the plant floor.

6.3 Non-Quantifiable Costs and Benefits

6.3.1 Operational Benefits

The case studies show that operational benefits are the main driver in most RFID projects. They provide short-term positive returns on investment, which should convince every controller. However, some RFID applications can leverage additional intangible benefits on top, which may tip the scale in favor of adoption, even though the short-term ROI may be negative. We have observed the potential for such effects regarding improved production planning, process optimization, and IT management.

Production planning requires accurate information on the availability of resources. RFID enables better control of assets and materials through its tracking functionality, thus reducing loss and search times. The direct effect of this is easy to quantify. However, these applications open up new opportunities by enabling the introduction of more flexible planning methods, such as switching to shorter planning periods. The same applies to RFID-enhanced methods for material tracking and inventory management. In combination with these methods, RFID can reduce uncertainty in planning. However, the resulting benefits are rarely quantifiable beforehand.

Process optimization is often a driver for RFID introduction, e.g., manufacturers exploit properties of RFID (such as reads without line of sight) to increase process automation and speed up manual scanning tasks. This kind of process optimization does not necessarily lead to intangible benefits. However, RFID can also facilitate more detailed data capturing. This enhanced business intelligence might enable data analysts to get more insight into the processes and potentially reveal unexpected potentials for improvements.

IT management in a plant is certainly affected by RFID introduction. Introducing RFID components into an existing IT landscape allows for a novel distribution of data and logic and for new means of data exchange. For instance, RFID-based architectures improve the autonomy of system components. Supply chains can use the memory on RFID tags to store routing data and to log production data right at the product. This enables system components on the plant floor to operate autonomously. Production stations can operate directly using data from RFID tags and become independent from back-end systems and network connections. Furthermore, RFID can help encapsulating data management tasks and support a system's scalability. As a result, RFID may improve the robustness and availability of the supply chain as a whole. However, the degree of improvement is often unknown before an actual implementation takes place, thus making this benefit very hard to quantify *ex ante*.

6.3.2 Strategic Benefits

The decision whether or not a company should adopt RFID has an impact beyond the operations on the plant floor. Depending on the specific industry, RFID may be a distinctive factor in a company's strategy. Strategic potentials of RFID may concern improving quality and customers' service, increasing reputation, and improving inter-organizational collaboration.

Improving quality and customer service are important strategic means to gain an advantage over one's competitors. The introduction of RFID possibly affects the quality and the range of customer services that a manufacturer can provide to its clients. As a side effect of operational improvements, better control of plant floor processes can improve the quality of a manufacturer's output. For instance, RFID-based process monitoring could enhance the detection and correction of production errors before products are shipped.

Moreover, RFID can improve production quality by helping to ensure that shipments are complete, consistently documented, and that all products passed through the production process correctly. As an additional service, the supply chain participants may share the captured RFID data among each other. This could streamline operations and leverage benefits (e.g., by better planning due to updates on the production status). Another potential for additional services is to leave RFID tags on the shipped products through the entire supply chain. Supply chain participants could thus benefit from RFID at their material intake. Manufacturers may also store production data on the RFID tags. This service could help clients routing products through their production and facilitate consistency checks on the plant floor.

Increasing reputation is another strategic benefit that RFID can contribute to. A company's reputation can profit from new technology advancements — such as RFID — because the company is perceived as innovative by its business partners. Additionally, RFID enables narrowing and avoiding recalls for some products, thus limiting adverse reputation effects associated with production problems.

Improving inter-organizational collaboration can leverage optimization across value chains and strengthen the position of partner networks. Depending on the market structure, good positioning in such a partner network is a crucial strategic issue. RFID is more and more developing into a technology for inter-organizational collaboration. Collaboration infrastructures — such as the EPCN — are increasingly based on RFID technology. An RFID rollout provides the strategic option to opt into RFID-based collaboration networks and become part of RFID-enabled value chains. Examples from the retail industry show that dominant players in a value chain may even try to force their suppliers into RFID adoption — with mixed success. Thus, getting ready for RFID is of strategic importance for many companies.

6.3.3 Risks and Costs

Any IT project bears intangible risks with associated costs that decision makers must weigh against expected benefits. In the following, we discuss specific intangible risks that are related to RFID technology. We identified three major risk categories concerning *technology integration*, *privacy and security*, and *standardization*.

Technology integration for RFID systems is composed of two levels: (i) the software level for back-end integration and (ii) the hardware level for physical integration in the process. Properties of the manufacturing environment are crucial for the latter. Solid objects (especially metal) can absorb and reflect RFID signals. Thus, tags may be missed or captured at positions outside the intended reader scope (e.g., at a different process step). At the software level, it is necessary to connect RFID middleware to other systems (e.g., an ERP). Similarly, in any IT integration project this poses challenges, e.g., in finding suitable interfaces and organizing the migration to new solutions. A special challenge of RFID data integration is data quality. It is important to understand that raw RFID data can include false positive and false negative reads. It is therefore crucial to define the required data quality and to implement appropriate cleaning mechanisms. Achieving the required data quality can be a serious obstacle in some projects and may pose the risk of failure. It is hardly possible to quantify all these aspects of the technology integration in advance.

Security continues to be a controversial aspect of RFID applications. Their (real or perceived) insecurity potentially jeopardizes the confidentiality of business operations. The possibility to read out tags without line of sight exposes RFID data to anyone who can come close to the tag (e.g., staff of logistic service providers). It is therefore important to assess the confidentiality of data on RFID tags, to weigh the risks, and to possibly implement counter measures. It may be advisable, for example, to remove or even destroy the tags at the end of the production line. Beyond protecting information on RFID tags, security analysts must carefully evaluate network-based exchange of RFID data. Again, one must trade the confidentiality of RFID data against the security risks of the technology used. However, compared with risks regarding technology integration and technology development the risks related to security are less important in the manufacturing domain; for a more detailed discussion of security issues, see Section 7.

Standardization is essential for the sustainability of an application and for leveraging network effects. Even though GS1 has released the well-known standard Gen2 for ultra-high-frequency tags, unsolved standardization questions still exist. The authorized frequency spectra for RFID must still be harmonized and dominating standards for high frequency technology are still missing. Even though the standardization situation is improving, there remains a degree of uncertainty for numerous solutions.

6.3.4 Weighing Intangible Costs and Benefits

Not all costs and benefits occur in each RFID rollout. Moreover, if they arise, their importance may differ substantially. In order to assess non-quantifiable costs and benefits, we suggest a lightweight multi-dimensional decision model where one assigns weights to the different aspects, specific to each case. Aspects and weights are represented by a tree whose root represents the specific RFID rollout (Figure 6.2).

The tree should be traversed first top-down, then bottom-up. While traversing the tree, each node should be assigned with a relative importance and a score, respectively. The relative importance will typically be assigned by management, whereas the improvement will be evaluated by domain experts. We assign positive scores for benefits and negative scores for risks and their associated expected cost.

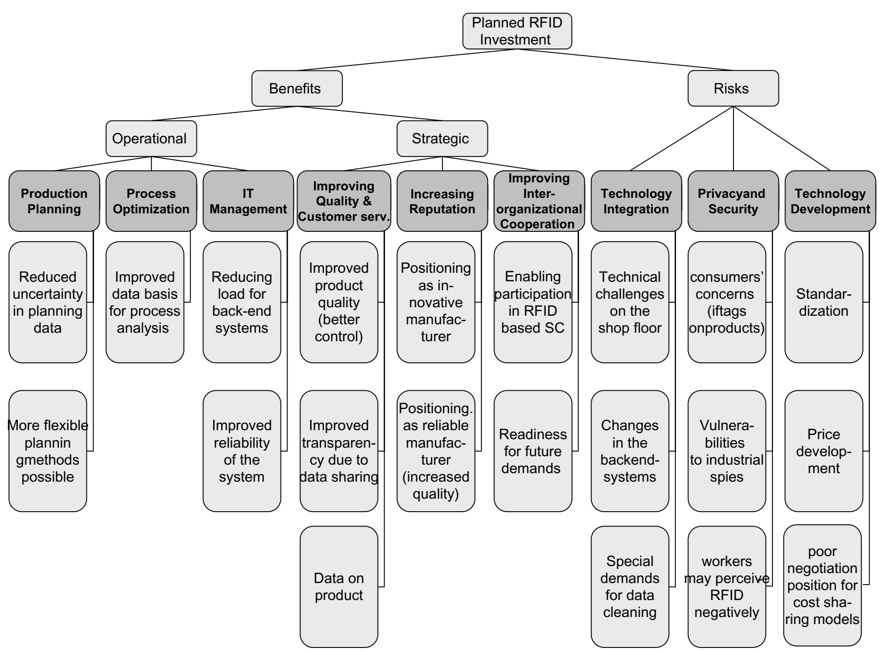

Fig. 6.2 Tree classifying the non-quantifiable, intangible aspects of RFID in manufacturing.

While traversing top-down, managers use their corporate knowledge when assigning weights for the relative importance of each node. For example, production planning may be considered more important than IT management or process optimization. During the top-down traversal, managers assign weights to all descendant nodes in relative importance to each other by using VBA, which is a common scoring model [10]. The goal of the pairwise comparison method is to create a rank table among the children for each node.

Subsequently, domain experts traverse the tree bottom-up and give each node a score for an expected improvement or occurring risk. They start by analyzing all leaves of the tree and assigning each leaf a score. The score denotes the impact of RFID on this particular aspect. We use a standard equidistant scale for the scores. After completing all scores for the leaves, we use the ranking data (the relative importance) created by the management. We calculate a weighted average score for each leaf. Then, we assess the final score of the analyzed investment by recursively calculating the scores bottom-up, i.e., for all interior nodes we multiply each child node's score with its relative importance, add the scores of all children, and pass the total score to the parent.

We calculate the overall score for the planed RFID rollout by traversing the tree both ways. An analogous approach can be used to evaluate possible alternatives, such as barcode-based solutions. Hereby, it is irrelevant whether the competing technology is already in use. If the competing technology is barcode, then the tree can be used as it is. If the RFID rollout should be compared with some other technology, such as OCR, the tree would need to be adjusted accordingly. After having evaluated competing alternatives from the perspective of non-quantifiable costs and benefits, evaluation results need to be integrated with the results from the monetary evaluation. This combined assessment then serves as the basis for the final investment decision.

In combination with the evaluation methods presented before, these guidelines offer decision makers a basis for an RFID investment analysis. However, integrating monetary and non-monetary assessments has always been a challenging task, due to the heterogeneity of decision-relevant factors, as well as the diversity of possible investment scenarios. In general, it is hardly possible to use one type of approach for all types of investment [5]. Therefore, we propose to apply different decision techniques, depending on the investment's main focus and motivation. For the manufacturing domain, the interested reader can find a description of diferent investment types in [61].

6.4 Conclusion

In this section, we reviewed work on assessing investments in RFID applications. We showed that substantial research has already been conducted on assessing costs and benefits of RFID investments. Until now, the focus has mainly been on logistic applications. Most models lack an evaluation of the intangible, non-quantifiable aspects of such an investment. In this section, we illustrated what factors are to consider regarding assessing cost and benefits of RFID. We discussed quantifiable costs and benefits resulting from the seven typical RFID-application scenarios evaluated in Section 3. We also described non-quantifiable aspects of an RFID investment and dealt with the question of how to combine tangible and intangible costs and benefits.

In the following section, we focus on the security and privacy aspects of RFID technologies and applications.

7

Security and Privacy

Security and privacy of Radio Frequency Identification (RFID) systems play an important role in the acceptance of RFID and related infrastructures [54]. For an early controversial, but influential expression of subjective fears for individual privacy, see Albrecht and McIntyre [3], for more objective early accounts of the problems involved compare Garfinkel and Rosenberg [45, 46]. In the following, we first describe security challenges of RFID tag and reader systems before we turn our intention to RFID back-end infrastructures and the EPCglobal Network (EPCN).

7.1 RFID Tag–Reader Security and Privacy Challenges

Ironically, the key advantage of RFID, namely the ability of tags to transmit data without having to stay in a direct contact with a reading device, has also caused most of the controversy surrounding RFID adoption. As discussed, a typical RFID tag stores a number that identifies some physical object. If the identifier is encoded according to the EPCglobal standards (e.g., SGTIN-96), the number can convey a great deal of information about the corresponding object. In case the tagged objects are someone's personal belongings (e.g., clothes, medicines, luxury items), the ease with which this number can be obtained may be perceived negatively by individuals, fearing loss of control over their private sphere.

Ubiquitous computing environments based on RFID may allow third parties to determine personal behavior and track individuals' physical movements without prior notice. RFID has also added a new dimension to the traditional privacy debate, because much more data can potentially be collected about individuals. Potential tracking of personal whereabouts and social network analysis has gained a physical dimension. Unique item identification inherent in the proposed Electronic Product Code (EPC) standard can potentially lead to a degree of personal attribution and surveillance never before possible [54].

In case a proprietary encoding scheme is used, it is usually only a matter of time until the interpretation of the encoding is leaked to the public. However, even if not, there exists a concern that the uniqueness of the identifier may be used for tracking of individuals by continuously querying the tag by readers distributed across various locations. Additionally, when dealing with tags capable of updating the stored values, existing standards provide a very limited protection against attacks in which the values are modified or erased, either with some malicious purpose or as an act of vandalism.

For preventing unauthorized reads, the Class-1 Gen 2 tags implement a "kill function" that allows permanently disabling RFID tags (e.g., at the point of sale). Unauthorized kills and writes are prevented having a tag storing two 32-bit passwords — one for authorizing a kill command and an optional one for authorizing a write access. The insufficient length of the passwords and weaknesses of the authorization algorithm provide, though, only a minimal level of security, protecting only against simple attacks. Moreover, killing a tag means that it cannot be used for after-sale purposes anymore (return, guarantee, utilization, etc.). Development of secure tag–reader communication schemes is currently a topic of active research with promising results that can be implemented in future generations of RFID tag standards.

The problem of secure communication is quite well studied and there exist numerous time-proven and reliable solutions that allow for ensuring the secrecy of the data transmission between two parties. In the light of the concerns, we have discussed above, ensuring the secrecy means (i) ensuring that the RFID tag is communicating with a trusted or authenticated reader and (ii) ensuring that the communication between a tag and a trusted reader cannot be eavesdropped by an untrusted third party, or communication encryption. Additionally, the specificities of the RFID technology have to be considered: namely, the passive character of the tag and the requirement to keep its cost as low as possible.

An early and relatively simple example of a tag–reader authentication protocol is a randomized hash-lock procedure proposed in [112]. According to the protocol, the logic of a tag implements a cryptographically strong hash function that allows locking the tag by storing in it a hash h of a randomly generated key k. The protocol successfully ensures that the tag communicates only with readers that know the correct key, and the key itself is never transmitted in the cleartext. The main problem with this approach is the requirement to have the back-end database permanently accessible to the readers. Note also that this simple protocol does not prevent tracking of the tag, as the tag always responds with the same value h.

To avoid any reader-back-end communication, authentication could be implemented using public key algorithms in which the tag and the authorized reader store public and private keys correspondingly. To authenticate itself to a tag, the reader sends a notification and receives a random challenge generated by the tag. The reader uses its private key to encrypt the challenge and sends it back to the tag. By decrypting the received cipher text and comparing it with the original challenge, the tag verifies whether the reader possesses the required private key and establishes the communication session if the resulting plaintext is equal to the issued.

The compact size of the tag and the requirement to keep its cost as low possible pose strict limits on the available functionality, often leaving no place for security mechanisms that could protect the tag-reader communications. In [73], it is argued that an RFID chip with production costs below 50 cents should contain 2.000–10.000 logical gates. Only 200–2.000 of them are available for security needs. This is not enough for being able to implement any of the mentioned authentication mechanisms. Of course, there is still potential for further miniaturization of the gates and assuming that Moore's Law also holds for RFID tags, the availability of low-cost tags capable of handling the listed algorithms may be a question of time. However, currently the primary concern of the industry is driving tag prices down.

To address the drawbacks of the security schemes relying exclusively on cryptographic primitives, some researchers have proposed an alternative approach in which the communication between tags and a reader are monitored and managed by an intermediary device. In [64], Juels et al. propose to use an RFID Enhancer Proxy device that, by aggregating information about the tags and putting them in a sleep mode, can simulate their behavior by performing all desired interactions with readers. A similar approach is proposed in [86] where a device named Privacy Guardian is described. Instead of acting as a proxy, Privacy Guardian acts more as an outgoing firewall. Integrated in a mobile phone, these devices can deliver a high degree of privacy protection giving the users direct control over the actions of their tags. However, the requirement to buy and to constantly carry an additional device may prevent this approach from being accepted as a standard approach for enforcing a tag–reader authentication.

To provide a user with the highest degree of control over the tag-reader communication, a PIN (or password) mechanism could be employed [92]. In this scheme, a user provides tags with the password at the point of sale, while checking out tagged items. Next time, when some reader attempts to read these tags, the tags respond only once the reader is provided a correct password. This approach is very similar to the PIN-based authentication of credit cards, where a user has an explicit control over the communication transaction. Moreover, such a scheme is quite easy to implement. In order to prevent transmitting the PIN as a plaintext, it still requires the tag to implement a cryptographically strong hash function. However, it does not rely on any data stored in a back-end. For more information about securing tag–reader communications, the one can consult reviews conducted by Garfinkel et al. [44] and Juels [63]. Another excellent source is a web site maintained by Avoine and representing a constantly updated list of relevant publications [7].

7.2 EPCglobal Network Security and Privacy Challenges

Security and privacy engineering for RFID systems must not only consider tag–reader communication, but also need to take back-end and global information infrastructures such as the EPCN (cf. Section 5: *RFID in the Supply Chain*) for RFID into account. Surveys of corresponding security requirements, issues, and defense mechanisms are given by BRIDGE [14, 15], Fabian and Günther [37], Fabian et al. [38], and Konidala et al. [66].

As the Object Naming Service (ONS) is a critical component of the EPCN, we focus on its exemplary security issues in the following. For ONS, a hierarchical, tree-like architecture has been proposed by EPCglobal. The ONS protocol is identical to the protocol used by the Domain Name System (DNS). The ONS Root is the central root of this tree. Further delegation works as in DNS, and information providers itself will deploy authoritative ONS servers — for their EPC ranges — that point to their actual EPC Information Services (EPCIS). This architecture and protocol choice will have a deep impact on the reliability, security, and privacy of the involved stakeholders and their business processes, especially for information clients.

From a technical point of view, ONS is a subsystem of the DNS. The main design idea of ONS is to first encode the EPC into a syntactically correct domain name, then to use the existing DNS infrastructure to query for additional information.

7.2.1 ONS Resolution Process

The ONS resolution process is described in [30]. For a schematic view of the communication procedure, compare Figure 7.1.

After an RFID reader has received an EPC in binary form, it forwards it to some local middleware systems. To retrieve the list of relevant EPCIS servers for this particular object, the middleware system converts the EPC into a domain name (e.g.,

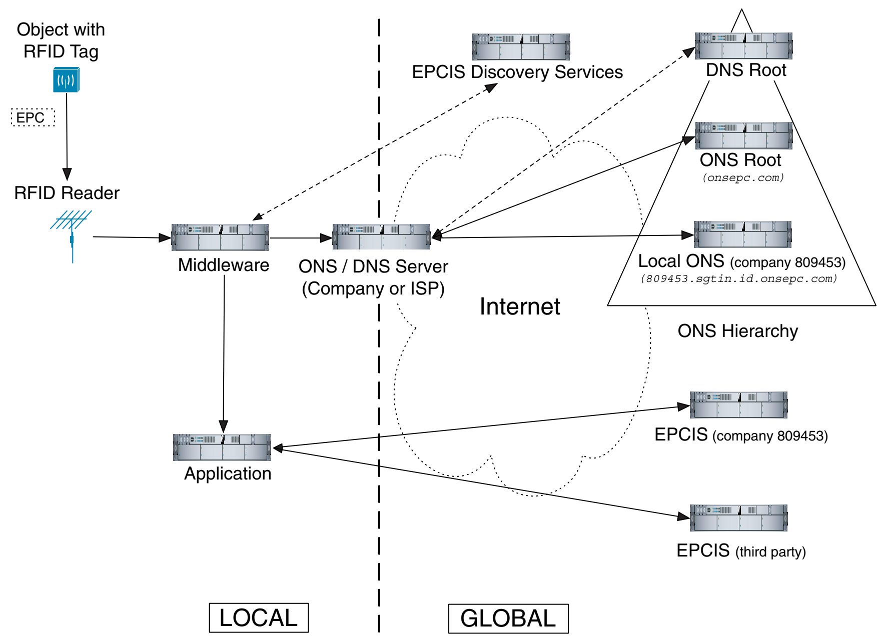

Fig. 7.1 ONS resolution process.

1734.809453.sgtin.id.onsepc.com) by following a well-defined procedure. This newly created domain name is now queried for by using the common DNS protocol, possibly involving a recursive query to a local DNS or service provider DNS server that then queries iteratively across the Internet. In addition to this primary ONS use of the DNS, note a secondary dependency on the existing DNS hierarchy: The names stored in ONS records and returned by the ONS query process will again have to be resolved into IP addresses — using the standard DNS hierarchy — to receive the IP addresses of the EPCIS servers, compare (3a, b) in Figure 5.2.

7.2.2 ONS Availability

ONS will constitute a service highly exposed to attacks from the Internet. A particular threat is Denial of Service (DoS), which abuses

Table 7.1. Risks caused by lack of availability.

Application area	Risks caused by lack of availability
Production	Reduced functionality Stop of production processes Possible sabotage
Logistics	Reduced functionality Problems with order and delivery processes Possible sabotage Lack of status updates Reduced transparency
Private applications	Lack of product information Reduced functionality of "Smart Applications" (Smart Home or Office, personalized counseling services)

system and network resources to make the service unavailable or unusably slow for legitimate users [22]. This could include Distributed Denial-of-Service (DDoS) attacks overwhelming a particular server or its network connection by issuing countless and intense queries.

Another facet of DNS politics relevant to ONS availability is a rather global political challenge. Who should control and operate the root and Top-level Domain (TLD) servers, and the name space as a whole? As was discussed in Section 5: *RFID in the Supply Chain*, to let a single company take control of the ONS root (in addition to its major role in the DNS root and certification authority (CA) services) may hinder international acceptance of the system as a whole. Therefore, an integration of the EPCN — with ONS as proposed — into core business processes could leave even formerly non-IT-related companies dependable on the availability of Internet services. This will most probably increase overall business risk (see Table 7.1).

7.2.3 ONS Integrity

Integrity in the ONS context refers to the correctness and completeness of the returned information, that is, in general, addresses of EPCIS corresponding to the queried EPC. An attacker controlling intermediate DNS servers or launching successful Man-in-the-Middle (MITM) attacks on the DNS communication could forge the returned list of

Table 7.2. Risks caused by lack of integrity and authenticity.

Application area	Risks caused by lack of integrity and authenticity
Production	Reduced functionality Stop of production processes Possible sabotage Possible industrial espionage
Logistics	Reduced functionality Problems with order and delivery processes Possible sabotage Lack of status updates Unauthorized manipulation of processes and object data Possible economic espionage
Private applications	Unauthorized manipulation of product information Reduced/maliciously changed functionality of "Smart Applications" (Smart Home or Office, personalized counseling services)

URIs and include, for example, a malware-hosting server under his/her control. DNS spoofing attacks are quite easily possible because there are no widely deployed integrity-preserving measures in the DNS protocol, for UDP, or the IP layer.

If there are no sufficient authentication measures for the EPCIS in place, the attacker could deliver forged information about this particular or other related EPCs from a similar domain. The corresponding risks will be specific to the application: If the query was initiated by a smart fridge to order matching ingredients for a cooking recipe, this could result in spoiled meals; if the query was issued by a smart medicine cabinet — as a precursor to an even smarter home medical advisor — to prevent harmful drug mixes, this could involve more serious risks to personal safety. Similar risks would exist for business environments (Table 7.2).

7.2.4 ONS Confidentiality and Privacy

ONS, being based on DNS, provides no mechanism to achieve confidentiality. This lack applies to the query originator, the query target, and, most of all, the query content. As a part of an information architecture on physical objects, ONS involves even more risks to confidentiality and privacy than DNS does for surfing the Web. For the publisher, the ONS lack of confidentiality is evident: all the information published to ONS has to be considered public. There is no encryption or access control mechanism available. However, for the basic name service function that ONS is to provide, that is, the retrieval of manufacturer EPCIS addresses, this can hardly be considered a real risk for the manufacturer, once the decision on using EPCs and to participate in the EPCN has been made.

In many situations, however, the EPC of an RFID tag has to be regarded as highly sensitive information — be it in private, or in business environments where product and raw material flows constitute valuable market information. Even if the complete serial number of the EPC is not known, the combination of object class and company, identifier is enough to determine the kind of object to which it belongs. Captured EPCs can be used to identify assets of an entity, be it an individual, a household, a company, or another organization. If someone happens to wear a rare item, or a rare combination of belongings, tracking him may be accomplished even without knowing the actual serial numbers, simply by using the object classes.

All traversed Internet service providers and backbone carriers might capture the EPC — this also holds for network taps placed by governmental organizations of countries the packets may cross. All of the ONS query logging and analysis can be achieved with tools and techniques already in use today, virtually without any risk, and only very moderate

Table 7.3. Risks caused by lack of confidentiality.

Application area	Risks caused by lack of confidentiality
Production	Possible economic espionage Analysis of good flows Analysis of business relationships
Logistics	Possible economic espionage Analysis of good flows Analysis of business relationships
Private applications	Profiling of individuals: (possessions, lifestyle, consumer behavior, social contacts) Inference of highly sensitive data (e.g., of medical condition from pharmaceuticals acquired)

effort on the collectors side. Some of those are DNS server logs, network analysis tools, Intrusion Detection Systems, and domain-specific transaction stream analyzers used in telecommunications.

Discovery Service providers will also be able to harvest the source IP and the full EPC from their log files. Even if the actual connection to an EPCIS server is encrypted, the EPCIS operator himself (e.g., the manufacturer) could compile profiles of the subset of EPCN users who query for information at this particular server. The initial DNS lookup for EPCIS name resolution could betray the object brand to an even larger set of adversaries.

It follows that attacks, which, for example, involve profiling of someones assets, will also include several remote tactics. See Table 7.3 for an overview of corresponding confidentiality risks.

7.3 Conclusion

If the EPCN becomes widely accepted, more and more business processes (B2B, B2C) as well as private applications will be able to use it without human intervention. This would leave those processes highly dependent on a robust and secure EPC resolution and information retrieval. In addition, it will expose them to potentially massive data collection by many possible adversaries.

This section discussed security and privacy challenges for RFID systems and the EPCN. The following section will present some alternative approaches for decentralized global information infrastructures for RFID.

8

Decentralized EPCglobal Network Architectures

In this section we present several proposals for a modification to the current Object Naming Service (ONS) architecture. The objective is to distribute the control over the ONS root among several independent parties in order to resolve the power structure problem described above.

8.1 Multipolar ONS

Here, we present the architecture of Multipolar ONS (MONS), a naming service for the Internet of Things in many respects based on the existing ONS architecture but with distributed (or multipolar) control over the root. This architecture is based on [33]. MONS, similar to ONS, uses domain names and relies on DNS for resolving them in IP addresses corresponding to the servers running EPCIS.

Compared with the organizational structure of the ONS root, where a single entity is responsible for its operations (Figure 5.3), today's organization of the DNS root does not have such a bottleneck. This allows us to conclude that although DNS is *de iure* controlled by the US Department of Commerce, *de facto* the control is distributed between numerous international entities [50], thereby making the problem of the

DNS unipolarity not so evident as in the ONS case. One has to note, however, that the introduction of DNSSEC [6] to secure DNS integrity can involve new challenges for multipolarity [67, 74].

One of the main reasons for choosing DNS as a basis for the EPCglobal Network (EPCN) name service is minimizing the effort required for its deployment. Over the past two decades, DNS has proved to be a stable and mature architecture. Such choice also allows deploying ONS servers by reusing already existing software and expertise. Using free or commercial software, a system administrator with experience in administering DNS servers can easily set up an ONS server. Therefore, when proposing modifications to the existing ONS standard, it makes sense remaining compatible with the DNS architecture.

Probably the easiest and the most obvious way for distributing the control over the ONS root is to re-use the approach adopted by DNS, in which the data describing the root domain are replicated among numerous physical servers operated by various independent entities. To synchronize the replicas, some organization (e.g., EPCglobal) should take the responsibility of maintaining records for the ONS root domain and making them available to the operators of the ONS root servers (Figure 8.1).

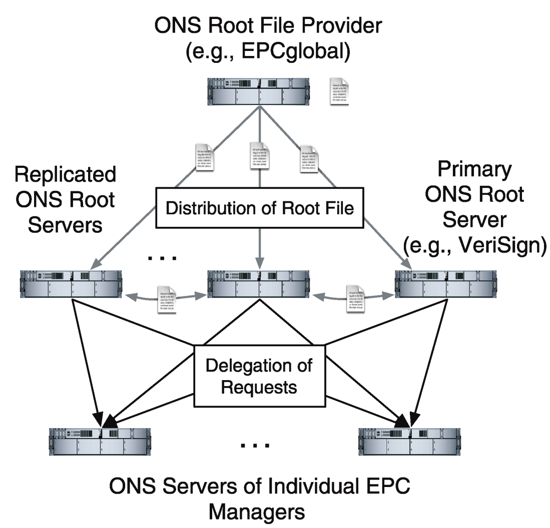

Fig. 8.1 MONS with replicated root.

The advantage of the described approach is that it allows distributing control over the ONS root with virtually no changes to the current ONS specification. All that is required is to ensure the availability of the records describing the ONS root domains to the entities willing to deploy own ONS root nameservers and that these mirrors are made reachable for ONS requests. The latter can be implemented either via anycast or via the registry of the .com domain (VeriSign), which should modify .com to include Resource Records (RRs) referencing onsepc.com domain name to the IP addresses of all the mirrors.

The problem with this approach is that although it allows avoiding the situation when the ONS root is controlled by a single entity, it cannot provide a complete independency of the replicated roots, as they still are periodically synchronized against a master description of the ONS root zone. Additionally, their binding to the onsepc.com domain name makes them dependent on the registry of the .com domain (note that changing to another domain still cannot solve this problem).

For completely solving the issue of unipolar control over ONS, the current ONS standard has to be modified to a greater extent. In the remainder of this section, we will provide the description of a truly multipolar architecture referred further as *MONS* (Multipolar ONS). The basic idea behind MONS is to split the ONS root zone into a number of non-overlapping zones and distribute them between several MONS root nameservers that are independent but, at the same time, are aware of each other.

To resolve a MONS query, it should be sufficient for a client to know the domain name of just one of these MONS root nameservers. If the query can be resolved within the zone of this nameserver, it simply proceeds with the resolution processes. Otherwise, the query is delegated to the MONS root nameserver authoritative for the zone within which the query can be resolved. As political issues are the primary source of this debate, it would make sense defining the MONS root zones according to the regional allocation of the corresponding EPC Managers. The region can be determined by the address under which the company is registered, by the regional GS1 organization that issued the Company Prefix, or by any other appropriate attribute. An instance of the regional MONS architecture is presented in Figure 8.2.

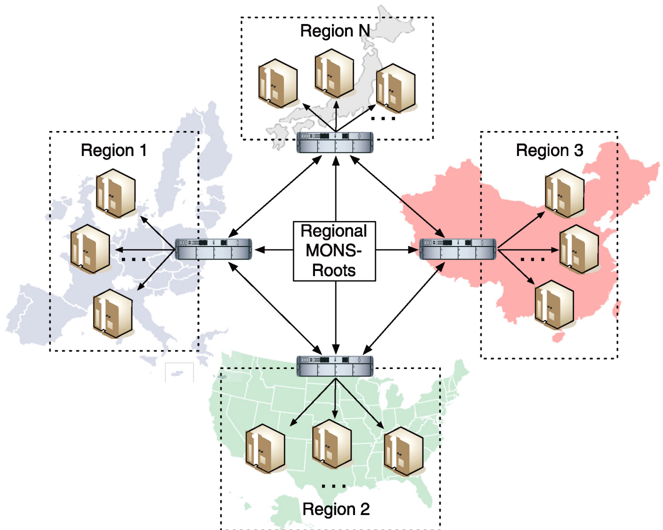

Fig. 8.2 Regional MONS.

Allocating MONS root nameservers to regions naturally shifts the load to nameservers authoritative for economically developed or industrial countries, as regional prefixes of such regions will occur in the majority of MONS queries. Regions with low export volumes or regions not interested in maintaining their own regional MONS root nameservers can temporarily delegate this responsibility to third parties, as it is sometimes done with country code TLDs [50]. Note that all regional MONS roots are completely independent from each other and do not rely on any central entity.

8.2 Peer-to-peer ONS

In this section, we describe another possibility for decentralized global Radio Frequency Identification (RFID) infrastructures, again specifically tailored to replace ONS, but are noting the applicability for other components of the EPCN and Internet of Things. Highly distributed alternatives to classical network service architectures exist in the form of Peer-to-Peer Systems (P2P), which can be considered to be a paradigm shift from the classical client-server architecture to a new paradigm with a roughly equal distribution of responsibility and load among peers [9].

Especially structured P2P systems using Distributed Hash Tables (DHT) offer high robustness to faults, avoid single points of failures (e.g., they have no single root like DNS), and distribute responsibility and load among participants in a systematic way by means of a prearranged topological overlay structure. DHT possess lookup functionalities analogous to a hash table, but in a distributed and decentralized fashion, involving multiple computers without central control. DHT usually present a simple lookup and storage interface based on a one-to-one correspondence between data items and keys.

The underlying distributed DHT algorithms determine which nodes are responsible for storing the data by organizing keys and nodes in a logical overlay network, which is in general independent of the physical or IP network topology on lower layers, using concepts such as consistent hashing with only few local information about the whole system. Consistent hashing balances data items to nodes in a roughly uniform way and allows for node joining and leaving, without the need for major redistribution of keys and data in the running system. Most DHTs resolve lookups in $O(\log N)$ hops through the overlay network, where N is the number nodes in the DHT, which implies an excellent scalability.

This scalability is enhanced by the fact that the routing table size and amount of state information stored at any particular node also scales with $O(\log N)$, which means that every node just needs to know a very small part of the whole overlay graph. DHTs also offer functionality such as message routing in the overlay, node joining and leaving procedures, and data redundancy in a self-organized fashion. Particular DHTs use several different algorithms and overlay topologies to structure node identifiers and keys [9]. In addition, they differ in the amount of performance enhancements they offer, and in the maturity of code available so far.

In the following, a DHT-based P2P-ONS architecture called *Object Information Distribution Architecture* (*OIDA*) will be briefly discussed (Figure 8.3), based on the design given in [36] and its implementation and testing presented in [35]. OIDA involves the following key

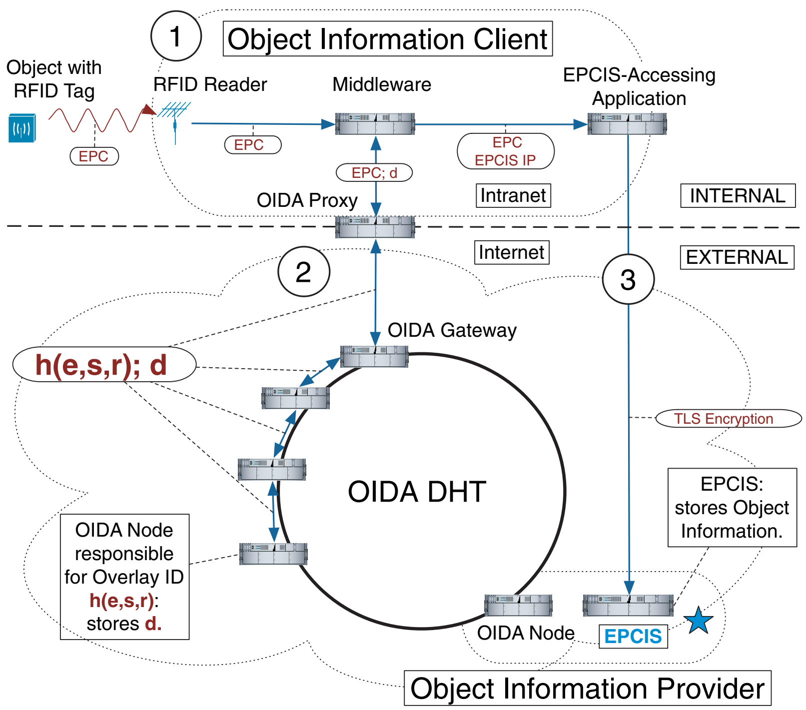

Fig. 8.3 OIDA resolution process.

ideas: Each interested company deploys dedicated OIDA-Nodes. Those nodes are part of a global critical infrastructure supported by business contracts. Technically, they form an overlay network, where a cryptographic hash function maps EPCs and nodes to overlay IDs. This pseudorandom mapping of identifiers to storage nodes balances load more evenly, allows for easy replication, avoids single points of failure, and reduces the feasibility of targeted attacks against particular information providers or clients.

The DHT provides the routing to the responsible nodes, as well as joining, leaving, repair, and optimization procedures, without a central entity managing those operations. Nodes store deterministically assigned — but from the perspective of a node owner or adversary interested in specic EPCs, apparently random — encrypted and signed documents belonging to hash value ranges. Those documents may contain object data or EPCIS IP addresses, because if possible indirect use of DNS should also be avoided. For scalable data authenticity, the existence of a certification authority (CA) infrastructure is assumed, which can also be distributed, similar to (possibly multipolar) version of DNSSEC [6] or a web of trust.

8.3 Conclusion

This section presented a short introduction to decentralized architectures that could replace parts of the EPCN for enhanced privacy and international distribution of control. Architectures such as MONS and OIDA would result in a flat power structure, since in theory no participating company has a central technical role to play.

Given an international deployment of OIDA where no single nation controls a large part of the participating nodes, OIDA would achieve a very high multipolarity in the sense that no single country could prevent the system from working, and no single country could be easily excluded by another nation. There are several organizational aspects of using OIDA as a name service for the IOT. To guarantee liability, especially in business environments using the IOT, there should be a common agreement and procedure in place that assigns EPC ranges to authoritative entities who are allowed to publish address records. An example convention would be that EPC Managers may publish address data exactly for EPCs belonging to their own company as would be indicated by the company prefix. Similar policies could be created for other object identifier systems.

9

Conclusions

In this paper, we give a case-study-based overview of the business applications of Radio Frequency Identification (RFID). All of the companies we surveyed see considerable business potential for RFID, both in terms of efficiency and in terms of effectiveness. Efficiency potential was seen by possible speedups in production, lower error rates, reduced shrinkage, improved asset tracking, and less downtime — all contributing to a higher overall productivity of manufacturing operations. Effectiveness potential was seen concerning a variety of additional services that companies could provide to their customers. Often the tagging of objects itself leads to immediate productivity gains at OEMs because they can use the tag and the additional information in their own operations. Moreover, the tracing of faulty components back to their manufacturing history is of great importance in security-sensitive industries such as the automotive sector.

In order for these positive potentials to come true, it is crucial that RFID does not form a technology island but is tightly integrated into existing IT infrastructures. Enterprise software systems need to be adapted to take advantage of the richness of data becoming available through RFID. Appropriate filtering techniques need to be put into place to make sure that software components receive the relevant information in the appropriate granularity — an information logistics problem that many ERP companies are addressing actively. Moreover, companies must consider carefully how to distribute storage and processing in the resulting multi-tier IT architecture that ranges from RFID tags and sensors, on the one hand, to data warehouses and business intelligence tools, on the other hand.

Given this positive outlook, one must ask: Why is RFID not much more widespread than it is today? We see three major reasons:

First, the technology is not always sufficiently robust and reliable. Every production and logistics environment is different, and the validity of related concerns varies accordingly. Especially the kinds of materials being processed play a major role in this context. According to our observations — not only in the case studies but also among other companies we surveyed — these technical roadblocks are gradually becoming smaller. New RFID technologies are often more robust with respect to adverse environmental conditions and they operate with very low error rates. This makes them attractive for a much broader range of manufacturing companies than was the case only a few years ago.

Second, in many cases barcodes are an attractive and economic alternative to RFID. As discussed in the previous sections, barcodes do not offer the same functionality as RFID, and they also expose different sensitivities to adverse environmental conditions (dirt, heat, etc). However, we have described several scenarios where barcode solutions fulfilled the requirements in a satisfactory manner, and they did so at a much lower price than RFID. In other words, the advantages that could potentially be achieved are not worth the price.

Third, and maybe most importantly, we have seen numerous situations where the costs and benefits of RFID do not occur at the same enterprise, which leads to investment deadlocks. Many supply chains find themselves in a kind of prisoners dilemma: Even though the introduction of RFID would improve the productivity of the supply chain as a whole, none of the participating companies goes ahead with it. The potential productivity gains are never realized because some participants would need to incur costs that are not justifiable in comparison with their local benefits — they are afraid of being stuck with the cost of the introduction while the benefits occur elsewhere. As a result, they decide — for completely rational reasons — not to adopt the new technology. This dilemma is particularly visible at many first- and second-tier suppliers. While it is known from other technologies (such as the barcode), it seems more pronounced in the RFID case, possibly due to higher overall costs or greater suspected inequalities. Suppliers are afraid of paying for RFID introduction while most of the productivity gains benefit the OEMs downstream the supply chain. One way to break this deadlock is to negotiate compensation payments between different participants in the supply chain with the objective of distributing the benefits fairly among the participants. Furthermore, significant security and privacy risks remain, partly due to the centralized nature of the most popular proposals for global RFID-based information infrastructures.

At this point, most working RFID applications are therefore motivated by short-term operational improvements, where a positive ROI over a few years seems likely. Without such operational improvements in sight, the adoption decision is a much harder one because it becomes purely strategic. The question is then whether there is an early-mover advantage for suppliers: Is it advantageous to invest into RFID even though the short-term ROI is negative? This depends on whether it may help the supplier in the long term to achieve a better competitive position. This is, it depends on the future behavior of the OEM — in particular on its intentions to favor suppliers that are using RFID in the future.

In our view, it is indeed the OEM that is most likely able to break the deadlock. OEMs that design and communicate an RFID strategy early on will be able to work with their suppliers on joint initiatives, which is likely to lead to competitive advantages. As shown by the Metro Group in retail, it can be advantageous to be an early mover [54]. In many cases, however, a successful RFID introduction will imply some cost-sharing arrangement between the supply chain partners. This may involve cross-payments or non-monetary compensation such as, for example, data sharing agreements.

If a sufficient number of OEMs is willing to break the existing log-jam, we will see RFID moving from a technology that is used mostly

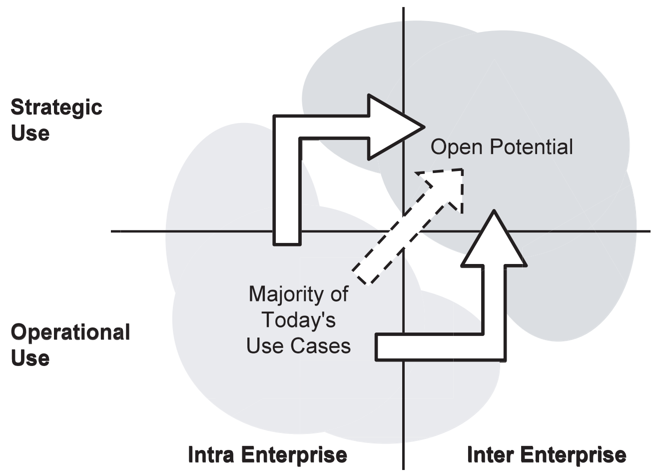

Fig. 9.1 Taxonomy of motives for RFID adoption.

operationally and intra-enterprise (cf. Figure 9.1) to one that fulfills strategic purposes and helps to improve the efficiency and effectiveness of inter-enterprise collaboration and supply chains as a whole. The Internet of Things will thus become an indispensable infrastructure of the twenty-first century economy.

Notations and Acronyms

Acronym	Extension
B2B	Business-to-business
B2C	Business-to-consumer
CA	Certification authority
DDoS	Distributed denial-of-service
DHT	Distributed hash table
DNS	Domain name system
DNSSEC	DNS security extensions
DoS	Denial-of-service
EAN	European Article Number
EPC	Electronic Product Code
EPCIS	EPC Information Service
EPCN	EPCglobal Network
GS1	Global Systems One
GTIN	Global Trade Item Number
HF	High frequency
ICANN	Internet Corporation for Assigned Names and Numbers
ID	Identifier
IOT	Internet of Things

Acronym	**Extension**
IP	Internet Protocol; also: Internet Protocol Address
IT	Information technology
ISP	Internet Service Provider
LF	Low frequency
MITM	Man-in-the-middle (attack)
MONS	Multipolar ONS
OCR	Optical Character Recognition
OEM	Original Equipment Manufacturer
OIDA	Object-Information Distribution Architecture
ONS	Object Naming (or Name) Service
P2P	Peer-to-Peer
RFC	Request for Comments
RFID	Radio-Frequency Identification
ROI	Return on Investment
RR	(DNS) Resource Record
SGTIN	Serialized GTIN
SIP	Session Initiation Protocol
SLD	Second-Level Domain
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLD	Top-Level Domain
TLS	Transport Layer Security
UCC	Uniform Code Council
UDP	User Datagram Protocol
UHF	Ultra High Frequency
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

References

[1] AFNIC, "L'afnic s'implique dans les services de registre de l'internet du futur et noue un partenariat avec gs1 France," Press release, October 2008.

[2] S. Ahson and M. Ilyas, eds., *RFID Handbook — Applications, Technology, and Privacy.* CRC Press, 2008.

[3] K. Albrecht and L. McIntyre, *Spychips: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move.* Plume, 2006.

[4] M. Amini, R. F. Otondo, B. D. Janz, and M. G. Pitts, "Simulation modeling and analysis: A collateral application and exposition of RFID technology," *Production and Operations Management*, vol. 16, pp. 586–598, 2007.

[5] J. Andresen, "A framework for selecting an IT evaluation method — in the context of construction," PhD thesis, Danmarks Tekniske Universitet, Lyngby, Denmark, 2001.

[6] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS security introduction and requirements," http://www.ietf.org/rfc/rfc4033.txt, 2005.

[7] G. Avoine, "Online bibliography on security and privacy in RFID Systems," http://www.avoine.net/rfid/, 2010.

[8] H. Baars, D. Gille, and J. Strüker, "Evaluation of RFID applications for logistics: A framework for identifying, forecasting and assessing benefits," *European Journal of Information Systems*, vol. 18, no. 6, pp. 578–591, 2009.

[9] H. Balakrishnan, M. F. Kaashoek, D. R. Karger, R. Morris, and I. Stoica, "Looking up data in P2P systems," *Communications of the ACM*, vol. 46, no. 2, pp. 43–48, 2003.

[10] E. Bernroider and S. Koch, "Empirische Untersuchung der Entscheidungsfindung bei der Auswahl betriebswirtschaftlicher Standardsoftware in

Österreichischen Unternehmen," in *Diskussionspapiere zum Tätigkeitsfeld Informationsverarbeitung und Informationswirtschaft*, (H. Hansen and W. Janko, eds.), Wien, Austria, 1999.

[11] C. Bornhövd, T. Lin, S. Haller, and J. Schaper, "Integrating automatic data acquisition with business processes — experiences with SAP's Auto-ID infrastructure," in *Proceedings of the 30th International Conference on Very large data bases (VLDB '04)*, pp. 1182–1188, 2004.

[12] E. Bottani and A. Rizzi, "Economical assessment of the impact of RFID technology and EPC system on the fast-moving consumer goods supply chain," *International Journal of Production Economics*, vol. 112, no. 2, pp. 548–569, 2008.

[13] E. Bozdag, R. Ak, and T. Koc, "Development of a justification tool for advanced technologies: An example for RFID," in *Proceedings of RFID Eurasia*, pp. 1–4, 2007.

[14] BRIDGE, "BRIDGE WP02 — Requirements document of serial level lookup service for various industries," http://www.bridge-project.eu/, August 2007.

[15] BRIDGE, "BRIDGE WP04 — Security analysis report," http://www.bridge-project.eu/, July 2007.

[16] A. Brintrup, D. Ranasinghe, and D. McFarlane, "RFID opportunity analysis for leaner manufacturing," *International Journal of Production Research*, vol. 48, no. 9, pp. 2745–2764, 2010.

[17] J. Brusey, C. Floerkemeier, M. Harrison, and M. Fletcher, "Reasoning about uncertainty in location identification with RFID," Workshop on Reasoning with Uncertainty in Robotics at IJCAI, August 2003.

[18] A. Z. Camdereli and J. M. Swaminathan, "Misplaced inventory and radio-frequency identification (RFID) technology: Information and coordination," *Production and Operations Management*, vol. 19, no. 1, pp. 1–18, 2010.

[19] A. R. Cannon, P. M. Reyes, G. V. Frazier, and E. L. Prater, "RFID in the contemporary supply chain: Multiple perspectives on its benefits and risks," *International Journal of Operations & Production Management*, vol. 28, pp. 433–454, 2008.

[20] G. Chappell, L. Ginsburg, P. Schmidt, J. Smith, and J. Tobolski, "Auto-ID on the line: The value of Auto-ID technology in manufacturing," Technical Report, Auto-ID Center, 2003.

[21] V. Chawla and D. S. Ha, "An overview of passive RFID," *IEEE Communications Magazine*, no. 9, pp. 11–17, 2007.

[22] S. Cheung, "Denial of service against the domain name system," *IEEE Security and Privacy*, vol. 4, no. 1, pp. 40–45, 2006.

[23] J. C. Cox, S. Ross, and M. Rubinstein, "Option pricing: A simplified approach," *Journal of Financial Economics*, vol. 7, no. 3, pp. 229–263, 1979.

[24] J. Curtin, R. Kauffman, and F. Riggins, "Making the most out of RFID technology: A research agenda for the study of adoption, usage and impact of RFID," *Information Technology and Management*, vol. 8, no. 2, pp. 87–110, 2007.

[25] D. Delen, B. C. Hardgrave, and R. Sharda, "RFID for better supply-chain management through enhanced information visibility," *Production and Operations Management*, vol. 16, no. 5, pp. 613–624, 2007.

[26] A. Dutta, H. L. Lee, and S. Whang, "RFID and operations management: Technology, value, and incentives," *Production and Operations Management*, vol. 16, pp. 646–655, 2007.

[27] EPCglobal, "The EPCglobal network: Overview of design, benefits, security," 2004.

[28] EPCglobal, "EPCglobal tag class structure," http://www.epcglobalinc.org/standards/TagClassDefinitions_1_0-whitepaper-20071101.pdf, November 2007.

[29] EPCglobal, "EPC radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz–960 MHz version 1.2.0," www.epcglobalinc.org/standards/uhfc1g2/, October 2008.

[30] EPCglobal, "EPCglobal object naming service (ONS) 1.0.1," http://www.epcglobalinc.org/standards/ons/, May 2008.

[31] EPCglobal, "EPCglobal tag data standards — Version 1.4," http://www.epcglobalinc.org/standards/tds/, August 2008.

[32] EPCglobal, "The EPCglobal architecture framework — Version 1.3," http://www.epcglobalinc.org/standards/architecture/, March 2009.

[33] S. Evdokimov, B. Fabian, and O. Günther, "Multipolarity for the object naming service," in *Proceedings of the Internet of Things (IOT 2008), Zurich, Switzerland, 2008*, pp. 1–18, Berlin-Heidelberg: Springer-Verlag, 2008.

[34] S. Evdokimov, B. Fabian, S. Kunz, and N. Schoenemann, "Comparison of discovery service architectures for the internet of things," in *Proceedings of the 3rd IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2010)*, 2010.

[35] B. Fabian, "Implementing secure P2P-ONS," in *Proceedings of the IEEE International Conference on Communications (IEEE ICC 2009), Dresden*, 2009.

[36] B. Fabian and O. Günther, "Distributed ONS and its Impact on Privacy," in *Proceedings of the IEEE International Conference on Communications (IEEE ICC 2007), Glasgow*, 2007.

[37] B. Fabian and O. Günther, "Security challenges of the EPCglobal Network," *Communications of the ACM*, vol. 52, no. 7, pp. 121–125, July 2009.

[38] B. Fabian, O. Günther, and S. Spiekermann, "Security analysis of the Object Name Service," in *Proceedings of the 1st IEEE Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2005), in conj. with IEEE ICPS 2005, Santorini, Greece*, pp. 71–76, 2005.

[39] G. Ferrer, N. Dew, and U. Apte, "When is RFID right for your service?," *International Journal of Production Economics*, vol. 124, no. 2, pp. 414–425, 2010.

[40] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification.* New York, NY, USA: John Wiley & Sons, Inc., 2003.

[41] E. Fleisch and F. Mattern, eds., *Das Internet der Dinge — Ubiquitous Computing und RFID in der Praxis.* Berlin-Heidelberg: Springer-Verlag, 2005.

[42] C. Floerkemeier and M. Lampe, "RFID Middleware design: Addressing application requirements and RFID constraints," in *Proceedings of the 2005 Joint Conference on Smart Objects and Ambient Intelligence (sOc-EUSAI '05)*, pp. 219–224, New York, NY, USA: ACM, 2005.

[43] B. Flyvbjerg, “Five misunderstandings about case study research,” *Qualitative Inquiry*, vol. 2, pp. 219–245, 2006.

[44] S. Garfinkel, A. Juels, and R. Pappu, “RFID privacy: An overview of problems and proposed solutions,” *IEEE Security and Privacy*, vol. 3, no. 3, pp. 34–43, May–June 2005.

[45] S. Garfinkel and B. Rosenberg, eds., *RFID Applications, Security, and Privacy*. Addison-Wesley, 2005.

[46] S. L. Garfinkel, “An RFID Bill of Rights,” http://www.technologyreview.com/communications/12953/, October 2002.

[47] G. Gaukler and R. Seifert, “Applications of RFID in supply chains,” *Trends in Supply Chain Design and Management: Technologies and Methodologies*, pp. 29–48, 2007.

[48] G. M. Gaukler, “Preventing avoidable stockouts: The impact of item-level RFID in retail,” *Journal of Business and Industrial Marketing*, vol. 25, no. 8, pp. 572–581, 2010.

[49] G. M. Gaukler, R. W. Seifert, and W. H. Hausman, “Item-level RFID in the retail supply chain,” *Production and Operations Management*, vol. 16, no. 1, pp. 65–76, 2007.

[50] S. Gibbard, “Geographic implications of DNS infrastructure distribution,” *The Internet Protocol Journal*, vol. 10, no. 1, pp. 12–24, 2007.

[51] C. Goebel and O. Günther, “Benchmarking RFID profitability in complex retail distribution systems,” *Electronic Markets*, vol. 19, no. 2–3, pp. 103–114, 2009.

[52] GS1, “Der RFID Kalkulator im Überblick,” Technical Report, GS1 Germany, 2007.

[53] O. Günther, W. Kletti, and U. Kubach, *RFID in Manufacturing*. Berlin, Heidelberg, Germany: Springer, 1st ed., 2008.

[54] O. Günther and S. Spiekermann, “RFID and the perception of control: The consumer’s view,” *Communications of the ACM*, vol. 48, no. 9, pp. 73–76, September 2005.

[55] S. Gupta, C. Koulamas, and G. J. Kyparisis, “E-Business: A review of research published in production and operations management (1992–2008),” *Production and Operations Management*, vol. 18, no. 6, pp. 604–620, 2009.

[56] B. C. Hardgrave, S. Langford, M. Waller, and R. Miller, “Measuring the impact of RFID on out of stocks at Wal-Mart,” *MIS Quarterly Executive*, vol. 7, no. 4, pp. 181–192, 2008.

[57] H. S. Heese, “Inventory record inaccuracy, double marginalization, and RED adoption,” *Production and Operations Management*, vol. 16, pp. 542–553, 2007.

[58] J. Holmstrom, K. Framling, and T. Ala-Risku, “The uses of tracking in operations management: Synthesis of a research program,” *International Journal of Production Economics*, vol. 126, no. 2, pp. 267–275, 2010.

[59] Z. Irani, A. Gunasekaran, and Y. K. Dwivedi, “Radio frequency identification (RFID): Research trends and framework,” *International Journal of Production Research*, vol. 48, no. 9, pp. 2485–2511, 2010.

[60] ISO/IEC-18000, “Information technology — radio frequency identification for item management — Part 6: Parameters for air interface communications at

860 MHz to 960 MHz," Technical Report, ISO — International Organization for Standardization, 2004.

[61] L. Ivantysynova, M. Klafft, H. Ziekow, O. Günther, and S. Kara, "RFID in manufacturing: The investment decision," in *Pacific Asia Conference on Information Systems*, 2009.

[62] S. R. Jeffery, G. Alonso, M. J. Franklin, W. Hong, and J. Widom, "A pipelined framework for online cleaning of sensor data streams," in *Proceedings of the 22nd International Conference on Data Engineering (ICDE '06)*, p. 140, Washington, DC, USA: IEEE Computer Society, 2006.

[63] A. Juels, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381–394, February 2006.

[64] A. Juels, P. Syverson, and D. Bailey, "High-power proxies for enhancing RFID privacy and utility," in *5th International Workshop on Privacy Enhancing Technologies (PET 2005)*, 2005.

[65] R. Khosla and B. Chowdhury, "Real-time RFID-based intelligent healthcare diagnosis system," *Medical Biometrics*, pp. 184–191, 2008.

[66] D. M. Konidala, W.-S. Kim, and K. Kim, "Security assessment of EPCglobal architecture framework," 2006.

[67] B. Kuerbis and M. Mueller, "Securing the root: A proposal for distributing signing authority," Paper IGP07-002, 2007.

[68] R. Laubacher, S. Kothari, T. Malone, and B. Subirana, "What is RFID worth to your company? Measuring performance at the activity level," *MIT Center for eBusiness Research Brief*, vol. 7, no. 2, pp. 1–6, 2005.

[69] H. Lee, "Peering through a glass darkly," *International Commerce Review*, no. 1, pp. 60–68, 2007.

[70] H. Lee and O. Ozer, "Unlocking the value of RFID," *Production and Operations Management*, vol. 16, no. 1, pp. 40–64, 2007.

[71] H. Lee, B. Peleg, J. Paresh, S. Sarma, M. Schoonmaker, and B. Subirana, "EPC value model," Technical Report, Board of Trustees of Leland Stanford Junior University, 2004.

[72] L. S. Lee, K. D. Fiedler, and J. S. Smith, "Radio frequency identification (RFID) implementation in the service sector: A customer-facing diffusion model," *International Journal of Production Economics*, vol. 112, no. 2, pp. 587–600, 2008.

[73] M. Lehtonen, T. Staake, F. Michahelles, and E. Fleisch, "From identification to authentication — A review of RFID product authentication techniques," in *Printed handout of Workshop on RFID Security — RFIDSec 06*, 2006.

[74] J. Leyden, "Homeland security grabs for net's master keys," The Register, 3 April 2007, 2007.

[75] C.-J. Li, L. Liu, S.-Z. Chen, C. C. Wu, C.-H. Huang, and X.-M. Chen, "Mobile Healthcare Service System Using RFID," in *Proceedings of the IEEE International Conference on Networking, Sensing and Control*, pp. 1014–1019, Taiwan, 2004.

[76] C. M. Liu and L. S. Chen, "Applications of RFID technology for improving production efficiency in an integrated-circuit packaging house," *International Journal of Production Research*, vol. 47, no. 8, pp. 2203–2216, 2009.

[77] C. Loebbecke, "RFID technology and applications in the retail supply chain: The early metro group pilot," 18th Bled eConference, 2005.

[78] C. Loebbecke, J. Palmer, and C. Huysken, "RFID's Potential in the fashion industry: A case analysis," *19th Bled eConference eValues*, pp. 1–11, 2006.

[79] H. C. Lucas, *Information Technology and the Productivity Paradox — Assessing the Value of Investing in IT.* Oxford University Press, 2nd ed., 1999.

[80] METRO AG, "METRO group future store initiative," http://www.future-store.org, February 2010.

[81] G. Miragliotta, A. Perego, and A. Tumino, "A quantitative model for the introduction of RFID in the fast moving consumer goods supply chain: Are there any profits?," *International Journal of Operations and Production Management*, vol. 19, no. 10, pp. 1049–1082, 2009.

[82] E. W. Ngai, J. K. Poon, F. F. Suk, and C. C. Ng, "Design of an RFID-based healthcare management system using an information system design theory," *Information Systems Frontiers*, vol. 11, no. 4, pp. 405–417, 2009.

[83] E. W. Ngai, C. K. M. To, K. K. L. Moon, L. K. Chan, P. K. W. Yeung, and M. C. M. Lee, "RFID Systems implementation: A comprehensive framework and a case study," *International Journal of Production Research*, vol. 48, no. 9, pp. 2583–2612, 2010.

[84] F. Niederman, R. G. Mathieu, R. Morley, and I.-W. Kwon, "Examining RFID applications in supply chain management," *Communications of the ACM*, vol. 50, no. 7, pp. 92–101, 2007.

[85] Y. Rekik, E. Sahin, and Y. Dallery, "Analysis of the impact of the RFID technology on reducing product misplacement errors at retail stores," *International Journal of Production Economics*, vol. 112, no. 1, pp. 264–278, 2008.

[86] M. Rieback, B. Crispo, and A. Tanenbaum, "Keep on blockin' in the free world: Personal access control for low-cost RFID tags," in *International Workshop on Security Protocols — IWSP'05*, Cambridge, England: Springer-Verlag, April 2005.

[87] A. Sarac, N. Absi, and S. Dauzere-Peres, "A literature review on the impact of RFID technologies on supply chain management," *International Journal of Production Economics*, vol. 128, no. 1, pp. 77–95, 2010.

[88] K. Sari, "Exploring the impacts of radio frequency identification (RFID) technology on supply chain performance," *European Journal of Operational Research*, vol. 207, no. 1, pp. 174–183, 2010.

[89] P. Schmitt and F. Michahelles, "Economic impact of RFID report," http://www.bridge-project.eu/, 2008.

[90] A. U. Smart, R. Bunduchi, and M. Gerst, "The costs of adoption of RFID technologies in supply networks," *International Journal of Operations & Production Management*, vol. 30, pp. 423–447, 2010.

[91] A. D. Smith, "Exploring the inherent benefits of RFID and automated self & serve checkouts in a B2C environment," *Int. J. Bus. Inf. Syst.*, vol. 1, no. 1/2, pp. 149–181, 2005.

[92] S. Spiekermann and O. Berthold, "Maintaining privacy in RFID enabled environments — proposal for a disable-model," in *Privacy, Security and Trust within the Context of Pervasive Computing*, (P. Robinson, H. Vogt, and W. Wagealla, eds.), Springer Verlag, 2005.

[93] P. Spiess, "Collaborative business items: Decomposing business process services for execution of business logic on the item," in *European Workshop on Wireless Sensor Networks*, 2005.
[94] J. Struker, S. Sackmann, and G. Müller, "Case study on retail customer communication applying ubiquitous computing," in *CEC '04: Proceedings of the IEEE International Conference on E-Commerce Technology*, pp. 42–48, Washington, DC, USA: IEEE Computer Society, 2004.
[95] S. M. Swartz, V. Vaidyanathan, and H. Raman, "A post-retail consumer application of RFID in medical supply chains," *Journal of Business and Industrial Marketing*, vol. 25, no. 8, pp. 607–611, 2010.
[96] C. Swedberg, "Hong Kong shoppers use RFID-enabled mirror to see what they want," http://www.rfidjournal.com/article/view/3595, September 2007.
[97] C. Tellkamp, "The Auto-ID calculator: An overview," Technical Report, Auto-ID Centre, 2003.
[98] F. Thiesse, J. Al-Kassab, and E. Fleisch, "Understanding the value of integrated RFID systems: A case study from apparel retail," *European Journal of Information Systems*, vol. 18, no. 6, pp. 592–614, 2009.
[99] F. Thiesse and C. Condea, "RFID Data sharing in supply chains: What is the value of the EPC Network?," *International Journal of Electronic Business*, vol. 7, no. 1, pp. 21–43, 2009.
[100] F. Thiesse and E. Fleisch, "On the value of location information to lot scheduling in complex manufacturing processes," *International Journal of Production Economics*, vol. 112, no. 2, pp. 532–547, 2008.
[101] M.-C. Tsai, W. Lee, and H.-C. Wu, "Determinants of RFID adoption intention: Evidence from Taiwanese retail chains," *Information and Management*, vol. 47, no. 5-6, pp. 255–261, 2010.
[102] S.-F. Tzeng, W.-H. Chen, and F.-Y. Pal, "Evaluating the business value of RFID: Evidence from five case studies," *International Journal of Production Economics*, vol. 112, no. 2, pp. 601–613, 2008.
[103] A. Ustundag, "Evaluating RFID investment on a supply chain using tagging cost sharing factor," *International Journal of Production Research*, vol. 48, no. 9, pp. 2549–2562, 2010.
[104] A. Ustundag and M. Tanyas, "Evaluating an RFID investment using fuzzy cognitive map," Technical Report, Technical University — RFID Research & Test Center, Istanbul, 2005.
[105] S. Veronneau and J. Roy, "RFID benefits, costs, and possibilities: The economical analysis of RFID deployment in a cruise corporation global service supply chain," *International Journal of Production Economics*, vol. 122, no. 2, pp. 692–702, 2009.
[106] J. K. Visich, S. Li, B. M. Khumawala, and P. M. Reyes, "Empirical evidence of RFID Impacts on supply chain performance," *International Journal of Operations and Production Management*, vol. 29, no. 12, pp. 1290–1315, 2009.
[107] S. F. Wamba and H. Boeck, "Enhancing information flow in a retail supply chain using RFID and the EPC network: A proof-of-concept approach," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 3, no. 1, pp. 92–105, April 2008.

[108] S. F. Wamba, L. A. Lefebvre, Y. Bendavid, and E. Lefebvre, "Exploring the impact of RFID technology and the EPC network on mobile B2B eCommerce: A case study in the retail industry," *International Journal of Production Economics*, vol. 112, no. 2, pp. 614–629, 2008.

[109] S. F. Wamba, L. A. Lefebvre, and E. Lefebvre, "Enabling intelligent B-to-B eCommerce supply chain management using RFID and the EPC network," in *Proceedings of the 8th International Conference on Electronic Commerce (ICEC '06)*, pp. 281–288, 2006.

[110] H. Wang, S. Chen, and Y. Xie, "An RFID-based digital warehouse management system in the tobacco industry: A case study," *International Journal of Production Research*, vol. 48, no. 9, pp. 2513–2548, 2010.

[111] S.-W. Wang, W.-H. Chen, C.-S. Ong, L. Liu, and Y.-W. Chuang, "RFID application in hospitals: A case study on a demonstration RFID project in a Taiwan hospital," in *HICSS '06: Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, p. 184.1, Washington, DC, USA: IEEE Computer Society, 2006.

[112] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *Security in Pervasive Computing*, pp. 201–212, 2004.

[113] S. Whang, "Timing of RFID adoption in a supply chain," *Management Science*, vol. 56, no. 2, pp. 343–355, 2010.

[114] J. Whitaker, S. Mithas, and M. S. Krishnan, "A field study of RFID deployment and return expectations," *Production and Operations Management*, vol. 16, pp. 599–612, 2007.

[115] T. Wilde and T. Hess, "Forschungsmethoden der Wirtschaftsinformatik — Eine empirische Untersuchung," *Wirtschaftsinformatik*, vol. 4, pp. 280–287, 2007.

[116] L. D. Xu, "Information architecture for supply chain quality management," *International Journal of Production Research*, vol. 49, no. 1, pp. 183–198, 2011.

[117] W. Zhou, "RFID and item-level information visibility," *European Journal of Operational Research*, vol. 198, no. 1, pp. 252–258, 2009.