Chapter 3
Autonomous Control in Logistics

Supply network management aims at balancing supplies and demands between suppliers and consumers (Section 2.1). This is a challenging task due to the complexity, the dynamics, and the distribution that are inherent in logistics processes (Section 2.3). The autonomous logistics paradigm addresses these challenges by applying local control rather than centralised decision-making. To this end, each of the participating logistics entities is itself responsible for satisfying its predefined logistics objectives. Delegating both the autonomy and the ability to make decisions to the logistics objects coincides with the natural distribution observed in logistics. The advantages over previous methods are as follows. Firstly, it is possible to react locally on exceptions. It is thus not necessary to re-schedule the whole system which might even be impossible due to the complexity and the dynamics. Secondly, it is not necessary to reveal internal information and decision processes to a central entity. This is important if competing companies cooperate only in particular processes. Thirdly, handling standard processes and reacting on exceptions is still possible in cases of physical distribution with limited or even without communication bandwidth.

The objective of this chapter is to present the paradigm of autonomous control in logistics. Section 3.1 describes how this approach allows decreasing the complexity and coping with the dynamics and the distribution that are inherent in logistics processes. Based on this foundation, Section 3.2 introduces an architecture for logistics entities that are capable of decentralised control. In doing so, the technologies enabling autonomous control in logistics are examined. The objective of this investigation is to underline the particular importance of Distributed Artificial Intelligence in supply network management.

A. Schuldt, *Multiagent Coordination Enabling Autonomous Logistics*,
DOI 10.1007/978-3-642-20092-2_3,

3.1 Paradigm Shift to Autonomous Control

Conventionally, supply network management is conducted from a centralised perspective. A central unit makes all decisions for planning and controlling logistics processes. This is a challenging task due to the high number of participants and parameters to be considered (Section 2.2.1). Furthermore, the complexity and the dynamics even increase due to new requirements on logistics (Section 2.2.2). These developments limit and sometimes even prevent centralised control. Instead, the paradigm of autonomous control in logistics, in short autonomous logistics, is a promising approach. Autonomous logistics aims at overcoming the limitations of conventional control in logistics by delegating decision-making to local entities (Herzog, Freitag & Scholz-Reiter, 2005, p. 222). The logistics entities are themselves responsible for satisfying the logistics objectives defined by their owners.

The general idea of autonomous control in logistics is presented in Section 3.1.1. It is particularly contrasted with conventional centralised control in order to examine how the new paradigm overcomes the limitations of centralised control. Based on this foundation, Section 3.1.2 investigates the potential for autonomous control in supply network management. Finally, limitations of autonomous logistics are discussed in Section 3.1.3.

3.1.1 Decentralised Decision-Making in Logistics

Following the discussion in Section 2.3, challenges for supply network management are the complexity, the dynamics, and the distribution that are inherent in logistics processes. The paradigm of autonomous control in logistics addresses the natural distribution of logistics processes by delegating decision-making to local entities (Figure 3.1). The term logistics entity denotes in this context both the material transformed as well as the facilities applied for transforming the material (Scholz-Reiter, Windt & Freitag, 2004, p. 362). That is, both providers and consumers of logistics services are considered active participants in the process (Hellenschmidt & Wichert, 2007, p. 99). Decentralised decision-making means that the local logistics entities are themselves responsible for achieving their logistics objectives (Section 2.1). For instance, consider a shipping container that is currently located in East Asia and that has to be transported to Europe. Being an active participant in the process, the container must then plan and schedule its route through the logistics network by itself. In order to be capable of this proactive behaviour, it is necessary to grant the respective autonomy to the shipping container. This particularly includes the permission to interact and to cooperate with other logistics entities in order to achieve its logistics objectives (Hellenschmidt & Wichert, 2007, p. 99).

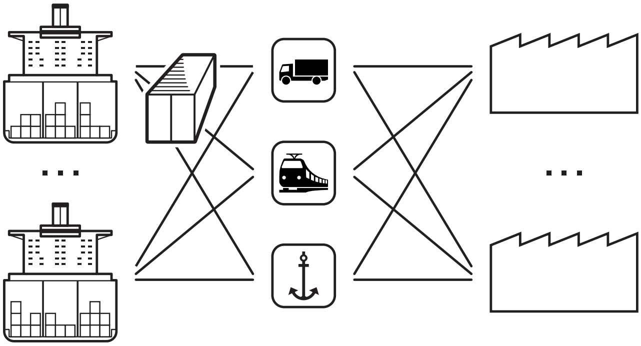

Fig. 3.1 An autonomous shipping container having sole responsibility for planning and scheduling its way through the logistics network. The container must cooperate with other entities such as means of transport and warehouses to achieve the logistics objectives imposed by the cargo owner.

Services provided by other entities like container vessels or trucks include transporting the container from its source to a sink. Other containers need the same resources. Hence, they compete for the logistics services offered. Because no central entity exists, containers and means of transport must themselves negotiate on the transport. In contrast to conventional centralised control, no hierarchy or structure is predefined on the logistics objects (Freitag, Herzog & Scholz-Reiter, 2004, p. 24). Instead, they flexibly interact based on their actual demands in a heterarchical way. Hence, the understanding of autonomous logistics here agrees with Windt and Hülsmann (2007, p. 8):

> "Autonomous Control describes processes of decentralized decision-making in heterarchical structures. It presumes interacting elements in non-deterministic systems, which possess the capability and possibility to render decisions.
>
> The objective of Autonomous Control is the achievement of increased robustness and positive emergence of the total system due to distributed and flexible coping with dynamics and complexity."

The idea of autonomous control in logistics is thus closely linked with the idea of self-organisation. Köhler-Bußmeier (2009) gives a general overview on the foundations of self-organisation. Hülsmann, Wycisk, Agarwal and Grapp (2007) particularly focus on aspects that underly autonomous logistics. An overview on the development of self-organisation in both information and communication technology is given by Becker, Kuladinithi, Timm-Giel and Görg (2007).

Autonomous control in logistics has several advantages over centralised approaches. Distributing decision-making to local entities coincides with the natural distribution of logistics processes discussed in Section 2.3.3. Proceeding this way particularly circumvents that all relevant information must be provided to a central decision-making entity (Freitag et al., 2004, p. 23). This step is no longer necessary because decisions are made locally. Control is therefore even possible without a permanent communication connection to a central entity. Apart from spatial distribution, also processes that cross company boundaries do not pose a problem. It is no longer necessary to disclose confidential information or reasons for decision-making. Instead, communication reduces to transmitting decisions taken directly by the local logistics entities.

The heterarchical organisation without a predefined structure of logistics entities allows reacting locally on dynamics occurring. Instead of updating the plan for the whole system, as it would have been necessary if centralised control was used, it is sufficient to modify only the plans of the entities that are directly affected. Decomposing problems into subproblems is a common approach in computer science, generally referred to as divide and conquer. Correspondingly, distributing control in logistics also decreases the problem complexity because each entity only has to consider its particular parameters (Windt, 2008, p. 352). This means a significant reduction of problem complexity compared to the centralised approach that incorporates all parameters of the whole system. With a limited number of parameters even problems with high computational complexity become manageable. As a further advantage, individual entities are only exposed to local dynamics and not to the dynamics of the whole logistics network (Windt, 2008, p. 352). A disadvantage, however, is that global optima are not necessarily achieved with decentralised control. For a more comprehensive discussion on global optima in supply networks, the reader is referred to Section 2.3.3.

Scholz-Reiter et al. (2004) divide logistics systems into three layers, namely the decision system, the information system, and the execution system (Figure 3.2). The execution system layer is already automatised to a high degree. Also autonomous systems have been successfully applied to this level. Think, for instance, of automated guided vehicles (AGV) which navigate through the real world (Schuldt & Gottfried, 2008a, 2008b). Examples can be found in intralogistics, e. g., in order to supply workshops and workplaces with material or to handle containers in automated container terminals. However, automated execution of primary logistics functions pertains rather to the field of robotics. In accordance with the general understanding of logistics (Chapter 2), also the notion of autonomous logistics used in this research focuses on planning and controlling processes instead of executing physical operations.

As illustrated in Figure 3.2, the decision and information system layers are currently less automatised. Hence, there is still potential for autonomously controlled technical systems. Applications for autonomous control in logistics can be found in all parts of the supply network. In procurement logistics, the intelligent container (Jedermann, Gehrke et al., 2007) is a novel application for autonomous logistics. This shipping container continuously monitors its content. In case of unexpected changes of the interior temperature or other parameters, the container can itself change its route or destination. This ensures that food loaded can still be sold and consumed before its shelf life is exceeded.

In production logistics, autonomous control can be applied to decrease the complexity of warehouse control (Trautmann, 2007). In distribution logistics, routing algorithms from computer and communication networks are applied to route packages through networks of courier, express, and parcel service providers (Wenning, Rekersbrink, Timm-Giel, Görg & Scholz-Reiter, 2007). Similar methods combine novel and conventional, i. e., centralised approaches (Berning & Vastag, 2007; Vastag, 2008).

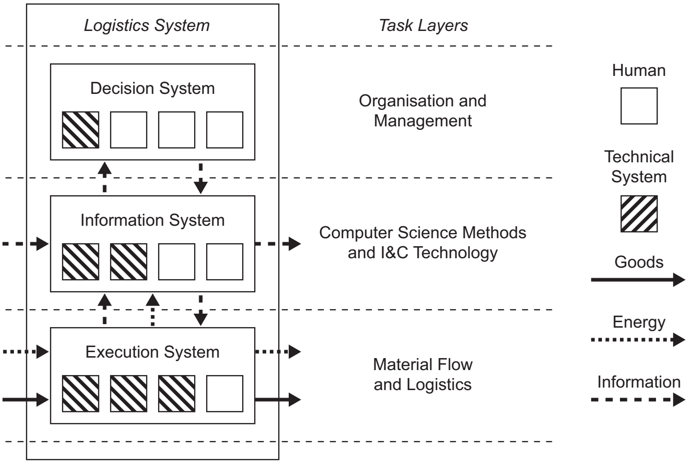

Fig. 3.2 The task layers in logistics divide into execution system, information system, and decision system. The execution level is already automatised to a high degree. By contrast, on the upper levels there is still potential for technical systems (adapted from Scholz-Reiter et al., 2004, p. 360).

3.1.2 Potential for Autonomous Control

The autonomous logistics approach aims at delegating decision-making to local logistics entities. In order to be able to make decisions on their own, these entities must have certain capabilities. Apart from the Artificial Intelligence to take the decisions themselves, they need identification and communication capabilities for interaction with other entities. In order to monitor their current state, they must be capable of localising themselves and sensing their environment. It is quite obvious that current logistics entities like cardboard boxes, pallets, containers, or trucks do not exhibit these capabilities. In order to implement autonomous control in logistics it is thus necessary to enhance them with the respective technologies required.

Augmenting physical objects with computational ability is possible because the miniaturisation observed in Section 2.2.2 does not only apply to the goods handled. It also has reduced the size of processors and related computer units (Hellenschmidt & Wichert, 2007, p. 94). According to Moore's law, the number of electronic components that can be placed on an integrated circuit doubles every 18 to 24 months (Moore, 1965, p. 115). That is, after this period the same computational power can be achieved with half the size. It turns out that this forecast is still accurate today. Interestingly, Moore's law does not only hold for processors but is also applicable for other technologies such as memory or communication bandwidth (Mattern, 2005, p. 43). However, Mattern (2005, p. 43) points out that Moore's law is eventually restricted by both physical and economical limitations.

Enhancing objects from the physical world as well as enhancing the physical environment is generally denoted by one of the following terms:

- Ubiquitous Computing
- Pervasive Computing
- Ambient Intelligence

Mattern (2005, p. 41) explains that the distinction between these terms is to a large extent an academical one. According to him, ubiquitous computing is a term that is mainly used as a vision for future developments. By contrast, the notion of pervasive computing is rather used by industry referring to solutions that can already be implemented today. While these terms are mainly used in North America, European scientists developed the notion of ambient intelligence which has a particular focus on human-machine interaction. These approaches have in common that they aim at assisting humans by Artificial Intelligence in the environment and interaction between physical objects, as in the case of autonomous logistics. Methods from Artificial Intelligence can be implemented on embedded systems that are attached to the physical object. Wöstmann (2006, p. 49) describes that RFID tags can even be integrated into cast components. Section 3.2 provides a more comprehensive overview on the key technologies enabling autonomous logistics.

3.1.3 Limitations of Autonomous Control

Autonomous control helps reduce the complexity of supply network management. Delegating decision-making to local logistics entities allows coping with both the dynamics and the distribution that are inherent in logistics processes. Therefore, it seems tempting to implement autonomous control at a very fine granular level. That is, to enhance every single article with the capability to make its own decisions. These articles are then expected to jointly control the logistics processes they are participating in. At first glance, this might seem the best strategy for reducing the complexity and for coping with the dynamics and the distribution. However, not only conventional centralised control is limited in its applicability. There are also limitations for autonomous logistics. Therefore, it is necessary to choose an adequate level at which autonomous control is applied (Windt, 2008, p. 350). Limitations that have to be considered for this choice are of technological, economical, and legal nature.

A limitation from the technological point of view is the computational power of autonomous entities. A particular question is which computational power can be expected with decreasing size of logistics entities. Embedded systems on comparatively small logistics entities, such as articles or packages, are rather limited in the power available. Power in this context not only refers to processor and memory, but also to the energy that can be consumed. Energy supply for mobile entities is generally implemented by battery. This is challenging because the miniaturisation of batteries does not keep up with the miniaturisation of processors (Mattern, 2005, pp. 42–43). Thus, energy must be used sparingly, i. e., computations should be reduced to a minimum. However, energy is not the only source of restriction to computational power. Furthermore, also the size of processor and memory is limited if the embedded system is affixed on small logistics entities. Limited memory demands efficient handling of knowledge acquired. Additionally, limited processing power requires knowledge bases to be kept manageable (Werner, Schuldt & Daschkovska, 2007, p. 15), particularly for complex reasoning tasks. This illustrates that with decreasing size of logistics entities also the number of computations that can be conducted decreases. Bigger entities, like warehouses, may have more processing power and are less limited regarding energy consumption. Nevertheless, it is worth remembering that also these entities are constrained by the asymptotical computational complexity (Section 2.3.1).

In addition to computational and energy considerations, interaction complexity is another potential limitation in autonomous logistics applications (Schuldt & Werner, 2007, p. 130). The more decision-making is distributed from one or few central to many local entities, the more communication is required for coordination. Therefore, it is important to categorise coordination mechanisms in accordance with the number of messages to be expected in relation with the number of participating entities. For this purpose, the complexity classes presented in Section 2.3.1 are applied accordingly. This allows comparing different approaches regarding their practical applicability. Interaction efforts depend on both the interaction complexity and the number of participants. Therefore, it is important to keep also the number of participating entities manageable in order to prevent a communication overhead. Otherwise, the decreased computational complexity of decentralised approaches is outweighed by the increased interaction complexity.

Apart from technological considerations also the economical perspective must be taken into account. The costs for components required to implement embedded systems for autonomous logistics are decreasing (Mattern, 2005, pp. 39, 42). Nevertheless, it is necessary to determine an acceptable granularity at which autonomous control is implemented. Enhancing every single article with the capability of decision-making requires providing these articles with the respective computational power. But many logistics applications do not require control on this fine granular level. Instead, it is often sufficient to stay on a coarser level where, for instance, a cardboard box or pallet is responsible for controlling all goods loaded. It might even be appropriate to implement autonomous control on the granularity of larger load carriers or means of transport such as containers or trucks.

From the discussion so far follows that the degree of granularity at which autonomous control in logistics is applied is important from both the technological and the economical perspective. The degree of granularity determines which logistics entities are capable of autonomous control. Apart from that, the degree of autonomy granted to logistics entities also is an important factor. On the one hand, this includes the temporal scope of their decisions, which may be operational, tactical, or strategic (Timm, 2006, pp. 7–11). On the other hand, the autonomy granted is closely linked with the degree of freedom for the decisions to be made. For instance, consider a shipping container that is transported by container vessel from East Asia to Europe. Due to a delay the container will not meet the estimated time of arrival. Depending on the autonomy granted the shipping container may itself initiate transshipping its cargo to an airplane. But transporting goods by airplane is significantly more expensive than delivering them by container vessel. Therefore, one might demand the autonomous container to consult a human dispatcher for this decision. Several legal aspects are closely linked with the autonomy granted to logistics entities (Nitschke, 2006, pp. 597–610). These include questions whether declarations of autonomous entities are legally effective and who is responsible in the case of misconduct. In this context, Matthias (2008) investigates under which circumstances intelligent autonomous entities might even be themselves accountable for their actions.

To summarise, the application of autonomous logistics is restricted by the degree of granularity at which autonomous control is applied and the degree of autonomy granted to logistics entities. The degree of granularity can be approached from both the technological and the economical point of view. It is thus necessary to find an appropriate level for the concrete logistics problem addressed. Thereby, it is important that increased cost and interaction complexity do not outweigh the decrease in computational complexity. Furthermore, the freedom in decision-making has to be defined in advance in order to implement a reasonable restriction in the autonomy granted to logistics entities.

3.2 Technologies Enabling Autonomous Control

Autonomous control of logistics processes means delegating decision-making to local entities. In order to implement the intelligent logistics entities required, new information and communication technologies have to be integrated (Section 3.1.2). Figure 3.3 proposes an architecture of the technologies demanded by autonomous logistics entities.

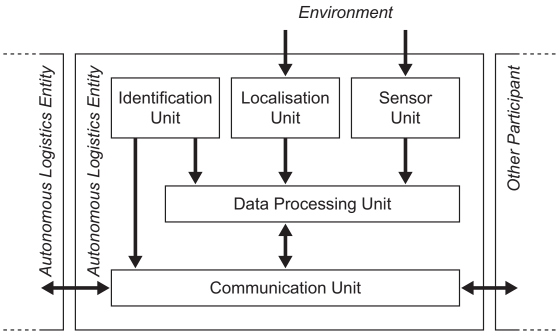

Fig. 3.3 Architecture for autonomous logistics entities. Enabling technologies include identification, localisation, and sensor technology, communication networks, and data processing.

In order to control a logistics process by a computer system, it is necessary to establish a link between the real world and the system. This holds for both centralised and decentralised approaches. Within the architecture presented, the identification unit provides the means to uniquely identify logistics entities (Section 3.2.1). To enable tracking and tracing of the goods transported, the localisation unit monitors the current location of the logistics entity (Section 3.2.2). For many applications, such as in the fresh food supply chain, it is additionally necessary to continuously monitor the condition of the cargo. The corresponding data about the logistics entity, its content, and its environment is contributed by the sensor unit (Section 3.2.3). Solving logistics tasks alone is only sufficient in special cases. Generally, autonomous entities have to cooperate with others, for instance, to negotiate on transport or storage capacities. Such interaction with other autonomous entities or other participants like humans is enabled by the communication unit (Section 3.2.4). Finally, the data processing unit (Section 3.2.5) integrates all incoming sensor data from the environment and coordinates interaction with the outside world.

The data processing unit is the central part of autonomous logistics entities because it has to actually implement the intelligence for the logistics object it represents. Like the data processing unit, the communication unit also is an essential part of the architecture. Without this unit, communication, and thus coordination, with other entities would be impossible. Likewise, the identification unit is indispensable because it provides the autonomous logistics entity with a unique identity. Its identifier can, for instance, be used by others to reason about the autonomous logistics entity and in order to address messages intended for it. Note that the identification unit has a direct link with the communication unit. Identification of objects is a frequent task in logistics, e. g., during shipping or receiving. Although access to identification information may be restricted, this restriction is generally not a task requiring intelligence. Thus, the design of the architecture enables identifying objects even without incorporating the data processing unit.

Localisation and sensor technology are also important in autonomous logistics. Nevertheless, these parts may be absent in autonomous logistics entities if the information can be acquired otherwise. As an example, consider a shipping container that monitors its interior and provides all packages loaded with the measurements obtained by its sensors. Another example incorporates a truck that takes responsibility for localisation for all logistics entities loaded. Then, the communication unit acts as a surrogate for the missing parts of the architecture. If also the data processing unit was replaced by the communication unit, one would arrive at centralised instead of autonomous control. The following sections provide a more detailed overview on the enabling technologies for autonomous logistics. Requirements for logistics and conventional solutions are discussed. Subsequently, more recent developments allowing the implementation of autonomous logistics entities in accordance with the architecture proposed are introduced.

3.2.1 Identification

Identification technology is the key aspect in order to synchronise information flows with their respective material flows. It is required in order to establish a link between real-world entities and their representation by computer-based control systems (Lampe, Flörkemeier & Haller, 2005, p. 69). Identification enables computer systems to become aware of movements and status changes of logistics entities. This allows reacting appropriately on changes in the real world. Approaches to identification are already applied today. The following paragraphs introduce two conventional systems and discuss their limitations. Based on this foundation, an innovative approach and its application to autonomous logistics is presented.

As a first example consider shipping containers. According to ISO standard 6346, each shipping container can be identified by a sequence of eleven characters and digits (Figure 3.4). The first three characters represent a code referring to the owner of the container. The fourth character is the product group code identifying the type of the equipment. The subsequent six digits form the serial number that is unique for all containers of one shipper. Finally, a check digit prevents data acquisition errors during handling.

The identification number is affixed as a marking on the surface of the container, either in horizontal or vertical orientation. Whenever a container is handled, for instance during loading or unloading, its identification number has to be recorded. Currently, this is mainly done manually which means a discontinuity of the information flow. Image processing methods constitute an alternative in that they support automated optical character recognition (OCR). Unfortunately, applying OCR in the shipping container domain is rather challenging. This can be explained by several reasons. Firstly, shipping containers have a large surface on which the marking may be affixed. This results in large-scale scans in order to find the marking. An effective scan requires a certain distance from the container. This requirement can often not be satisfied due to the narrow storage spaces of container terminals. Secondly, during maritime transport, shipping containers are directly exposed to the forces of nature. This results in dirt and abrasion which aggravate correct character recognition. Finally, illumination and weather conditions in the container terminal pose additional problems. Hadow (2005, p. 58) points out that current optical character recognition system achieve only a recognition rate of about 80% under these real-world conditions. This rate is far from being acceptable for professional applications.

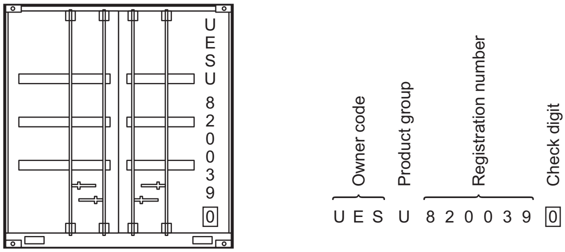

Fig. 3.4 According to ISO 6346, shipping containers are identified by markings on their surfaces. These markings are built up by human-readable sequences of characters and digits.

Another example for identification of real-world objects is the International Article Number EAN (Vahrenkamp, 2007, p. 60), formerly European Article Number. An EAN consists of 13 digits (Figure 3.5 left), for small-sized products a special version with only eight digits exists. EAN-13 is started by a Global Location Number (GLN) company prefix which allows identifying companies uniquely. The company prefix is five to seven digits in length. It is assigned by the Global Standards One (GS1) company. The remaining digits can be used by the respective company as a serial number for their products. The last digit serves as a check digit to ensure the validity of the code. EAN-13 codes are generally printed as a bar code on the respective packaging. Such article numbers identify articles as members of a certain article group. This allows, for instance, simply scanning the bar code at a point of sale in order to find out its price. Likewise, the entry of the respective article group in the inventory control system can be decremented by one when an article is sold. Coupled with automated replenishment, this allows keeping supplies coming.

A shortcoming, however, is that it is impossible to distinguish shipping units of the same article group during transport just by their EAN. All shipping units containing the same type of articles have the same EAN because the EAN always pertains to a whole group of articles. This problem is addressed by the Serial Shipping Container Code (Vahrenkamp, 2007, p. 60), in short SSCC, a numerical identifier with 18 digits. Following an extension digit, SSCC starts with the GLN company prefix like EAN-13 (Figure 3.5 right). The following digits minus the check digit can be assigned by the respective company itself. This allows, for instance, identifying complete shipping units like pallets. While identification on this level may be sufficient for some applications, it is not for all of them. Cardboard boxes on pallets may be re-packed on their way through a logistics network. Without unique identifiers for each cardboard box, it is impossible to implement a continuous monitoring, e. g., of the cold chain. Furthermore, a reliable permanent stocktaking is impossible without identification on the article level. Another shortcoming results from the bar code representation. The bar code has to be scanned each time a shipping unit is handled. Scanning is often carried out manually which again results in an information flow discontinuity. Furthermore, bar code scanning requires visual contact. As an example, this prevents cardboard boxes located on a pallet from being scanned when they are occluded by other cardboard boxes. Further challenges result, like in the shipping container example, from dirt and abrasion.

Fig. 3.5 EAN-13 (left) and SSCC (right) are intended to encode article numbers and numbers of shipping units, respectively. Both of them contain started by the GLN company prefix of their company. The application identifier 00 is part of the EAN128 bar code encoding standard for SSCC.

To summarise, the shortcomings of the current solutions presented above are as follows. Shipping units are mainly identified by non-digital codes. Dealing with analogue representations results in a discontinuity of the information flow because, in general, they have to be acquired manually. Automatic recognition is a hard task due to dirt, abrasion, poor illumination, and occlusion. Furthermore, identification is currently only applied on a high level of granularity of shipping units which is not sufficient for some applications. These issues are addressed by radio-frequency identification (RFID) which aims at automated identification without direct physical or visual contact, thereby avoiding information flow discontinuities (Lampe et al., 2005, p. 69). RFID tags consist of three components: a serial number identifying the object the tag is attached to, a transponder for wireless communication, and a microchip as data storage.

A standard to format serial numbers is the Electronic Product Code, in short EPC. Today, it is most commonly used with at least 96 bits in length. This length allows identifying single objects uniquely; reading serial numbers of this length does not pose a problem because it is done automatically. Nevertheless, the actual granularity at which objects are marked still depends on the demands imposed by the application at hand and the cost (Section 3.1.3). Originally, EPC was intended to be universally applicable for arbitrary applications in arbitrary domains (Flörkemeier, 2005, p. 90). This, however, is contradictory to existing industry standards. Thus, companies involved in the EPC standardisation process demanded to create customised sub-standards that are in compliance with existing formats like EAN (Flörkemeier, 2005, p. 90). Kuhlmann and Masuhr (2007, p. 257) explain that the intention is to protect previous investments and to support a smooth transition from bar codes to EPC. The EAN-based derivate of EPC is structured as follows. A header defines the format used. It is followed by a filter value that identifies the type of the load carrier, e. g., whether it is a pallet or cardboard box. A partition field defines where to divide the subsequent company prefix and item reference. Company prefix and item reference correspond to the EAN identifier. Finally, the serial number identifies single objects uniquely. In general, it is also possible to store additional data on RFID tags. Nevertheless, this is often avoided in order to save costs by keeping RFID tags simple. Instead, the EPC can be used as a reference in order to retrieve additional data (Flörkemeier, 2005, p. 89).

The EPC that is stored on an RFID tag can be readout with RFID readers. The energy supply for both transponder and microchip can either be passive, semi-active, or active (Lampe et al., 2005, p. 73). The first group of tags exclusively uses the energy field induced by the reader. Semi-active have an internal battery for the microchip, the transponder is served by the reader. In contrast, the energy supply of active tags is completely covered by their internal battery. Bulk scanning currently allows to read up to 400 transponders per second (Kuhlmann & Masuhr, 2007, p. 258). Different load carriers can be distinguished by the EPC filter value. This allows defining the level of granularity at which to scan, e. g., only pallets or cardboard boxes. Signal collisions may occur during bulk scan if multiple transponders respond in parallel. Such collisions can be prevented either by deterministic or probabilistic methods (cf. Lampe et al., 2005, p. 73).

While EPC and RFID enable the unique identification of objects, it is still necessary to link them to their representations in computer systems. For this purpose, the Internet of Things (Fleisch & Mattern, 2005; Bullinger & ten Hompel, 2007) aims at extending the common internet to objects in the real world (Figure 3.6). Therefore, all relevant objects are equipped with an RFID tag carrying the respective EPC identification. The connection to software applications is as follows (Flörkemeier, 2005, p. 89). Applications can access the EPC identification stored on the RFID tag either directly via the RFID reader or through a middleware. This middleware allows, for instance, filtering and bundling data streams with RFID tags. The EPC is only for identification purposes and does rarely provide any additional information about the object scanned. Additional information can be retrieved from an EPC Information Service (EPC IS). To avoid bottlenecks, there exists no central EPC Information Service. Instead, Information Services may be distributed, e. g., one for each company. An Object Naming Service (ONS) can be contacted in order to find out which EPC IS administers a real-world object. Hence, the ONS corresponds to the Domain Name Service (DNS) on the common internet.

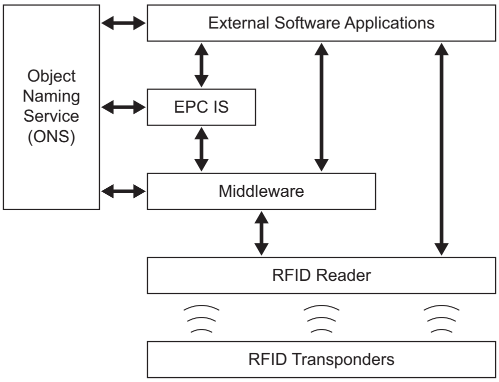

Fig. 3.6 The Internet of Things infrastructure encapsulates access to RFID tags by a middleware. The middleware queries the Object Naming Service (ONS) for EPC Information Services that provide additional information on the object scanned (adapted from Flörkemeier, 2005, p. 89).

EPC and RFID enable identifying objects more reliably and with less effort than previous systems. The information flow discontinuity of previous systems is abolished by wireless digital communication. Dirt and abrasion of bar codes no longer pose a problem, recognition rates are beyond 99% (Hadow, 2005, p. 58). In order to protect them from environmental influences it is possible to embed RFID tags into products or load carriers (Lampe et al., 2005, p. 70) and even cast components (Wöstmann, 2006, p. 49). This is possible because no visual contact is required. However, note that certain limitations exist because radio signals are attenuated, for instance, by metal and water. Lampe et al. (2005, p. 69) list the following advantages of RFID: decreased error rates, increased process efficiency, increased product quality, as well as cost saving by faster and better information processing. Example applications that can be implemented with identification technology include tracking lots through a factory or supply network as well as permanent stocktaking (Thiesse, 2005, pp. 114 –115). In autonomous logistics, electronic identification allows logistics entities becoming aware of both their own identity and the identity of other entities.

3.2.2 Localisation

Tracking and tracing goods is an important application in logistics (Scholz-Reiter, Toonen & Windt, 2008, pp. 596–597) to make logistics processes transparent to customers. Therefore, cargo owners are provided with a continuous visibility of their goods. Tracking in this context refers to the discrete or continuous localisation of goods. Tracing is the process of analysing and archiving the data records. The automatised identification of goods is one of the key technologies to implement tracking. However, it is usually not sufficient so that there is a demand for additional technology. This section outlines applications in logistics and different approaches to implement them.

In the courier, express, and parcel (CEP) business, it is quite common to provide customers with tracking and tracing services. These services are generally implemented by periodically scanning identification labels affixed to the packages transported (Cardeneo, 2008, pp. 787–788). The first time the CEP provider gets in contact with a package is when it is collected from the customer (Figure 3.7). The package is scanned for the first time then. Afterwards, the identification is recorded each time the package enters or leaves a hub. Finally, the package is also scanned when it is delivered to its recipient. In this context, identification is conventionally implemented with bar codes (Cardeneo, 2008, pp. 787–788). The temporal resolution of this localisation method is rather limited and allows only locating packages coarsely within the logistics network. Nevertheless, it is still sufficient to find out who is currently in charge of the shipment. Whenever a package should get lost during the transport process, this periodical scanning still allows determining the person responsible, e. g., for reimbursement. A more elaborate solution employs RFID and EPC, thereby enabling automated identification by radio-frequency scanning without visual contact (Section 3.2.1). Handling effort is massively reduced because bulk scanning can be applied.

Scholz-Reiter et al. (2008, p. 596) argue that tracking and tracing can also improve other transport processes. In particular, they mention intermodal transport which often involves several logistics providers in multiple countries. Hitherto, cargo owners normally lost contact with their shipping containers with pre carriage. The containers remained invisible until their arrival at the final destination. This is dissatisfying for several reasons. Firstly, like in the CEP domain, responsibility is an important issue. In particular, if potentially untrustworthy partners participate in the process, one must be able to trace

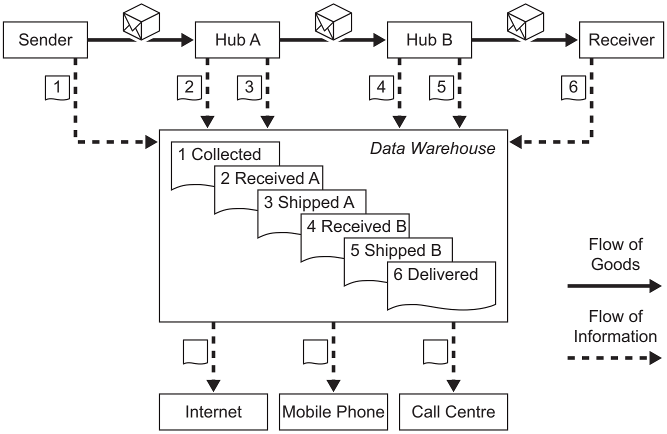

Fig. 3.7 Tracking and tracing in the courier, express, and parcel business. Packages are scanned when they are collected and delivered as well as when entering or leaving a hub in between (adapted from Cardeneo, 2008, p. 787).

responsibility if a shipping container is lost. However, the complete loss of containers is only the worst case. Secondly, without tracking and tracing it is impossible to reliably predict the time of arrival for shipping containers. This is due to the fact that delays may occur during transport. These delays may be caused, for instance, by bad weather conditions or overbooked container vessels. Therefore, tracking and tracing helps improve planning of production processes. If it is known in advance that cargo arrives late, production plans can be updated accordingly. An autonomous logistics entity might even reschedule its transport to a faster means of transport (Section 3.1.1). If the cargo is required on time, it might, for instance, be appropriate to change from container vessel to airfreight.

To enable such decisions in a timely manner it is necessary to implement localisation with high temporal resolution. Continuous updates of the cargo location are required. Pflaum and Hupp (2007, p. 109) point out that even RFID does not provide enough precision and therefore does retain one of the problems identified when bar codes are used. It is only possible to use RFID base stations as a beacon in order to find out whether or not a tag is located near a station. Localisation therefore requires a close-meshed network of base stations. In intralogistics, it is often no problem to install the readers required to enable at least periodic monitoring (Lampe et al., 2005, p. 70). But tracking RFID tags in transport logistics is significantly more challenging due to the long-range spatial distribution. A potential solution might include scanning EPC codes of cargo at each highway overpass (Hadow, 2005, p. 58). Similar solutions are already applied in order to track the movement of rail cars (Gallagher, 2002, p. 48). However, this has some disadvantages. Firstly, it is still necessary to install lots of additional hardware at the routes along which trucks or shipping containers move. Secondly, RFID readers at highway overpasses still do not enable real-time monitoring.

Apart from improved planning, security is another motivation for cargo tracking and tracing. Consider, for instance, trucks with valuable goods or hazardous material. A requirement might be to prevent such trucks from deviating from their scheduled route. This route can be defined by a corridor in which a truck can move freely. In general, such corridors should follow the course of highways, thereby also enabling trucks to leave the highway for refuelling. But if the predefined corridor is left, the autonomous logistics entity has to stop the car immediately and inform the dispatcher or the responsible authorities (Hannon, 2002, pp. 39–40). Likewise, this allows preventing trucks with hazardous materials from approaching vulnerable facilities such as nuclear power plants (Pekow, 2005, p. 14). RFID-based approaches may suffice to keep production plans up-to-date. But the temporal resolution of beacon-based approaches is too coarse for the security application intended.

As an alternative to beacon-based approaches, trilateration can be applied (Pflaum & Hupp, 2007, p. 112). Trilateration allows determining the position of objects based on their distance to reference points whose position is known. Figure 3.8 illustrates an example for the two-dimensional case. The position of point P is to be determined. The position of reference points R_1, R_2, and R_3 is known. Likewise, also the distances between P and the reference points are known. The distance to reference point R_1 constrains the position of P to a circle with radius $\overline{PR_1}$ around R_1. Adding reference point R_2 further constrains the position of P to the intersection of the circles around R_1 and R_2. Finally, adding R_3 reveals the actual position of P.

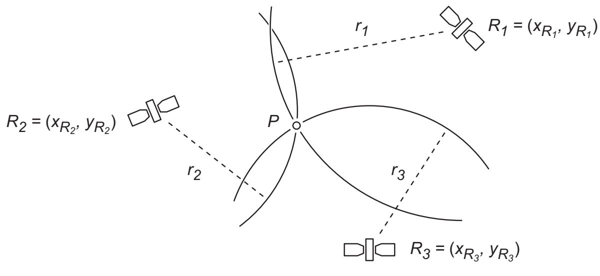

Fig. 3.8 A two-dimensional trilateration example. The position of P has to be determined by its distance to the reference points R_1, R_2, and R_3. P lies at the intersection of the distance circles around the reference points.

Instead of employing arbitrary landmarks, global navigation satellite systems (GNSS) are a generic alternative with worldwide coverage (Hofmann-Wellenhof, Lichtenegger & Wasle, 2008, pp. 4–6). Apart from the existing satellites, no additional equipment has to be installed in the environment. Only the autonomous logistics entity whose location is to be determined must be equipped with a receiver for position transmissions by the satellites

(Pekow, 2005, p. 14). Existing global navigation satellite systems include the US global positioning system GPS and the Russian GLONASS. In the future, also the European Galileo will be available. These systems have in common that they consist of a number of medium Earth orbit satellites (Tanenbaum, 2003, p. 114). The satellites are aware of their current position. Furthermore, they are equipped with high-precision clocks. Each satellite continuously broadcasts its current position and time (Pflaum & Hupp, 2007, p. 112). The distance to the satellite can be computed based on the delay with which the signal is received. Determining a position on the surface of Earth requires signals from at least four satellites (Hofmann-Wellenhof et al., 2008, pp. 8–9). Alternatively, one could also apply base stations of cellular networks. However, the precision of satellite-based systems is generally higher. Furthermore, while cellular networks do not cover oceans, global navigation satellite systems can also be applied to locate shipping containers worldwide.

In intralogistics, it is quite common to employ automated guided vehicles (AGV), for instance, to transport workpieces between different workplaces. The control and navigation of such vehicles also requires means for localisation. Unfortunately, the benefit of satellite-based localisation systems is rather limited in this context. This is due to the fact that the satellite signal is too weak to be reliably received inside buildings and through some materials (Pflaum & Hupp, 2007, p. 112). Conventional guidance systems are thus based on wire-guided tracks or optical following of surface markings (Martin, 2006, pp. 265–267). In the first case, the possibility to change the production layouts is rather limited; in the second case, abrasion can significantly decrease recognition rates (ten Hompel, Schmidt, Nagel & Jünemann, 2007, pp. 199–204). In contrast to machines, humans do easily succeed in such navigation tasks, even in dynamic environments. Hence, cognitively motivated spatial representations are a promising alternative (Schuldt & Gottfried, 2008a, 2008b).

In this context, RFID may support computer vision methods and help identify both stationary objects and other vehicles in the environment. Without RFID support, objects can be recognised by their visual appearance. In general, several visual properties such as size, position, orientation, colour, and texture are applicable for object recognition. According to Palmer (1999, p. 363), however, the visually most significant property of objects is their shape. For fast object recognition compact shape representations (Schuldt, Gottfried & Herzog, 2006a, 2006b, 2006c) can be applied. Choosing such compact representations can be motivated by their low computational complexity (Section 2.3.1) for shape comparison. Numeric representations characterise shapes even by only one numeric value (Duda & Hart, 1973; Garson & Biggs, 1992; Gottfried, Schuldt & Herzog, 2007). In order to ease object recognition, special visual markings can be attached in order to recognise categories of objects.

To summarise, localisation allows implementing services like tracking and tracing in logistics. Tracking and tracing is the foundation for both improving planning and increasing security in transport processes. The technologies that can be applied to localise objects range from beacon-based approaches to trilateration and recognition of the environment by computer vision. The concrete technology to be chosen depends on the application addressed. Likewise, also the granularity at which localisation is implemented depends on the concrete application (Section 3.1.3). For instance, it does not seem reasonable to equip every package transported on a truck with a GPS receiving unit. Instead, the receiver could be part of the respective truck. The truck would then use its communication unit to share the current global position with its packages.

3.2.3 Sensor Technology

Identification allows distinguishing autonomous entities in order to link them to computer-based control systems. With localisation technology, it is possible to determine the current location of logistics entities. Sensors additionally enable monitoring both objects and their environment. The necessity for monitoring can be motivated by actual requirements from logistics practice. This section present applications in logistics requiring sensor technology to ensure quality and security. Subsequently, it is examined how wireless sensor networks can be applied to address these demands.

One of the major objectives in logistics is to deliver goods in the right quality (Chapter 2). Hence, goods must be protected appropriately, e. g., by transporting them in refrigerated shipping containers. However, implementing protection alone does not suffice. Additionally, adequate quality monitoring has to be conducted in order to validate the protection. On the one hand, this allows reacting early if, for instance, the cooling system fails. On the other hand, regarding claims for reimbursement, monitoring allows finding out who is responsible for failures occurring.

As an example consider shipping containers that are transported by container vessel from East Asia to Europe. During their transport, these shipping containers undergo fluctuating extreme climate conditions, in particular regarding temperature and humidity (DHL Express Vertriebs GmbH & Co. OHG, 2005, pp. 393–394). Both temperature and humidity are influenced by ambient air and water. On deck of container vessels, containers are directly exposed to sunlight. On some shipping routes this leads to heating of up to 80° C on the surface of the container. Consequently, also the interior temperature increases, thereby heating the cargo to more than 50° C. Likewise, the water temperature heats containers in the body of the vessel on warm routes. Problems resulting are manifold (DHL Express Vertriebs GmbH & Co. OHG, 2005, p. 393). Extremely high temperatures often lead to changes in the physical state of matter, i. e., transitions between solid, liquid, and gas. As a consequence, packages may burst due to thermal expansion. Apart from that, growth of microorganisms may accelerate under increased temperature. This, in turn, may lead to earlier deterioration, self-heating, and even spontaneous combustion. Humidity is closely linked with temperature. Decreasing temperature results in water condensing on the goods loaded in the container because the absorption capacity of air decreases with lower temperatures. Condensation water, in turn, leads to a loss of quality of the goods carried (DHL Express Vertriebs GmbH & Co. OHG, 2005, p. 394).

Both temperature and humidity can be controlled by refrigerated containers. Legal obligations require to prove a gapless cold chain for some goods, e. g., in the food supply chain (Jedermann, Behrens, Westphal & Lang, 2006, p. 370). Therefore, it is necessary to monitor the interior climate of shipping containers (Thiesse, 2005, p. 113). Quality models exist that determine the perishability of particular forms of food in relation to the environmental temperature (Jedermann, Emond & Lang, 2007, pp. 233–234). Detecting a cooling system failure allows re-routing a container to a point of sale nearby. Another container with equal goods can then be re-routed to the original destination.

The positioning of the sensor significantly influences the measurements of the interior climate. In standard containers air temperature is higher near the hull of the container (DHL Express Vertriebs GmbH & Co. OHG, 2005, p. 393). Likewise, the temperature sensed in refrigerated containers depends on the vicinity to the cooling unit and air ventilation. Temperature differences of up to five kelvin require placing multiple sensors in the container (Jedermann, Stein, Becker & Lang, 2008). Besides temperature and humidity, also ethylene is an indicator for food quality (Jedermann, Schouten, Sklorz, Lang & Kooten, 2006, p. 3). The ethylene concentration influences the ripening process of fruits.

Apart from quality, other important issues to be regarded in logistics concern safety and security (Werner et al., 2007). The demand for security in logistics has been brought into focus after the terrorist attacks of September 11, 2001 (Daschkovska & Scholz-Reiter, 2007, p. 305). Shipping containers are particularly considered in these efforts due to their high throughput in the intercontinental transport of packaged goods. The two main objectives are protecting the cargo from thieves as well as preventing terrorists from smuggling dangerous goods. A conventional approach is to employ mechanical seals, e. g., numbered bolts. After loading, the seal is affixed on the container. Before unloading, it has to be validated that the seal is undamaged and that it has not been replaced (Tirschwell, 2005, p. 54).

Conventional seals are comparatively cheap because they only consist of a numbered bolt. A new seal has to be affixed each time a container has been opened legitimately because the seals are not reusable (Hadow, 2005, p. 58); the unique number (Field, 2005, p. 48) of the new seal has to be recorded. Despite of the low purchase price for mechanical seals, their handling cost is quite high because their manual inspection is time consuming (Tirschwell, 2005, p. 54). Mechanical seals increase the effort for tampering with a container. Nevertheless, their benefit is still limited. Hadow (2005, p. 58) elaborates that criminals can remove the doors of the container completely, thereby not damaging the seal. Alternatives are cutting a hole into another wall or creating a new seal after having finished.

Electronic seals are a more sophisticated approach as they notice tamper immediately and alert the cargo owner (Hickey, 2004, p. 34). Container security systems additionally include sensors in order to monitor tampering, theft, and placement of unintentional freight (Figure 3.9). Sensors applied range from light sensors and gamma ray detectors to chemical sensors (Schwartz, 2004, p. 16). In order to save energy and cost, the sensors applied have to chosen with respect to the concrete purpose. Thus, electronic seal and sensors must be able to establish ad hoc networks. Access to such networks has to be restricted in order to exclude untrustworthy sensors that have been placed by thieves or terrorists in order to inject manipulated data. To summarise, augmenting electronic security systems by additional sensors placed inside containers can significantly improve security.

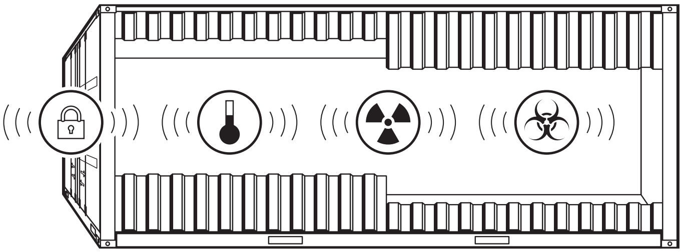

Fig. 3.9 Sensors can be applied in order to monitor the interior of shipping containers. The combination of sensors depends on the task at hand. Common sensors include door lock sensors, temperature sensors, gamma ray detectors, and chemical sensors.

The above examples demonstrate that sensors are an important technology in order to monitor logistics processes. Sensor technology provides the means to guarantee quality and security in logistics. In the applications discussed above, it is not sufficient to place single sensors within a shipping container. Instead, there is a demand for sensor networks. On the one hand, this is due to the fact that the data measured varies depending on the location of the sensor, e. g., temperature in refrigerated containers. On the other hand, different types of sensors may be required in order to measure different phenomena that correlate with, for instance, the ripening process of fruits. This can be achieved by wireless sensor networks (Akyildiz, Su, Sankarasubramaniam & Cayirci, 2002) which allow distributing sensors with a high degree of freedom. Jedermann, Behrens, Laur and Lang (2007, p. 384) describe an approach to automatically configure sensor systems depending on the goods transported. The configuration can be determined during loading of freight, e. g., by reading an RFID chip that is attached on the goods.

Apart from flexible configuration, energy consumption is another important issue when dealing with wireless sensor networks. Being distributed within a shipping container, sensors cannot be supplied from a central power source. Instead, they must be equipped with batteries. This, in turn, raises requirements regarding economical energy consumption because battery lifetime is limited (Section 3.1.3). A particularly high amount of energy is consumed by wireless communication between the sensor nodes and their base station. Therefore, sensor nodes should cooperate in order to decrease the amount of energy spent during the transmission of collected data. This can be accomplished by applying clustering algorithms that aim at optimising energy consumption for communication purposes. Clustering sensors by spatial proximity is a common approach. Routing data messages is then organised in a hierarchical way (Al-Karaki & Kamal, 2004). Each cluster collects the sensor data of its environment, aggregates it, and transmits it to the base station. A prominent approach is LEACH, which stands for low-energy adaptive clustering hierarchy (Heinzelman, Chandrakasan & Balakrishnan, 2000). In this method, some sensor nodes choose to be cluster-heads. The remaining nodes join the cluster that requires minimum communication energy. If sensor nodes generally choose the spatially closest cluster-head, a Voronoi (Klein, 2005, pp. 83–102) tessellation evolves (Figure 3.10). To distribute power consumption for long-range communication, the cluster-heads are regularly changed, which also leads to a new cluster partitioning.

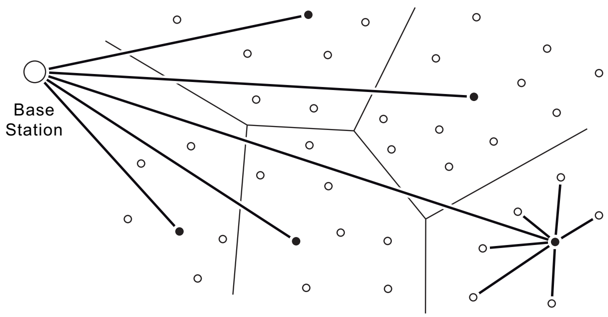

Fig. 3.10 Nodes (transparent circles) of a wireless sensor network. In order to save energy, sensors cluster themselves in order to aggregate data locally. Dynamically chosen cluster heads (opaque circles) then transmit the data sensed to their base station.

To summarise, sensor technology enables monitoring of goods handled in logistics processes. Applying sensors allows ensuring both quality and security. The actual type and number of sensors chosen depends on the concrete objective. Wireless sensor networks allow dynamically combining the independent sensor nodes required. The limited amount of power that is provided by batteries can be saved by appropriate clustering methods. The data acquired locally by wireless sensor networks can be applied in both conventional and autonomous logistics. However, pre-processing data and making decisions on the local level enables immediate reactivity without waiting for a central entity, a potential bottleneck. Additional technologies required for this objective are discussed in the following sections.

3.2.4 Communication

Identification, localisation, and sensor unit provide autonomous logistics entities with information about themselves, their condition, and their environment. Interaction with the outside world requires an additional unit, namely the communication unit. This part of the architecture provides the means to exchange with other autonomous entities or humans by sending and receiving messages.

Today, communication has become cheap for many applications. Broadband communication providers offer access to their guided networks with high bandwidth and low charges. But logistics entities are usually widely distributed, often over multiple continents. Furthermore, they are rarely stationary. Instead, they move through the logistics network. Therefore, autonomous logistics entities cannot employ classical guided transmission media, i. e., copper wire or fibre optics (Tanenbaum, 2003, p. 85). Instead, wireless or satellite communication has to be applied. From the point of view of an autonomous logistics entity it does not make much difference whether guided or wireless media are accessed. Architectures like the ISO OSI (Open Systems Interconnection) reference model and TCP/IP provide an abstraction from the underlying physical layer, thereby enabling end-to-end connections on the application layer (Tanenbaum, 2003, pp. 37–49).

This allows logistics entities communicating with each other independently of the underlying network infrastructure. Differences arise, of course, regarding availability and cost of communication. One possibility is to establish private wireless local area networks (WLANs) to connect autonomous logistics entities to guided networks. This approach, however, is only reasonable in intralogistics. For instance, consider trucks on a highway. Even assumed that connection to wired networks was possible, one would need many wireless access points. For containers on the ocean it is even more obvious that there is virtually no possibility to connect them to wired networks. Wireless communication over cellular networks or communication satellites could provide an alternative. The problem, however, is that bandwidth of these communication channels is comparatively limited. Therefore, higher utilisation fees are charged for these networks. Another cost factor for communication in autonomous logistics is the energy needed for mobile communication. This section presents the application of communication for reporting and interaction. Thereby, standards for message exchange and security issues are discussed.

Radio-frequency identification is one application for communication (Section 3.2.1). Furthermore, communication is also required to transmit localisation and sensor information in order to implement real-time visibility of supply networks. This information can then be centrally evaluated in order to react appropriately if the conditions of the cargo or its environment change. Consider detecting an increase in temperature level within a shipping container because its cooling unit fails. As described in Section 3.2.3, the remaining shelf life of food depends on the environmental temperature. In case of increasing temperature, it might thus be appropriate to re-route the container to a nearer sink or to re-pack the cargo onto another load carrier. In centralised control approaches one would simply provide a central unit with all sensor measurements.

Akyildiz et al. (2002, p. 403) point out that, that communication generally consumes more energy than sensing and data processing. Therefore, it is advisable to use communication as economically as possible. This can be achieved by pre-processing sensory data before transmitting it to other autonomous or centralised entities. For instance, it is not necessary to send all measurements by a temperature sensor to a dispatcher. By contrast, the dispatcher is only interested in being notified about substantial changes (Jedermann, Behrens et al., 2006, p. 370). Thus, it is sufficient to inform him if certain thresholds are exceeded. Autonomous logistics goes even one step further. In this paradigm, autonomous logistics entities may take actions required to react appropriately themselves or at least to propose possible reactions. Reasoning about adequate reactions is not conducted by the communication unit but by the data processing unit of the autonomous logistics entity (Section 3.2.5).

Apart from reacting to environmental changes, communicating autonomous logistics entities may also cooperate with others in order to achieve their logistics objectives. The communication unit is the interface to the outside world for coordination with other entities. Communication with such partners is generally conducted on an ad hoc basis (Section 3.1.1). Firstly, this requires a common vocabulary that is understood by all participating entities (Hellenschmidt & Wichert, 2007, p. 94, 102). This issue is, for instance, addressed by the EDIFACT standard, which is an acronym for Electronic Data Interchange for Administration, Commerce and Transport (Vahrenkamp, 2007, p. 56). Secondly, the communication unit is also a vulnerable point that must be secured appropriately (Werner et al., 2007).

As an example, consider a shipping container that is currently located at a container terminal. This container is loaded with hazardous material. Communication regarding the content of the container must then be restricted to trustworthy partners. From the perspective of safety it might be desirable for such containers to inform the environment about their hazardous content. But this is not the case from a security point of view. It is not advisable to broadcast the attractiveness of a container for terrorist attacks to everyone including the terrorists themselves (Hadow, 2005, p. 58). Only personnel at the container terminal, such as stevedores and truckers, is a legitimate recipient of some security-related data. Therefore, one must ensure that only legitimate recipients obtain data from the container security system. This can be accomplished by encryption. Additionally, it is important to clearly identify authorised cooperation partners. This issue is addressed by signatures.

Both demands for trustworthiness can be addressed by applying public key cryptography (Tanenbaum, 2003, pp. 752–755) which is based on pairs of asymmetric encryption keys. In this approach, the public key of each entity is known to everyone and is applied in order to encrypt the content of messages for the respective entity (Figure 3.11). Decrypting such contents can only be accomplished by applying the private key which is concealed and only known to the entity itself. A sender additionally signing the message with its own private key enables the receiver to validate its authenticity with the respective public key. To be capable of identifying trustworthy communication partners each entity must be provided with the public key of the company. The respective private key can, however, not simply be provided to all participants. Otherwise, the whole system runs into danger of being compromised, for instance, if a hand-held device with the key is lost. A finder or thief would then be able to decrypt all messages intended for the company. Instead, a public key infrastructure (Tanenbaum, 2003, pp. 768–771) has to be established. In this concept each entity gets its own private key that is signed by the private root certificate of the company. Validating the respective public keys with the public key of the company then reveals whether a communication partner is trustworthy. The problem of loss can be approached by expiring keys that must be renewed regularly.

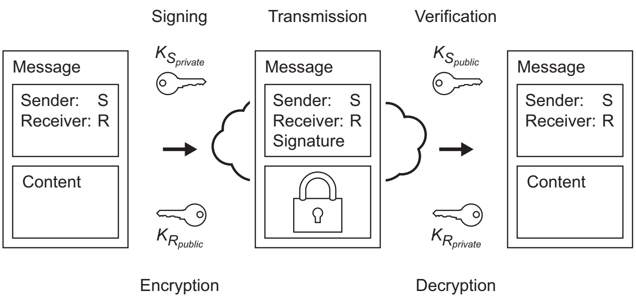

Fig. 3.11 Two autonomous logistics entities communicate with pairs of public and private keys. Sender S signs and encrypts the content of its message before transmission. The received message is then validated and decrypted by the receiver R.

To summarise, communication is needed for both cooperation between logistics entities as well as interaction with other participants in logistics processes. Cooperation may include coordination regarding joint utilisation of transport or storage capacities. Examples for other participants are owners who are informed about the current condition of their logistics entities. For security reasons communication must be restricted to trustworthy partners. This can be achieved by encryption and signatures. Like for localisation and sensor technology, it is not necessary to provide all autonomous logistics entities with all communication facilities. Instead, it might be sufficient that entities at a high granularity are capable of long-range communication. That is, trucks could have access to cellular networks. Container vessels may use a satellite uplink. Other entities loaded, such as packets or containers, can then share the communication infrastructure of the respective load carrier.

3.2.5 Data Processing

The technologies for autonomous entities examined so far lay the foundations for enabling autonomous control in logistics. The identification unit enables each entity to identify itself and to recognise other entities (Section 3.2.1). The localisation unit allows gathering tracking and tracing information for autonomous entities (Section 3.2.2). Combined with additional sensor technology, this helps ensure quality as well as safety and security in logistics (Section 3.2.3). The communication unit allows interacting with other logistics entities and to provide the cargo owner with information on the current state (Section 3.2.4).

However, these units are necessary but not sufficient to implement autonomous logistics. They could also be applied in order to improve conventional centralised supply network management. Then, all identification, localisation, and sensor information is provided to a central decision-making entity. By contrast, the autonomous logistics paradigm envisions that decisions are made locally by the logistics entities themselves. But none of the units investigated so far has the capability for decision-making. To this end, the data processing unit is the crucial part to implement autonomous control in logistics. In the architecture for autonomous logistics entities (Figure 3.3), the data processing unit integrates all other parts, thereby enabling decisions to be made locally.

The miniaturisation of integrated circuits allows attaching the data processing unit directly to the respective logistics entity (Section 3.1.2). Such embedded systems enable truly decentralised decision-making without centralised control (e. g., Jedermann, Antúnez Congil et al., 2007, p. 193–194). As an example, consider several shipping containers of the same company that are supposed to be loaded onto a container vessel in a port in East Asia. Furthermore, consider that it turns out that the vessel is overbooked and that not all containers can be loaded. It is then possible that the containers directly negotiate which of them are most important based on the priority of the cargo loaded. If the containers have the knowledge demanded for that decision, no intervention by a human dispatcher is required.

Distribution usually constrains the resources available (Section 3.1.2). On the one hand, resources are bound regarding the power available. But on the other hand, computational and memory capacities are also limited. As an alternative, intelligent representatives that are located on one or multiple central servers can act on behalf of the logistics entity represented by them. This is the variation of autonomous logistics that represents the smallest deviation from truly distributed decision-making. Nevertheless, the advantages of reduced complexity and the improved ability of coping with dynamics are retained. It is, of course, only applicable in environments with guaranteed communication connectivity to the autonomous logistics entity. The particular advantage is that a more powerful central server offers more computational power to representatives of logistics entities than embedded devices. Nevertheless, also central servers do not possess unbounded resources because they are likewise constrained by the limitations of asymptotical computational complexity regarding time and space (Section 2.3.1). Thus, sophisticated knowledge management approaches are required. Methods applied must consider learning of relevant, but also forgetting of irrelevant knowledge (Werner et al., 2007, p. 15).

3.3 Conclusion

Conventional supply network management from a centralised point is limited by the complexity, the dynamics, and the distribution that are inherent in logistics processes. In contrast to previous approaches, autonomous control in logistics delegates decision-making to the local logistics objects, e. g., sales units, cardboard boxes, pallets, containers, and trucks. These autonomous logistics entities are provided with logistics objectives defined by their owners. They must then cooperate in order to achieve these objectives. The miniaturisation of integrated circuits and other technologies allows enhancing logistics entities with the capabilities required. However, technological and economical limitations demand finding an adequate granularity at which autonomous control is applied. Additionally, also the degree of freedom in decision-making must be constrained. Technologies enabling autonomous logistics include identification, localisation, sensors, communication, and data processing. The data processing unit is the crucial part for autonomous logistics entities. The important question is how to actually implement the Artificial Intelligence required by autonomous logistics entities.

References

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y. & Cayirci, E. (2002). Wireless Sensor Networks: A Survey. *Computer Networks*, *38*(4), 393–422.

Al-Karaki, J. N. & Kamal, A. E. (2004). Routing Techniques in Wireless Sensor Networks: A Survey. *IEEE Wireless Communications*, *11*(6), 6–28.

Arnold, D., Isermann, H., Kuhn, A., Tempelmeier, H. & Furmans, K. (Eds.). (2008). *Handbuch Logistik* (3rd ed.). Heidelberg, Germany: Springer-Verlag.

Becker, M., Kuladinithi, K., Timm-Giel, A. & Görg, C. (2007). Historical Development of the Idea of Self-Organisation in Information and Communication Technology. In M. Hülsmann & K. Windt (Eds.), *Understanding Autonomous Cooperation and Control in Logistics: The Impact of Autonomy on Management, Information, Communication and Material Flow* (pp. 45–56). Heidelberg, Germany: Springer-Verlag.

Berning, M. & Vastag, S. (2007). Simulation selbststeuernder Transportnetze. In H.-J. Bullinger & M. ten Hompel (Eds.), *Internet der Dinge* (pp. 119–126). Heidelberg, Germany: Springer-Verlag.

Bullinger, H.-J. & ten Hompel, M. (Eds.). (2007). *Internet der Dinge.* Heidelberg, Germany: Springer-Verlag.

Cardeneo, A. (2008). Kurier-, Express- und Paketdienste. In D. Arnold, H. Isermann, A. Kuhn, H. Tempelmeier & K. Furmans (Eds.), *Handbuch Logistik* (3rd ed., pp. 782–788). Heidelberg, Germany: Springer-Verlag.

Daschkovska, K. & Scholz-Reiter, B. (2007). Electronic Seals for Efficient Container Logistics. In H.-D. Haasis, H.-J. Kreowski & B. Scholz-Reiter (Eds.), *1st International Conference on Dynamics in Logistics (LDIC 2007)* (pp. 305–312). Bremen, Germany: Springer-Verlag.

DHL Express Vertriebs GmbH & Co. OHG. (2005). *Logistik-Lotse 2005* (13th ed.). Bonn, Germany: Verkehrs-Verlag Fischer.

Duda, R. O. & Hart, P. E. (1973). *Pattern Classification and Scene Analysis.* New York, NY, USA: John Wiley & Sons.

Field, A. M. (2005). Seals of Approval. *Journal of Commerce*, *6*(38), 46–48.

Fleisch, E. & Mattern, F. (Eds.). (2005). *Das Internet der Dinge.* Heidelberg, Germany: Springer-Verlag.

Flörkemeier, C. (2005). EPC-Technologie – vom Auto-ID Center zu EPCglobal. In E. Fleisch & F. Mattern (Eds.), *Das Internet der Dinge* (pp. 87–100). Heidelberg, Germany: Springer-Verlag.

Freitag, M., Herzog, O. & Scholz-Reiter, B. (2004). Selbststeuerung logistischer Prozesse – Ein Paradigmenwechsel und seine Grenzen. *Industrie Management*, *20*(1), 23–27.

Gallagher, J. (2002). Test Tracking. *Traffic World*, *266*(46), 48.

Garson, G. D. & Biggs, R. S. (1992). *Analytic Mapping and Geographic Databases.* Newbury Park, CA, USA: Sage Publications.

Gottfried, B., Schuldt, A. & Herzog, O. (2007). Extent, Extremum, and Curvature: Qualitative Numeric Features for Efficient Shape Retrieval. In J. Hertzberg, M. Beetz & R. Englert (Eds.), *30th Annual German Conference on Artificial Intelligence (KI 2007)* (pp. 308–322). Osnabrück, Germany: Springer-Verlag.

Haasis, H.-D., Kreowski, H.-J. & Scholz-Reiter, B. (Eds.). (2007). *1st International Conference on Dynamics in Logistics (LDIC 2007).* Bremen, Germany: Springer-Verlag.

Hadow, R. (2005). E-Seals and RFID. *Journal of Commerce*, *6*(43), 58.

Hannon, D. (2002). High-Tech Security Becomes Top Priority in Supply Chain. *Purchasing*, *131*(11), 39–41.

Heinzelman, W. R., Chandrakasan, A. & Balakrishnan, H. (2000). Energy-Efficient Communication Protocol for Wireless Microsensor Networks. In *33rd Hawaii International Conference on System Sciences (HICSS 2000)* (Vol. 8, pp. 8020–8029). Maui, HI, USA: IEEE Computer Society.

Hellenschmidt, M. & Wichert, R. (2007). Selbstorganisation: Dinge in eigenverantwortlicher Kooperation – eine Systemanalyse. In H.-J. Bullinger & M. ten Hompel (Eds.), *Internet der Dinge* (pp. 91–105). Heidelberg, Germany: Springer-Verlag.

Herzog, O., Freitag, M. & Scholz-Reiter, B. (2005). Selbststeuerung logistischer Prozesse – Ein Paradigmenwechsel. In Bundesvereinigung Logistik (BVL) e.V. (Ed.), *22. Deutscher Logistik-Kongress* (pp. 219–224). Berlin, Germany: Deutscher Verkehrs-Verlag.

Hickey, K. (2004). Insecurity Over E-Seals. *Traffic World*, *268*(3), 34.

Hülsmann, M. & Windt, K. (Eds.). (2007). *Understanding Autonomous Cooperation and Control in Logistics: The Impact of Autonomy on Management, Information, Communication and Material Flow.* Heidelberg, Germany: Springer-Verlag.

Hülsmann, M., Wycisk, C., Agarwal, R. & Grapp, J. (2007). Prologue to Autonomous Cooperation – the Idea of Self-Organisation as its Basic Concepts. In M. Hülsmann & K. Windt (Eds.), *Understanding Autonomous Cooperation and Control in Logistics: The Impact of Autonomy on Management, Information, Communication and Material Flow* (pp. 23–44). Heidelberg, Germany: Springer-Verlag.

Hofmann-Wellenhof, B., Lichtenegger, H. & Wasle, E. (2008). *GNSS Global Navigation Satellite Systems: GPS, GLONASS, Galileo and more.* Wien, Austria: Springer-Verlag.

Jedermann, R., Antúnez Congil, L. J., Lorenz, M., Gehrke, J. D., Lang, W. & Herzog, O. (2007). Dynamic Decision Making on Embedded Platforms in Transport Logistics – A Case Study. In H.-D. Haasis, H.-J. Kreowski & B. Scholz-Reiter (Eds.), *1st International Conference on Dynamics in Logistics (LDIC 2007)* (pp. 191–198). Bremen, Germany: Springer-Verlag.

Jedermann, R., Behrens, C., Laur, R. & Lang, W. (2007). Intelligent Containers and Sensor Networks Approaches to apply Autonomous Cooperation on Systems with Limited Resources. In M. Hülsmann & K. Windt (Eds.), *Understanding Autonomous Cooperation and Control in Logistics: The Impact of Autonomy on Management, Information, Communication and Material Flow* (pp. 365–392). Heidelberg, Germany: Springer-Verlag.

Jedermann, R., Behrens, C., Westphal, D. & Lang, W. (2006). Applying Autonomous Sensor Systems in Logistics — Combining Sensor Networks, RFIDs and Software Agents. *Sensors and Actuators A*, *132*(1), 370–375.

Jedermann, R., Emond, J.-P. & Lang, W. (2007). Shelf Life Prediction by Intelligent RFID – Technical Limits of Model Accuracy. In H.-D. Haasis, H.-J. Kreowski & B. Scholz-Reiter (Eds.), *1st International Conference on Dynamics in Logistics (LDIC 2007)* (pp. 231–238). Bremen, Germany: Springer-Verlag.

Jedermann, R., Gehrke, J. D., Becker, M., Behrens, C., Morales-Kluge, E., Herzog, O. et al. (2007). Transport Scenario for the Intelligent Container. In M. Hülsmann & K. Windt (Eds.), *Understanding Autonomous Cooperation and Control in Logistics: The Impact of Autonomy on Management, Information, Communication and Material Flow* (pp. 393–404). Heidelberg, Germany: Springer-Verlag.

Jedermann, R., Schouten, R., Sklorz, A., Lang, W. & Kooten, O. van. (2006). Linking Keeping Quality Models and Sensor Systems to an Autonomous Transport Supervision System. In J. Kreyenschmidt & B. Petersen (Eds.), *2nd International Workshop on Cold Chain Management* (pp. 3–18). Bonn, Germany.

Jedermann, R., Stein, K., Becker, M. & Lang, W. (2008). UHF-RFID in the Food Chain – From Identification to Smart Labels. In J. Kreyenschmidt (Ed.), *3rd International Workshop on Coldchain Manangement.* Bonn, Germany.

Köhler-Bußmeier, M. (2009). Emergenz, Selbstorganisation und Komplexität. In R. v. Lüde, D. Moldt & R. Valk (Eds.), *Selbstorganisation und Governance in künstlichen und sozialen Systemen* (pp. 17–71). Münster, Germany: LIT Verlag.

Klein, R. (2005). *Algorithmische Geometrie: Grundlagen, Methoden, Anwendungen* (2nd ed.). Heidelberg, Germany: Springer-Verlag.

Kuhlmann, F. & Masuhr, D. (2007). Prozesse in offenen Systemen gestalten. In H.-J. Bullinger & M. ten Hompel (Eds.), *Internet der Dinge* (pp. 257–265). Heidelberg, Germany: Springer-Verlag.

Lampe, M., Flörkemeier, C. & Haller, S. (2005). Einführung in die RFID-Technologie. In E. Fleisch & F. Mattern (Eds.), *Das Internet der Dinge* (pp. 69–86). Heidelberg, Germany: Springer-Verlag.

Martin, H. (2006). *Transport- und Lagerlogistik – Planung, Struktur, Steuerung und Kosten von Systemen der Intralogistik.* Wiesbaden, Ger-

many: Friedrich Vieweg & Sohn Verlag.
Mattern, F. (2005). Die technische Basis für das Internet der Dinge. In E. Fleisch & F. Mattern (Eds.), *Das Internet der Dinge* (pp. 39–66). Heidelberg, Germany: Springer-Verlag.
Matthias, A. (2008). *Automaten als Träger von Rechten. Plädoyer für eine Gesetzesänderung.* Berlin, Germany: Logos Verlag.
Moore, G. E. (1965). Cramming More Components onto Integrated Circuits. *Electronics*, *38*(8), 114-117.
Nitschke, T. (2006). Legal Consequences of Agent Deployment. In S. Kirn, O. Herzog, P. Lockemann & O. Spaniol (Eds.), *Multiagent Engineering: Theory and Applications in Enterprises* (pp. 597–618). Heidelberg, Germany: Springer-Verlag.
Palmer, S. E. (1999). *Vision Science: Photons to Phenomenology.* Cambridge, MA, USA: MIT Press.
Pekow, C. (2005). GPS Proven Best for Hazmat Tracking. *LP/GAS*, *65*(3), 14.
Pflaum, A. & Hupp, J. (2007). Sensornetzwerke und Lokalisierungsverfahren als Schlüsseltechnologien für die intelligente logistische Umwelt von morgen. In H.-J. Bullinger & M. ten Hompel (Eds.), *Internet der Dinge* (pp. 107–118). Heidelberg, Germany: Springer-Verlag.
Scholz-Reiter, B., Toonen, C. & Windt, K. (2008). Logistikdienstleistungen. In D. Arnold, H. Isermann, A. Kuhn, H. Tempelmeier & K. Furmans (Eds.), *Handbuch Logistik* (3rd ed., pp. 581–607). Heidelberg, Germany: Springer-Verlag.
Scholz-Reiter, B., Windt, K. & Freitag, M. (2004). Autonomous Logistic Processes — New Demands and First Approaches. In *37th CIRP International Seminar on Manufacturing Systems* (pp. 357–362). Budapest, Hungary.
Schuldt, A. & Gottfried, B. (2008a). Selbststeuerung in der Intralogistik: Kognitive räumliche Repräsentationen für autonome Fahrzeuge. *Industrie Management*, *24*(4), 41–44.
Schuldt, A. & Gottfried, B. (2008b). Spatiotemporal Cooperation at the Geographic Scale. In B. Loos & V. Micelli (Eds.), *Interdisciplinary College (IK 2008)* (p. 32). Günne, Germany.
Schuldt, A., Gottfried, B. & Herzog, O. (2006a). A Compact Shape Representation for Linear Geographical Objects: The Scope Histogram. In S. Nittel & R. A. de By (Eds.), *14th ACM International Symposium on Advances in Geographic Information Systems (GIS 2006)* (pp. 51–58). Arlington, VA, USA: ACM Press.
Schuldt, A., Gottfried, B. & Herzog, O. (2006b). Retrieving Shapes Efficiently by a Qualitative Shape Descriptor: The Scope Histogram. In H. Sundaram, M. Naphade, J. Smith & Y. Rui (Eds.), *5th International Conference on Image and Video Retrieval (CIVR 2006)* (pp. 261–270). Tempe, AZ, USA: Springer-Verlag.

Schuldt, A., Gottfried, B. & Herzog, O. (2006c). Towards the Visualisation of Shape Features: The Scope Histogram. In C. Freksa, M. Kohlhase & K. Schill (Eds.), *29th Annual German Conference on Artificial Intelligence (KI 2006)* (pp. 289–301). Bremen, Germany: Springer-Verlag.

Schuldt, A. & Werner, S. (2007). Distributed Clustering of Autonomous Shipping Containers by Concept, Location, and Time. In P. Petta, J. P. Müller, M. Klusch & M. Georgeff (Eds.), *5th German Conference on Multiagent System Technologies (MATES 2007)* (pp. 121–132). Leipzig, Germany: Springer-Verlag.

Schwartz, E. (2004). The Cost of Safe Commerce. *InfoWorld*, *26*(45), 16.

Tanenbaum, A. S. (2003). *Computer Networks* (4th ed.). Upper Saddle River, NJ, USA: Pearson Education.

ten Hompel, M., Schmidt, T., Nagel, L. & Jünemann, R. (2007). *Materialflusssysteme — Förder- und Lagertechnik.* Heidelberg, Germany: Springer-Verlag.

Thiesse, F. (2005). Architektur und Integration von RFID-Systemen. In E. Fleisch & F. Mattern (Eds.), *Das Internet der Dinge* (pp. 101–117). Heidelberg, Germany: Springer-Verlag.

Timm, I. J. (2006). *Strategic Management of Autonomous Software Systems: Overview Article* (Tech. Rep. No. 35). Universität Bremen: Technologie-Zentrum Informatik.

Tirschwell, P. (2005). An Opportunity from Container Seals. *Journal of Commerce*, *6*(6), 54.

Trautmann, A. (2007). Multiagentensysteme im Internet der Dinge – Konzepte und Realisierung. In H.-J. Bullinger & M. ten Hompel (Eds.), *Internet der Dinge* (pp. 281–294). Heidelberg, Germany: Springer-Verlag.

Vahrenkamp, R. (2007). *Logistik — Management und Strategien* (6th ed.). Munich, Germany: Oldenbourg.

Vastag, S. (2008). Simulative Bewertung von Selbststeuerung in Transportnetzen. In M. Rabe (Ed.), *13th ASIM Dedicated Conference on Simulation in Production and Logistics (ASIM 2008)* (pp. 219–228). Berlin, Germany: Fraunhofer IRB Verlag.

Wenning, B.-L., Rekersbrink, H., Timm-Giel, A., Görg, C. & Scholz-Reiter, B. (2007). Autonomous Control by Means of Distributed Routing. In M. Hülsmann & K. Windt (Eds.), *Understanding Autonomous Cooperation and Control in Logistics: The Impact of Autonomy on Management, Information, Communication and Material Flow* (pp. 325–335). Heidelberg, Germany: Springer-Verlag.

Werner, S., Schuldt, A. & Daschkovska, K. (2007). Agent-Based Container Security Systems: An Interdisciplinary Perspective. In R. Koschke, O. Herzog, K.-H. Rödiger & M. Ronthaler (Eds.), *37th Annual Conference of the German Society for Computer Science (GI 2007)* (pp. 11–16). Bremen, Germany: Gesellschaft für Informatik.

Windt, K. (2008). Ermittlung des angemessenen Selbststeuerungsgrades in der Logistik – Grenzen der Selbststeuerung. In P. Nyhuis (Ed.), *Beiträge zu einer Theorie der Logistik* (pp. 349–372). Heidelberg, Germany: Springer-Verlag.

Windt, K. & Hülsmann, M. (2007). Changing Paradigms in Logistics – Understanding the Shift from Conventional Control to Autonomous Cooperation and Control. In M. Hülsmann & K. Windt (Eds.), *Understanding Autonomous Cooperation and Control in Logistics: The Impact of Autonomy on Management, Information, Communication and Material Flow* (pp. 1–16). Heidelberg, Germany: Springer-Verlag.

Wöstmann, F.-J. (2006). Intelligente Gussbauteile: Wenn Bauelemente mit ihrer Umgebung interagieren. *RFID im Blick*, *7*, 49.

Springer
http://www.springer.com/978-3-642-20091-5

Multiagent Coordination Enabling Autonomous Logistics
Schuldt, A.
2011, XVI, 272 p., Hardcover
ISBN: 978-3-642-20091-5