Vienna University of Technology

Institute for Software Technology and Interactive Systems
Information and Software Engineering Group

Feasibility Study for RFID-based Temperature Monitoring of Blood Bags

Master's Thesis

supervised by
O. Univ.-Prof. Dipl.-Ing. Dr. techn. A Min Tjoa

Bakk. techn. Peter Schrammel
Bertha-von-Suttner-Straße 8
3300 Amstetten, Austria

Vienna, June 9th 2006

Abstract

Blood conserves are temperature-sensitive products with strictly regulated test and storage procedures in order to ensure their quality. However, there are problems in guaranteeing temperature integrity and full traceability. A significant portion of erythrocyte concentrates is discarded because of a supposed interruption of the cold chain. This thesis assesses the feasibility of a system based on RFID technology tackling these problems by monitoring each blood bag ”from vein to vein”, i.e. from its collection over its processing to the transfusion. The goals to be achieved are an increase of blood quality by providing the medical doctors with assistance concerning the temperature integrity, and identifying the problem sources in the supply chain and fixing them in order to reduce the discard percentage. Based on an exemplary analysis of the blood supply chain and the capabilities and limitations of RFID technology and temperature sensing, the requirements on such a system are examined. By analyzing common features of transponders capable of temperature logging, specific problems and their solutions are discussed and the basic functionality is defined. It is proposed how the RFID technology is integrated into the supply chain workflow and the reuse of transponders can be implemented. RFID system architectures and their suitability in the given application are discussed and different design options are considered. An RFID temperature monitoring framework and some use cases have been implemented which demonstrate the technical feasibility of the key concepts. Security, privacy, data integrity, reliability and usability aspects, as well as issues of bulk detection, RFID middleware systems, and the current situation of standardization are incorporated in the discussion. Further applications of RFID temperature monitoring in wine trading, the distribution of beer kegs, pharmaceuticals and the climatic monitoring of sensitive documents are presented. Although some open technical issues concerning the reliability of the transponder hardware have to be evaluated, based on the concepts elaborated in this thesis, RFID technology is a suitable means for the temperature monitoring of blood bags. Generally, there are a number of benefits which arise from RFID deployment such as full traceability, automatic documentation, reporting in terms of haemovigilance and achieving less error-prone processes, e.g. reducing blood bag confusion.

Kurzfassung

Blutkonserven sind temperaturempfindliche Produkte, die strengen Qualitätsbestimmungen bezüglich Tests und Lagerungsbedingungen unterliegen. Allerdings ist derzeit die Nachvollziehbarkeit der Lagerungs- und Transporttemperatur nicht gegeben. Eine nicht unerhebliche Anzahl von Erythrozytenkonzentraten wird auf Grund einer möglichen Unterbrechung der Kühlkette verworfen. Diese Arbeit untersucht die Machbarkeit eines Systems zur durchgehenden Temperaturüberwachung eines jeden einzelnen Blutbeutels „von Vene zu Vene“ basierend auf der RFID-Technologie. Damit soll die Qualität der Blutprodukte gesteigert werden, indem das verantwortliche medizinische Personal in Fragen der Temperaturintegrität unterstützt wird. Weiters kann durch das Erkennen und Beseitigen von Problemen in der Lieferkette längerfristig der Verwurf reduziert werden. Nach einer detaillierten Analyse einer exemplarischen Blut-Supply-Chain von der Blutgewinnung über die Verarbeitung bis hin zur Transfusion, der Stärken und Schwächen der RFID-Technologie, sowie der spezifischen Probleme der Temperaturmessung werden die Anforderungen an ein solches System untersucht. Die erforderlichen Basisfähigkeiten von Transpondern mit Temperatur-Logging-Funktion werden festgelegt. Neben der geeigneten Einbettung des Systems in den Prozessablauf soll auch eine Wiederverwendung der Transponder ermöglicht werden. Designoptionen von RFID-Systemarchitekturen werden hinsichtlich der gegebenen Anwendung diskutiert. Ein RFID-Temperaturmonitoring-Framework wurde implementiert, sowie einige repräsentative Anwendungsfälle, um die technische Machbarkeit der Schlüsselkonzepte zu untermauern. Aspekte der Security und Reliability werden in die Diskussion miteinbezogen ebenso wie die Möglichkeiten der Pulkerkennung, RFID-Middleware und der derzeitige Stand der Standardisierung. Als weitere Anwendungen der Technologie wird der Weinhandel, die Verfolgung von Bierfässern, Medikamente und die Klimakontrolle alter Handschriften vorgestellt. Einige Fragen der Reliability der Transponder müssen noch praktischen Tests unterzogen werden. Basierend auf den ausgearbeiteten Konzepten ist die Machbarkeit eines RFID-basierten Systems zur Temperaturüberwachung von Blutkonserven gegeben. Außerdem ergeben sich noch andere Vorteile des RFID-Einsatzes, wie Rückverfolgbarkeit, automatische Dokumentation, eine Reduktion der Fehleranfälligkeit der Prozesse, z.B. betreffend die Verwechslung von Blutbeuteln, und lückenloseres Hämovigilanz-Reporting.

Acknowledgements

Acknowledgements are due to

- Siemens Österreich AG, especially Dipl.-Ing. Georg Schwondra, PSE PRO CES, for sponsoring this work, providing me with a working environment, RW devices, and valuable contacts,
- University Hospital for Blood Serology and Transfusion Medicine, especially Dr. Thomas Wagner, for support in questions of blood and blood logistics, and data on passive transponder experiments [Wagn06b],
- KSW microtec GmbH for prototype transponders [KSW06],
- Schweizer Elektronik AG for information on foil accumulator tests [Ocke06],
- MacoPharma SA for data on temperature conductivity tests with blood bags [Zimm05].

Furthermore for their assessment of the applicability of RFID-based temperature monitoring in the respective domains:

- Wein&Co Handelsges.m.b.H., Gerhard Hammer, wine trading [Hamm06],
- Ottakringer Brauerei AG, Gottfried Arocker and Michael Ruth, beer kegs [Aroc06],
- Merck GmbH Österreich, Hannes Döller, pharmaceuticals [Döll06],
- Österreichische Nationalbibliothek, Institut für Restaurierung, Mag. Christa Hofmann, sensitive documents [Hofm06].

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Human blood as a valuable, but temperature-sensitive resource is characterized by a short storage life which makes the avoidance of bottle necks in the supply of hospitals a difficult task. Recent guidelines of the European Commission require full traceability of blood bags and the ensurance of the cold chain.

This thesis discusses an approach using the innovative technology of RFID (radio frequency identification) transponders equipped with a temperature sensor in order to monitor each blood bag in the blood supply chain ”from vein to vein”. We investigate the feasibility of the deployment of RFID technology, and discuss the technical requirements and suggested solutions.

1.1 Problem and Motivation

In 2001 6.26% of blood conserves (erythrocyte concentrates) – about 25600 – were discarded in Austria, almost 40% of these because of a possible interruption of the cold chain [Parr03]. The main reasons therefore are the improper transportation or the uncontrolled temporary storage (before and after transport and in hospital wards). Medical doctors responsible for the transfusion take the final decision therefore [OGBT00] by visually inspecting the conserve for haemolysis, i.e. the decomposition of red blood cells, which is accelerated after exposition to unacceptable temperatures.

Currently, the temperature is continuously monitored only in the depots, where temperature alarm systems are installed in blood refrigerators [BMSG02], whereas the temperature of the bags is not controlled during transport. If at all, punctual measurements are performed, e.g. after transport, which do not sufficiently prove that the acceptable temperature range has not been left.

Continuous or close-meshed temperature monitoring with the help of RFID technology appears to be a solution. The approach is aiming at satisfying the following expectations [Wagn06a], [Dalt05]:

- A better foundation of decisions taken by medical doctors on “use or elimination of blood conserves” is achieved by providing additional information about the blood bag’s temperature integrity.
- The detection of possible problems in the cold chain is facilitated. The identification of critical points and problems and subsequently their fixing should lead to a reduction of the elimination percentage
- A complete temperature monitoring allows for returning blood bags which have not been transfused to the blood depots which is not possible at the moment.
- The current process can be improved and made less error-prone by being accompanied by a workflow system and a sound documentation of good medical practices. It is essential to carefully embed the new technology in the existing process in order to be accepted.
- A significant reduction of manual input errors caused by unreadable barcodes and a better prevention of confusions of blood bags by automatic data processing is expected.
- Blood bag data is available everywhere and therefore offers an increase in efficiency, productivity and time savings due to the omission of paper forms by automated documentation.
- The blood supply chain is closed which enables effective, complete reporting in terms of haemovigilance. RFID technology helps to bridge the gap between institutions.
- Thus an overall increase in security and quality of blood products and complete transparency of the blood supply chain can be achieved.

The compatibility of the conserve's and the patient's blood is checked twice by cross-matching in the blood depot and directly before transfusion (bedside test). Most severe incidents arise by confusion of bags at the bedside (85%), often because of inadequate identification of patients and the confusion of probes (66%) in rush situations [OBIG04]. Further problems are incorrect labelling, unreadable labels, and detachment of labels [Wagn06a], [Dalt05].

The need for such a temperature monitoring system is also economically justified: The potential for saving resources and financial means up to one million € (i.e. only by the discarded erythrocyte concentrates due to temperature problems) per year in Austria [Parr03].

The main advantage of the approach presented in this thesis is based on the separate monitoring of each bag using an innovative RFID transponder which functions as a distributed data store - an application which proves that RFID transponders are more than a simple barcode substitution!

This thesis discusses the technical feasibility of RFID temperature monitoring and its broad range of critical issues ranging from physical and usability constraints imposed by the process over technical and functional requirements on the transponder hardware, possible system architectures and the integration of legacy systems to economic considerations.

1.2 Previous Work

Some important steps in the deployment of RFID technology in medical applications, especially in the blood supply chain, have been made in the past:

In 2001 Siemens started a pilot project with passive transponders used for identification and blood depot warehousing at the Hanusch Hospital in Vienna, Austria [Schl03].

Intel, Autentica and Cisco successfully installed a pilot for the identification of blood conserves for autologous transfusions with passive transponders at the San Raffaele Hospital in Milan, Italy [Dalt05].

The survival of passive transponders from vein to vein was evaluated at the University Hospital in Graz, Austria [Wagn06a]. The results are quite promising if we take into account that off-the-shelf transponders were used (see 3.2.8).

Continuous temperature monitoring is already possible using temperature indicator labels [Will06], i.e. stickers which irreversibly change their color if the temperature leaves a fixed range of acceptable values. They can be used only once and have an accuracy of about ±1°C for temperatures from -10°C to 40°C. Their lifetime ranges from a few hours up to some weeks. A disadvantage we encounter is their immediate reaction to surfacial heating, e.g. when they are touched or near to a radiating heat source.

RFID transponders must be attached to the surface of the blood bag. The question in how far the measured temperature on the surface corresponds to the core temperature of the bag contents has been addressed by temperature measurement tests performed by MacoPharma [Zimm05]: The surface temperature adequately represents the core temperature when the transponder is insulated against the ambience (see 3.2.1).

Temperature logging requires an independent energy source on the transponder. Schweizer Elektronik AG [Ocke06] has performed foil accumulator tests with respect to long time de-charging and exposure to physical strain such as acceleration. A product by Infinite Power Solutions [Infi04] has been detected which satisfies the requirements (see 3.2.7).

The University Hospital Graz, Austria, will start survivability tests during blood processing with semi-active tags equipped with this battery technology in 2007 [Wagn06b].

Technopuce [Tech02] has developed a temperature monitoring tag especially targeted at blood conserves, Hemotag, in 2002. Tests by MacoPharma have been aborted because they did not yield the expected results [Zimm05].

Novatech Research performed tests in cooperation with the General Hospital Vienna, Austria, in development of their Liquid Control Unit [Nova05]. The results were rather disappointing [Kurz05].

Möller Medical [Schr05] announced to integrate RFID features into their blood mixer equipment ”Docon”. Re-entering of data collected during donation could be made superfluous and thus ultimately confusion can be reduced.

1.3 Overview

This section outlines the contents and the structure of this thesis.

Chapter two gives an overview of the fundamentals. First of all the blood supply chain is examined and presented in detail; then important prerequisites of RFID technology and temperature sensing are given.

Chapter three describes the requirements on the system originating from the blood supply process, the transponder, the temperature logging functionality and the whole system in general.

Chapter four discusses general concepts of RFID system design and gives proposals for embedding an RFID system into the blood supply chain. In the course of this work an edgeware framework has been implemented demonstrating the technical feasibility of RFID-based temperature monitoring.

Chapter five deals with further aspects of an RFID-based solution concerning bulk detection, RFID middleware and tracking and tracing systems as well as standardization issues.

Chapter six discusses the properties of the system, economic aspects, open problems and gives a prospect to the future.

Further applications of RFID-based temperature monitoring are described in chapter seven.

The conclusion summarizes the results of the work.

Chapter 2

Fundamentals

RFID-based temperature monitoring of blood bags involves three basic topics: the blood supply chain, RFID technology and temperature monitoring.

An in-depth understanding of the blood supply chain is required for designing a blood bag temperature monitoring system. The first section of this chapter gives fundamental background information on blood and blood bags before analyzing in detail the current blood supply chain processes.

The second section delivers an introduction to RFID technology, especially to issues used in the reference implementation work described in this thesis.

The third part deals with the basic elements of temperature sensors and temperature measurement which are of specific relevance and must be kept in mind during system design.

2.1 The Blood Supply Chain

The blood supply chain is a logistic process which is controlled by medical factors. A basic understanding of medical terms and problems involved with blood, blood processing and blood transfusion is therefore necessary. In Europe blood logistics generally do not cross national or even regional borders. Only in case of bottlenecks blood products are requested from neighbouring organizations. The blood supply chain is analyzed in detail by an example. We concentrate on the processes and their circumstances, as well as the spatio-temporal relationships of the tasks.

2.1.1 Organization

Actual blood supply conditions vary heavily between developing and industrialized countries, thus the WHO (World Health Organisation, www.who.int) aims at raising the standards throughout the world. The ISBT (International Society Blood Transfusion, www.isbt-web.org) deals with the essential medical issues; the ICCBBA (International Council for Commonality in Blood Bank Automation, www.iccbba.com) aims at unifying blood supply on a worldwide scale.

In Europe blood supply is performed by the Red Cross and public health institutions. Blood logistics is either organized *centrally*, e.g. in France where 18 regional blood donor centres (EFS, établissement français du sang, about 2.5 millon products per year [OBIG04]) are directed centrally; or in a *federated* way, e.g. in Austria where 13 independent donor centres which issue about 543800 products per year [OBIG04]; or to a further extreme each hospital performs it independently as in Denmark. Nonetheless, a European-level haemovigilance network (www.ehn-org.net) for blood supply chain surveillance has been founded in 1998. Due to the short storage life span of blood products a regional structure for blood supply is obvious, although a supra-regional cooperation is advantageous.

2.1.2 Blood and Blood bags

Blood is composed of liquid, the *blood plasma*, which makes up the major part, and *blood cells* of which 99% are red blood cells or erythrocytes and the rest being different types of white blood cells or leucocytes, and platelets or thrombocytes. About 80% of transfused blood products are *erythrocyte concentrates*, i.e. *blood conserves which consist to their largest extent of erythrocytes* (value per bag about 105€) [Parr03].

Blood is collected using a blood bag system (about 13€ [Wagn06b]) which normally consists of four PVC (polyvinyl chloride) bags and a filter connected by tubes (see Fig. 1). The whole blood is collected in the collection bag; after centrifugation plasma and erythrocytes are separated in the respective bags; the erythrocytes are filtered and finally stored in the fourth bag for transfusion.

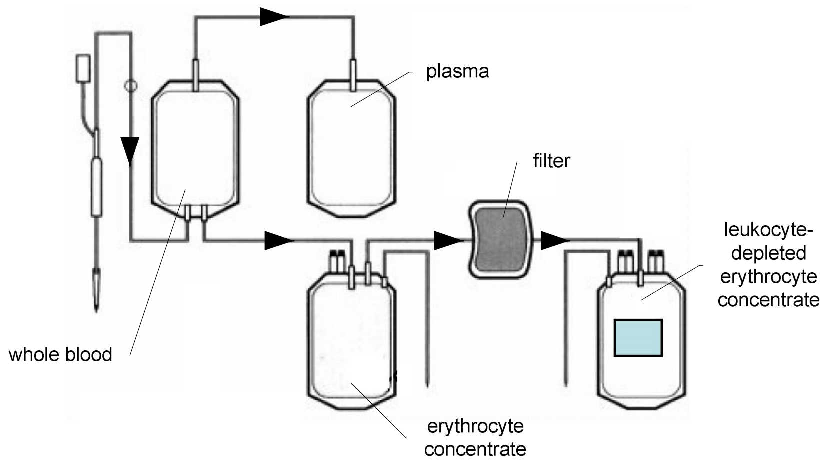


Fig. 1: Blood bag system

The whole blood donation is collected in the leftmost bag. After the centrifugation the plasma and erythrocyte concentrate are separated in the respective bags. The erythrocyte concentrate is filtered and stored in the rightmost one until transfusion. (cf. www.macopharma.com)

Blood is tested in order to determine its compatibility properties. Blood types [Psch98] differ in the presence or absence of antigenes on the erythrocytes. The main blood types are A, B and 0, if none of these antigenes is present. Another factor are the Rhesus antigenes of which D is most important; Rhesus positive means that the antigene D is present. There is a number of other properties e.g. Kell antigenes. An incompatibility of the transfused and the patient's blood will result in a transfusion reaction. For example if A,B, and 0 blood types are confused (currently about 1:12000), antibodies are produced which result in a haemolytic reaction which causes circulatory disorders and organic failure and which could end up lethally in 2% of the cases. Most common transfusion reactions are not related to blood types: Fever and shivering fit are often caused by immunoreactions due to the remaining (not filtered out) leukocytes. Severe, but much less frequent problems arise from contaminated blood conserves, e.g. by HI (human immunodeficiency), HB (hepatitis B), and HC (hepatitis C) viruses [Dalt05].

2.1.3 Supply Chain Example

The analysis of the supply chain is illustrated by an example of the blood donor centre of Styria situated at the University Hospital Graz, where approximately 65000 whole blood conserves (about 12% in Austria) are processed per year [Wagn06a].

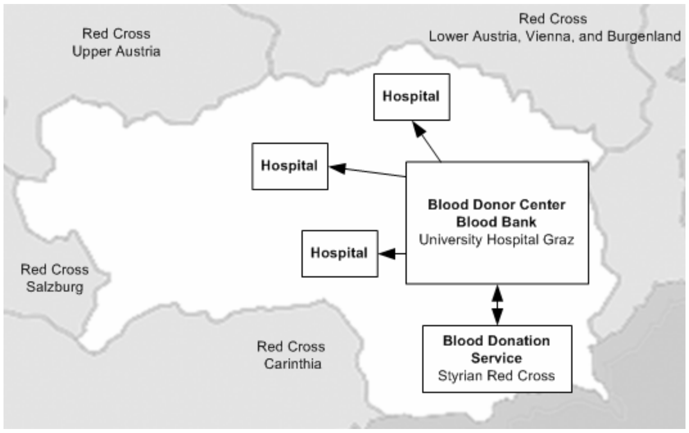


Fig. 2: Blood supply organization in Styria

The majority of hospitals are part of the Styrian Hospital Association (Steiermärkische Krankenanstaltengesellschaft). The donations are collected by the Red Cross, and processed and distributed by the University Hospital Graz.

A blood centre (or blood establishment) is responsible for the blood supply of a region. It organizes and coordinates the donation activities, performs the blood processing, administrates the donation and donor data and distributes the blood products.

The blood centre orders the blood bags from a blood bag manufacturer and distributes them to donation services.

Donation services perform the necessary donation activities. They are responsible for the selection of donors, the identification of the collected whole blood and the test probes and perform the collection itself. The donated blood is cooled down to room temperature (20 ±2°C) [Wagn06b] and transported in between of cooling plates in cooling boxes to the blood bank.

The blood bank performs the blood processing, the laboratory analysis of the samples, stores the released blood bags and distributes them. The blood processing encompasses the following steps, which are performed at room temperature: The bags are weighed; plasma and erythrocytes are separated after centrifugation and leukocytes are filtered out subsequently. The blood bag system remains closed from the donation until transfusion. Each blood bag system yields one bag of leukocyte-depleted erythrocyte concentrate which must be stored at 4 ±2°C, and one bag of blood plasma which is deep-frozen at down to -30°C [OGBT00]. The processing must be finished within at most 24 hours after donation [Wagn06b]. In parallel the blood probes are tested: The blood types are determined (usually AB0, Rh, and Kell) and an antibody test is performed to find out contaminations. After receiving the test results from the laboratory the bags which are proper for use are labelled and released. Contaminated bags are discarded; in case of a health hazard the donor will be informed. There are different storage areas for processed, but not released and for released, distributable bags. The maximal storage life of erythrocyte concentrates is 42 days [OGBT00].

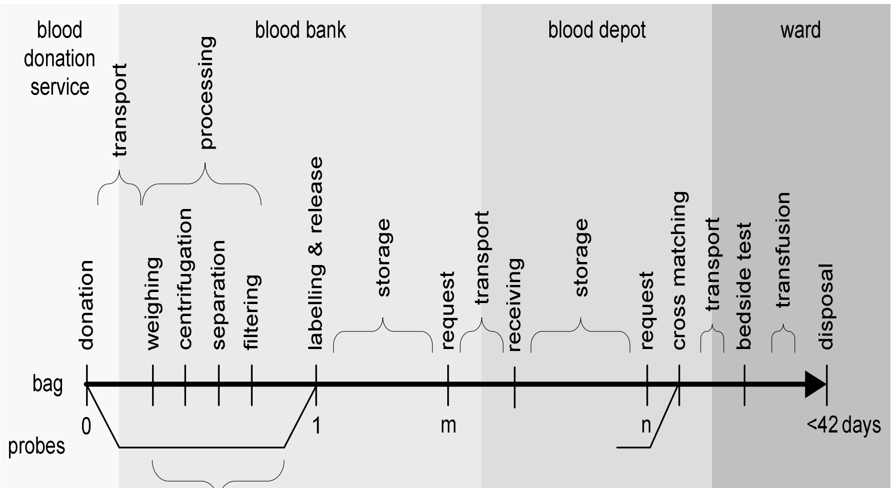


Fig. 3: Blood supply chain on the timeline

The blood bags pass through the institutions from donation to transfusion within at most 42 days.

A hospital blood depot obtains the blood products from a blood bank. The transport of erythrocyte concentrates is performed in boxes with cooling plates at a temperature between 2°C and 10°C [BMSG02]. Blood depots are the centre for documentation of storage, use, disposal and haemovigilance, i.e. reporting on transfusion problems and notification on undesirable side effects of drugs. Hospitals where the blood products must be stored for more than six hours have their own blood depot and a laboratory for blood analysis. Hospitals without a blood depot request their blood bags directly with test probes at the blood bank or neighbouring blood depots where the cross-matching is performed. Blood depots are responsible for the blood supply of a hospital and therefore they have to perform strategic warehousing in order to meet the expected demand for at least two days [BMSG02]. On receiving the blood products the transport documents are checked. The blood bags are stored in a continuously temperature-monitored blood refrigerator. A hospital ward orders a blood product for a particular patient including test probes which are used to perform the cross-matching to determine the required compatibility. The transfusion compartment of the blood bag must in any case remain closed until transfusion; thus the blood is either taken from test tubes delivered with the bag or from tube segments of the bag; a last possibility to get blood for cross-matching is welding-off a corner of the blood bag. Tests on AB0, Rh(D) and blood group antibodies are performed. The whole procedure including documentation takes up to two hours [Wagn06b]. Cross-matching is performed in any case, even in case of emergency, although the bag can be shipped before the test has been finished [OGBT00]. Dependent on the proximity the transport to the ward is performed in a cooling box.

Hospital wards are the blood consuming institutions. Previously labelled blood probes are taken from the patient and are sent together with the request to the blood depot. Temporary storage in a cooling box before use is possible if the transport temperature requirements are fulfilled and proper documented [BMSG02]. Once warmed up above 10°C erythrocytes are not allowed to be cooled down again, thus the transfusion must be finished within six hours or the bag must be disposed [BMSG02]. As a rule of thumb it can be said that a blood bag is warmed up above 10°C when it is exposed to room temperature for about 30 minutes [Wagn06b]. The doctor performing the transfusion checks the matching between the patient's identity and the document accompanying the blood. He/She poses a question to which the patient – if conscious – responds with his/her first and second name and the date of birth [OGBT00]. Furthermore it is checked if it is the right ward and room, the bag number in the document is the same as on the bag; expiry date and the physical integrity of the bag are also controlled. Before transfusion the patient is informed about the risks. In any case a bedside test is performed at the patient's bed: A blood sample is taken and the correspondence of AB0 and Rh(D) is once more checked on test cards or in test tubes using test liquids directly beside the patient's bed. This takes one or two minutes [Wagn06b]. All testing material has to be kept until the transfusion is finished. Warming up the blood is only allowed in certified appliances under certain indications. Then the transfusion is started. In case of transfusion reactions the transfusion is aborted, the bag with the remaining blood and all blood probes are returned to the blood depot for analysis in order to determine the reasons. After transfusion the patient is observed for another 30 minutes [OGBT00]. A transfusion report is also sent to the blood depot if the transfusion has been successfully finished. Sometimes blood bags are not used because e.g. for operations there is more blood requested in advance. The blood depot can only take them back if it can be proved that they have not been warmed up. The blood depot forwards the transfusion reports to the national haemovigilance organization [BMSG02].

2.2 RFID Technology

RFID (radio frequency identification) is not a new technology. Its predecessor technologies were used in the 1940ies by US and UK military; since the 1960ies it is used for electronic article surveillance and in the 1980ies it found an application in animal identification [BSI04]. In the 1990ies – as RFID systems became cheaper and more powerful – it gained major importance in logistics. An excellent overall presentation of RFID technology can be found in [Fink03]; thus this chapter gives only an overview on basic technology fundamentals which are necessary with respect to the given application and it summarizes the properties of RFID systems, their possibilities, strengths and weaknesses.

2.2.1 Overview

RFID is an RF-based wireless identification technology, such as a barcode is an optical identification method. Objects are tagged with a device providing RFID, which is generally called tag or transponder (short for transmitter/responder); quite flexible ones on paper or foil are addressed as smart label; credit card like tags are called smart cards. We will use the term transponder throughout this work. A transponder's main capability is communicating a worldwide "forever" unique serial number through a wireless communication channel on request. Object identification is provided if the transponder is attached to a single object with a common lifetime. The transponder only transmits data on request by a read/write device – normally called *reader* as this term originates from the barcode world where labels can only be read – other terms are interrogator, or transceiver (short for transmitter/receiver). In the following we will use the term "RW device" which emphasizes its capability of reading from and writing data on the transponder.

An RFID system (see Fig. 4) consists of a transponder, an RW device and as a third component a computer system – in the simplest form a host computer. Transponders and RW devices are both equipped with antennae and communicate via radio waves. The host computer and the RW device are usually connected by wire using serial or network interfaces.

The variety of RW devices ranges from plug-in cards for handheld devices as PDAs (personal digital assistants) up to industrial appliances supporting several antennae. RW devices are targeted at a single RFID technology. The RW device has to be configured with respect to its communication parameters e.g. RS232, USB or Ethernet interface and antenna tuning. RW devices are often capable of communicating to several transponders in its range at the same time. This is called multi-tagging or bulk detection (see 5.1). Medium access mechanisms for anti-collision must be provided in the communication protocol to distinguish the signals from different transponders. For more information on the RW devices used for the prototyping implementation see 4.3.7.

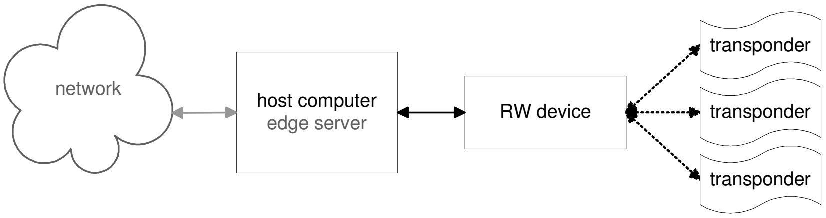


Fig. 4: RFID system

The RW device links the transponders and the computing systems. A computer forming a gateway between the RW device and the rest of the network and thus situated at the edge of the network is called edge server.

A transponder consists of an antenna, a rectifier circuit, and a chip which implements the transponder's functionality. Normally, it is a finite state machine entirely realized in hardware; some high-end transponders have a microprocessor. The alternating electromagnetic field generated by the RW device's antenna is used to transfer both energy and data. When the transponder comes into the field it becomes powered and the circuit is reset. Also the clock signal is derived from the field frequency. The minimum data stored on a transponder is its unique identifier (UID). Currently, the memory capacity of transponders with non volatile memory, mostly EEPROMs, is typically about 10kbit. Transponders may also have further computational and sensing capabilities (cf. [Want04]) and security functions (see Fig. 5).

Transponders are categorized by different properties, which are intrinsically linked. Passive transponders do not have their own energy source but take the energy from the RW device's field, whereas active transponders are equipped with e.g. a battery. Active transponders emit radio waves; whereas passive transponders use backpressure mechanisms on the RW device's field for communication. Semi-active transponders are those which communicate as passive transponders but have a battery for internal functions, e.g. periodic sampling of sensor data, which need a permanent power supply [Flei05].

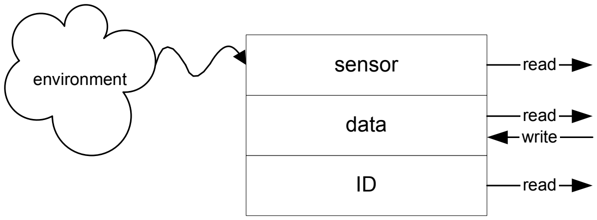


Fig. 5: Transponder capabilities
.(see text)

A second distinguishing property is the communication range. Close-coupling means up to 10cm; remote or vicinity coupling up to 1m, and long range lies beyond [Fink03]. In short range technologies the transponder is in the near field of the RW device, i.e. they are inductively coupled, which works like a transformer. Data is returned to the RW device using load modulation. In long range technologies the transponder is in the far field – so called electromagnetic coupling –, and the response is sent using backscatter modulation [Fink03].

The main property which differentiates RFID technologies is the radio frequency used. Low frequency (LF) technologies uses the band from 10kHz to 135kHz. High frequency (HF) uses 13.56MHz; in the ultra high frequency (UHF) range the bands are different in Europe, the US and Japan, lying between 868MHz and 956MHz. Microwave (MW) at 2.45GHz and 5.8GHz is also in use [Fink03]. LF and HF work in the near field and allow for a higher reader density because of the short range. UHF is also used for many other applications as mobile telecommunication and has strict regulations by law, such as transmission power restrictions (see 3.1.2). The long range makes RW device anti-collision necessary; therefore a listen-before-talk mechanism must be applied [Eede04]. A higher frequency allows for higher communication speed but involves other problems: Only LF cannot be easily shielded by metals. UHF and MW suffer from heavy absorption by liquids. Metals pose a general problem as reflexion and scattering is concerned [Fink03].

The normal operation sequence of communicating with a transponder is depicted in Fig. 6. First the RW device has to perform an inventory, i.e. it collects the UIDs of the transponders in its field. In applications where only the UID is needed RW devices are often configured to continuously scan for transponders and return their UIDs. If multi-tagging is enabled, a transponder must be selected before another command (e.g. read from or write some data on a transponder) can be issued.

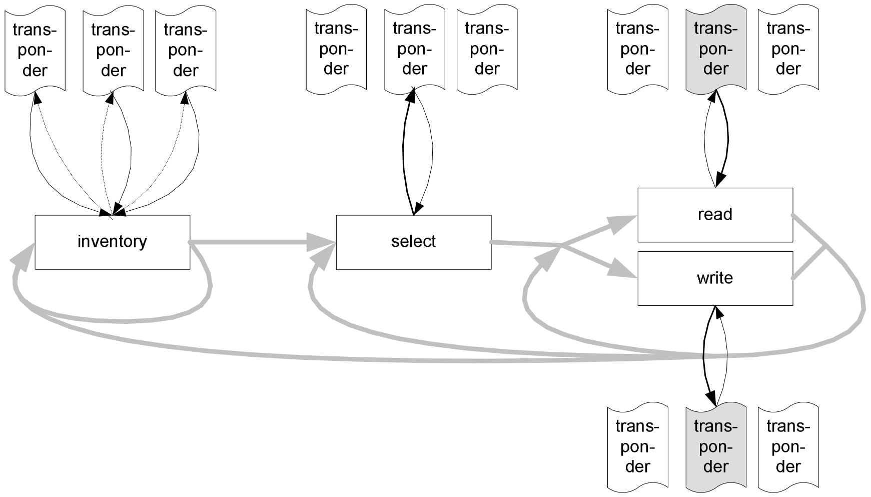


Fig. 6: RW device operation sequence
.(see text)

RFID transponders are widely seen as a substitution for barcodes, as they show a lot of advantages:

- RFID allows faster automatic reading without human intervention because no line-of-sight is required. Several transponders can be read “at once” [McFa03]. Long range RW devices make a bulk detection of an entire palette possible; however, transponders can be read without being recognized which poses privacy problems (see 2.2.4).

- Transponders are not or less sensitive to dirt, moisture, abrasion and other adverse environmental conditions [McFa03]. They have a lifetime of at least ten years [Pfla02].

- Data can be both read and written. A higher data capacity is possible. The data is not human readable; they cannot be forged as easily as a barcode, on the other hand an object is unidentifiable if the transponder is defect, respectively the data stored on it is lost.

Summarizing, it has to be said that none of the currently available RFID technologies can be regarded as superior in all respects. The choice of the right technology always depends on the application.

2.2.2 HF, 13.56 MHz, Inductive Coupling, and ISO 15693

One of the most widely deployed RFID technologies works in the high frequency band at 13.56MHz. There are several standards which define transponders and communication between transponders and RW devices. The ISO (International Organization for Standardization) 14443 [ISO01a] defines the proximity integrated circuit cards (PICC) which work at a maximum range of 10cm and allow for a transmission rate of 106kbit/s. They are mainly used for high-end applications as electronic wallets where much energy is needed to power a processor for cryptographic operations. ISO 15693 [ISO01b] defines the vicinity integrated circuit cards (VICC) which work at a range up to 1m and are designed for low-end applications. Recently, the ISO has started to unify RFID technologies standards for item identification in ISO 18000 [ISO04c], in which part 3 is dedicated to 13.56MHz technology which corresponds essentially to ISO 15693.

In the following the 13.56MHz RFID technology is explained with the example ISO 15693, which has also been used in the prototype implementation. The unique ID consists of 8 bytes, the first byte containing 0xE0, the second one a code identifying the transponder manufacturer and a 6 bytes serial number. Furthermore there is a 1 byte application family identifier (AFI) which can hold (partly) predefined codes to distinguish transponders from different application domains during inventory.

The coil antennae of RW device and transponder are both tuned to the same resonance frequency. They must be oriented in parallel in order that the alternating magnetic field induces the maximum current in the transponder's coil. The magnetic field strength decreases with the inverse cube of the distance to the antenna. The interrogation field strength ($[H_{min}]$=A/m) is the minimum field strength which allows for scavenging a voltage sufficient for powering the transponder. The energy range ([r]=m) is the maximum distance at which the energy is still sufficient for powering the transponder, i.e. where the field strength falls below the transponder's interrogation field strength [Fink03].

If the internal impedance of the transponder is altered the amount of energy drawn from the magnetic field is changed. Thus the transponder reacts upon the field and consequently the voltage in the RW device's antenna changes and can be detected. This mechanism is called load modulation [Fink03]. Because of the loose inductive coupling of the two antennae the signal produced by load modulation is quite weak. For an RW device antenna voltage of 100V the signal is normally not higher than 10mV. Therefore subcarriers at 484kHz are used for transmission in the backward channel. This mechanism needs a higher bandwidth but the signal can be easily separated from the RW device's signal by a bandpass filter [Fink03].

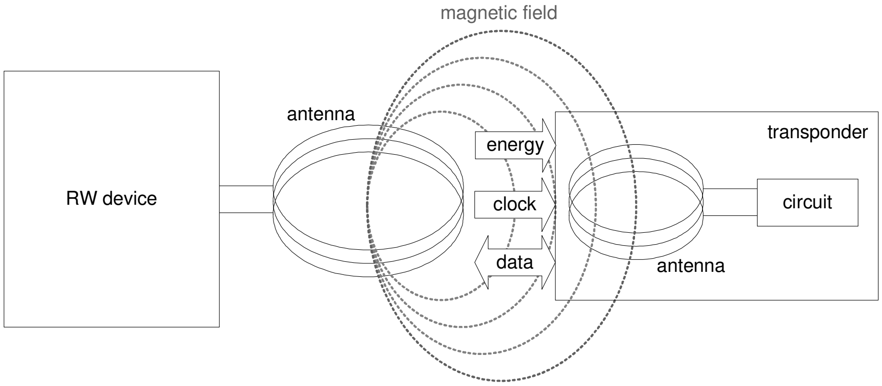


Fig. 7: Inductive coupling
The transponder is in the near field of the RW device's antenna. The alternating electromagnetic field supplies the transponder with energy and a clock signal while data is transferred. (cf. [Fink03], [Flei05])

An ISO 15693 transponder has to support two communication modes: long distance mode and fast mode; and two modulation techniques: amplitude shift keying (ASK) and frequency shift keying (FSK). Normally, ASK is used with a pulse position modulation (PPM) with 10% amplitude suppression and a 1 of 256 encoding in long distance mode and a 100% amplitude reduction (on-off-keying in fact) with a 1 of 4 encoding. Long distance mode enables a range up to 70cm at a rate of 6.62kbit/s; fast mode up to 30cm and 26.48kbit/s [Fink03].

An advantage of 13.56MHz technology is that it enables to manufacture very cheap labels with printed or etched coil antennas on paper or foil in credit card format or even smaller (see Fig. 8). Therefore it is the most widespread technology at the moment. It is highly standardized and uses a licence free ISM (industrial-scientific-medical) frequency range. The data rate is higher than for LF technology and the frequency is reasonably high for providing a processor with a clock signal. The absorption by water is much lower than for UHF technology.

As main disadvantages we have to mention its short range and the reflexion by metals. More details on the transponder used in the prototype implementation can be found in 4.3.7.

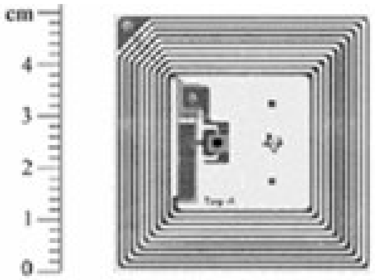


Fig. 8: Passive smart label
(Tag-it™, www.ti.com)

2.2.3 Applications

As pointed out in 2.2.1 RFID shows a series of advantages as an automatic identification and data collection (AIDC) technology. An RFID transponder serves as a bridge between the physical and logical world and makes the physical world accessible for computer systems. RFID technology can be employed in different manners in an application.

In an *open-loop application* the transponder is attached to an object which runs once through the business processes and is discarded at the end of the object's lifetime or even before, e.g. consumer articles. When transponders are employed in a *closed loop* the object and thus the transponder passes several times through the same processes, e.g. freight containers which are used more than once.

A second property is the way the transponder is used: The transponder may only provide low end functionality such as identification or it may be used for autonomous sensing operations. Fig. 9 classifies typical RFID application domains which are described in the following sections using these properties.

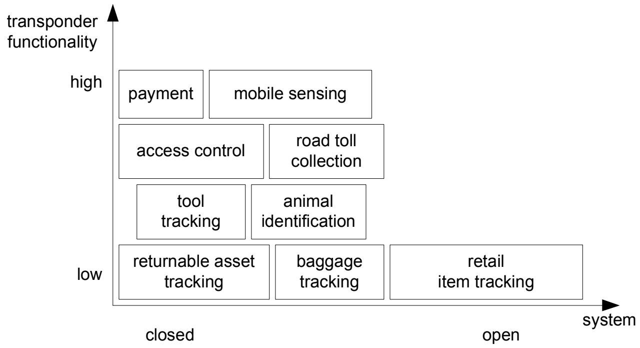


Fig. 9: RFID applications
classified by the required transponder functionality and the system's openness respectively closeness.

One application domain is *security*. RFID technology has already been successfully deployed in applications ranging from primitive electronic article surveillance (EAS) over vehicle anti-theft systems, product authenticity control and access control in skiing areas, enterprise time keeping systems up to contactless payment systems [Flei05].

The currently most important field spans logistics, supply chain management (SCM), and transportation. Tracking and tracing (see 5.2.1) of products, efficient loading and automatic verification of shipments on receiving are only some of the keywords which promise to revolutionize logistics. The granularity of tagging can be on a pallet, carton, or item level. Tracking of returnable items such as containers is already widely employed [McFa03]. In retail an increase of availability coupled with a reduction of warehouse space can be achieved through continuous inventorying. Self-check-out cashdesks are simplified while preventing from theft [McFa03].

Other promising applications are the tracking of parts and assemblies during manufacturing or processing goods, tracking tools and documenting tools usage and wear out, and the identification of parts in complex assemblies for finding the right spare parts are other promising applications. Packet sorting and airline baggage tracking are examples for applications where the increase in reliability can be directly noticed by the customer. Other domains which can profit from RFID deployment are product life cycle management, waste management and recycling of goods containing valuable or dangerous substances. RFID technology is already used for a long time in animal identification, and also currently in libraries, sport time recording and road toll collection. At the very high-end mobile sensing applications for scientific purposes and environmental monitoring have to be mentioned. Further applications are real time localization of objects and the vision of smart things which are able to communicate with stationary appliances and with each other – known as ubiquitous or pervasive computing.

However, the use of RFID technology does not only involve the tagging of objects but it also means a lot of new challenges. An RFID infrastructure consisting of transponders, RW devices, networks of computers hosting distributed applications must be managed and maintained. Furthermore big amounts of data have to be efficiently processed. A detailed discussion of RFID middleware systems is given in 5.2. But solely to collect data is not enough; actually, it is necessary to interpret the data in a way that is possible to draw actual value from data for an enterprise, so that the advantageous effects of the RFID deployment can be economically assessed.

There are various paradigms (see also 4.1.1) of RFID use. The most primitive and cheapest transponders carry only a UID which is used as “a pointer to a database record” [Rana05], where the object information is looked up. In this extreme case an RFID transponder is no more than a barcode with advantages in reading. Another paradigm concerns more sophisticated transponders for high-level applications where the transponder is used as a portable data store and distributed computing device. In case of a sensor equipped transponder it is even capable of gathering information about its environment.

2.2.4 Problems

Besides the successful RFID deployment there are still some negative aspects encoutered.

False negative reads in multi-tagging [Floe04] occur when many transponders are concurrently in the field and some transponders remain undetected. This problem is especially addressed in 5.1.

Another problem concerns security aspects which result in the fact that RFID technology is not yet broadly accepted. The most common argumentation is related to privacy because transponders can be read out without being recognized and thus people can be tracked by the transponders attached to the things they wear [Weis04], i.e. location privacy is violated. This might cause in particular a problem for RFID applications with long range technologies. RFID systems suffer also from the same security problems [BSI04] as all other computer systems such as intrusion, i.e. unauthorized access, and data manipulation. Even more weaknesses result from relations to the physical world and there are really a variety of possibilities of preventing RFID systems from working correctly: Cloning of transponders, thus yielding two transponders with the same ID compromising unique identification; blocking, i.e. preventing other transponders from being detected or read by disturbing the anti-collision mechanism, occupying or jamming the communication channel, de-charging of batteries of active transponders, shielding, detachment from the object or mechanical destruction. There are many ideas of thwarting these security threats [Weis04] [Rana04] [BSI04], but since severe cryptography methods – the only sufficient means of guaranteeing security in traditional computer systems – are far from being realizable on small low cost computation devices as transponders, the problems are still not settled in current systems. In closed-loop applications (where key management is easier), close-coupling systems (where the transponder receives enough energy for more complex processors) mutual authentication of RW device and transponder is employed [Phil05b].

An RFID system is required to be highly reliable since the whole business process of an enterprise becomes increasingly dependent on it. Although the advantages of RFID systems, e.g. in logistics, are obvious, the economic benefits and efficiency measured by the return-on-investment (ROI) are not clear [Flei05].

2.3 Temperature Sensing

Temperature monitoring requires temperature sensing, i.e. the temperature must be measured by a device integrated in the RFID transponder. The knowledge of some basic properties of temperature sensors [Frad04] and the understanding of general problems involved with temperature measurement [Mich01] are regarded as prerequisites for reading this section.

2.3.1 Overview

Temperature is an aggregate property of a substance, which cannot be directly measured. Thus temperature sensors make use of temperature-dependent properties of materials, e.g. the resisitivity of platinum increases with increasing temperature, the temperature of a platinum wire can be determined e.g. by measuring the voltage between its ends while a constant current runs through it [Frad04].

There are a couple of different temperature sensor types [Mich01] relying on different physical principles: There are sensors which determine the temperature without getting in direct contact with the investigated body, such as pyrometers which measure heat radiation. Most sensors require to be in contact with the substance either on the surface or by being dipped into it. There are non-electrical sensors which mostly work on the principle of thermal expansion, e.g. mercury thermometers. Electrical sensors use special thermoelectric effects, e.g. the Seebeck effect which thermocouples take advantage of, or the modulation of electrical quantities by temperature, such as the resisitivity of conductors, e.g. platinum, and semiconductors, e.g. in thermistors, diodes and transistors.

The transfer function [Frad04] of a sensor describes the overall relation between the quantity to be measured and the output of the sensor. It is desired that the output is linearly proportional to the temperature:

$$u(t) = d + k \cdot T(t) \tag{1}$$

Normally, the relation is almost linear with some non-linearity error within a certain range and saturation effects towards the ends (see Fig. 10) [Frad04].

The signal is conditioned to meet the sensor's output needs and to make it more stable (see Fig. 11) [Gyge05]: It is amplified, rapid changes caused by noise are smoothed by filtering, the offset (constant *d* in formula (1)) of the transfer function is corrected, and it is linearized if necessary. The sensor output has to be sampled and quantized in order to be used in a computer system which is performed by an analog-digital converter (ADC). The resolution depends on the quantization steps of the ADC. Normally, the full sensor output range is mapped to 8 up to 16 bits [Opas06].

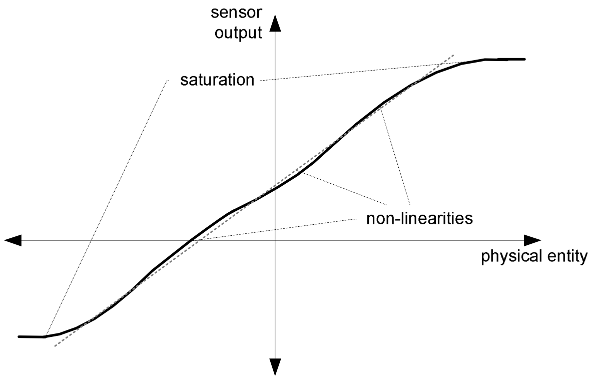


Fig. 10: Sensor output properties

A typical transfer function with an almost linear relationship within a certain range and saturation at both ends of this range (cf. [Frad04]).

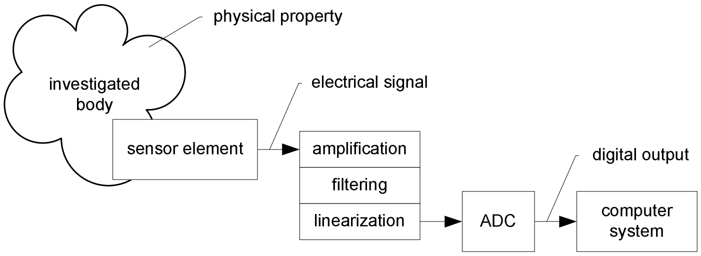


Fig. 11: Sensor system

The physical property to be measured is transformed into an electrical system. After signal conditioning steps digitalization makes it processible for computer systems (cf. [Gyge05]).

An important property (especially in experimental physics and industrial applications) is repeatability, i.e. two measurements should return the same value if the temperature is constant. Another requirement is long term stability, i.e. under constant conditions the issue that the measured value gradually changes with a certain tendency over time [Frad04].

2.3.2 Integrated Semiconductor Sensors

Semiconductors exhibit a strong linear dependency between conductivity and temperature in the range between -50°C and 150°C; the nonlinearity is usually less than ±3% [Frad04]. Diodes and transistors can be used for temperature measurement because the behaviour of their PN-junction(s) is influenced by temperature. Temperature sensors can be integrated directly into chips by two transistors using the following principle called PTAT (proportional to absolute temperature) [Mich01] [Opas06]: The difference between two base-emitter junction voltages is directly proportional to the absolute temperature when the two emitter currents are not equal but at a constant ratio. The transfer function is expressed in formula (2) [Mich01]:

absolute temperature *T*, voltage PTAT V_T, constant circuit parameters *k, q, r*

$$V_T = T\frac{k}{q}\ln r \tag{2}$$

Sensor accuracy does not only depend on the good modelling of the transfer function but it is also degraded by power supply noise, thermal noise of the circuit and clock jitter during AD conversion. Therefore an RFID transponder equipped with a temperature sensor should not be in the field while the temperature is sampled [Opas06].

2.3.3 Properties and Problems

A temperature sensor generally represents a first order dynamic system, because the sensor element itself and its package must be warmed up to the temperature of the measured medium. Thus a temperature sensor exhibits dynamic errors until steady state is reached. The smaller the sensor, the faster the reaction. The dynamic behaviour is specified by the time required to reach 90% of steady state or by the time constant of the exponential function describing the step response (corresponds to 63% of steady state) [Frad04].

Anyway the sensor must be brought into contact with the investigated body. In case of blood bags this is by contact on the surface of the bag. The best solution, mounting the RFID transponder in the bag, in the centre of the concentrate, poses both hygienic and technical difficulties. The sensor interacts with the surface dependent on the specific thermal conductivity of the materials involved. The step response on the surface is obviously different to the temperature measured within the substance, because the sensor is not entirely surrounded by it [Mich01]. In case of blood bags the blood temperature does not change itself but is changed by the ambient temperature. A surface sensor reacts faster than the blood in the beginning but a steady state is not reached earlier (see Fig. 12). The dependency between the bag content's temperature and the sensor temperature can be improved by increasing the contacting surface, reducing the thickness of the layers in between and using materials of higher specific thermal conductivity and by insulating the sensor against the ambience [Mich01].

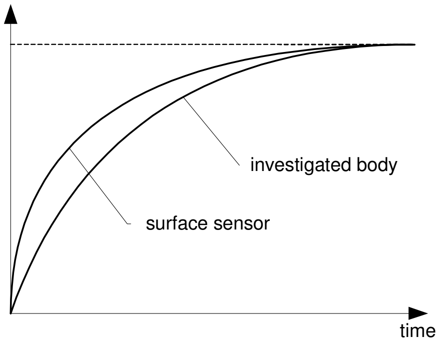


Fig. 12: First order response
of the investigated body and the surface contact sensor's response to a step in ambient temperature (cf. [Frad04])

Dynamic errors can be corrected by applying a dynamic correction filter which compensates for the temporal effects [Mich01]. A practical problem has been observed with RFID RW devices with an integrated antenna which radiate big amounts of heat and thus warm up the blood bags and disturb the measurement process.

2.3.4 Calibration

Calibration means bringing the real value of the quantity and the sensor output closer together by applying a function to the sensor output. Calibration is normally performed using fixed points, e.g. defined in the ITS-90 (international temperature scale), practically points with lower accuracy are widely used, e.g. the ice or boiling point of water (0°C resp. 100°C). Laboratory calibrators have an inaccuracy of about 0.3°C down to 0.03°C [Mich01].

A sensor with a linear transfer function requires at least two calibration points for correcting both, offset and slope. The sensor output is read for two points and a correction function is calculated as shown in formula (3) (cf. [Frad04]).

calibration points $(T_1, T_{1,sensor}), (T_2, T_{2,sensor})$

$$T_{measurement} = \frac{T_{sensor}(T_1 - T_2) + T_1 T_{2,sensor} - T_2 T_{1,sensor}}{T_{2,sensor} - T_{1,sensor}} \qquad (3)$$

Calibration is often performed computationally by the computer system processing the sensor data, thus called digital calibration [Mich01].

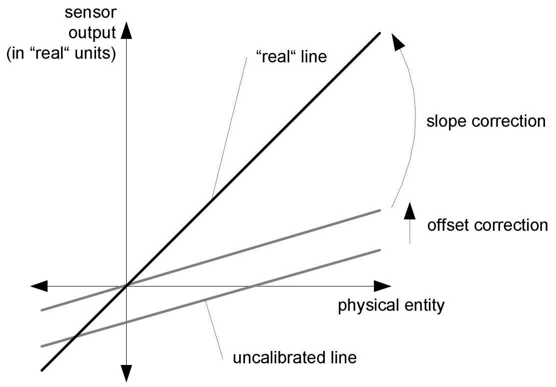


Fig. 13: Digital calibration
(cf. [Frad04])

2.3.5 Applications

A temperature sensor allows to determine the temperature at a particular instance in time. Temperature monitoring requires continuous observation of the temperature. Thus for a given application, the temperature has to be sampled at a sufficiently high frequency. Plotting the values over the instances at which they were obtained is the most common representation. In many applications [Flei05] it is required that the temperature stays within a certain temperature window defined by a lower and an upper temperature limit. In this case it is sufficient to report when the temperature falls out of this range. Nevertheless the temperature must be sampled in the same manner at regular intervals in order to be able to recognize the changes.

Mobile sensing as performed by an RFID transponder equipped with a temperature sensor implies that the measurements must be stored on the transponder at least until they are read by an analyzing computer system. Since the transponder memory is limited the values must be efficiently stored. In case of a temperature alarm system of which the only aim is to detect whether the valid range has been left a single Boolean flag is sufficient. But in most cases a more detailed representation of the temperature history or log is requested (see 3.2.2).

In some applications an object is changed proportionally to the amount of heat having acted upon it. This is of special importance in biological applications, e.g. the development of organisms is often directly proportional to the heat accumulated over time. The time-temperature product provides a mean of quantifying this heat and furthermore gives a compact representation by summarizing the temperature history (see formulae (4), Fig. 14).

temperature T_t measured at time t, upper temperature limit T_u, logging interval Δt

$$TTP(0) = 0$$

$$TTP(t+\Delta t) = \begin{cases} TTP(t) + \Delta t(T_t - T_u) & if\ (T_t - T_u > 0) \\ TTP(t) & else \end{cases} \tag{4}$$

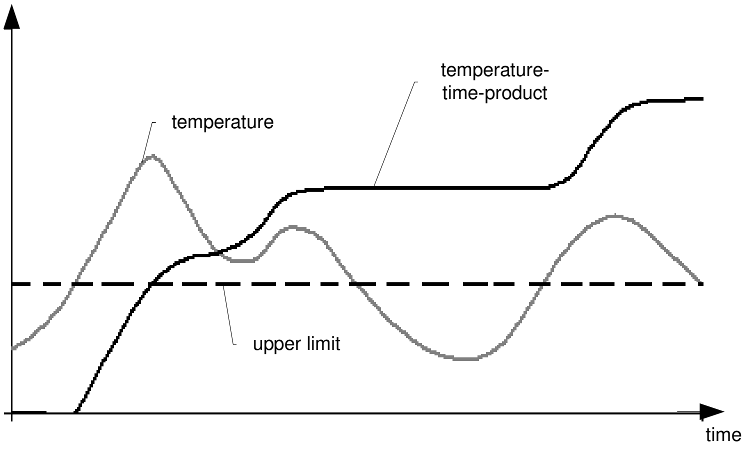


Fig. 14: Time-temperature product
It is in fact the integral over time of the temperature outside a limit.

The real value of temperature data for the different applications is its analysis. For example aggregate information (e.g. the number of times the temperature has exceeded certain limits, the mean or total duration of exceeding the allowed temperature interval) can be calculated. Furthermore it can be superimposed with other data, e.g. event logs, in order to find correlations between certain events and corresponding changes in the temperature curve.

Chapter 3

Requirements

Blood supply is a domain highly regulated by laws and guidelines. Based on the blood supply chain as presented in section 2.1.3 the emerging requirements on the system are analyzed. Special attention is put on the features of the transponder hardware which is naturally the core of an RFID-based temperature monitoring system. The processes are mainly guided by medical demands, thus the system is required to fit into these processes and the various aspects as legacy system integration, security and usability.

This chapter discusses these requirements and states different solution options. The first section is concerned with general blood supply chain issues and legal regulations. The second section deals with requirements on the transponder hardware, the third with the requirements on RW and computation devices and the fourth section considers further requirements, e.g. security and reliability issues.

3.1 Blood Supply Chain and Legal Issues

The blood supply chain (see 2.1) is a rigid process which an RFID-based temperature monitoring system has to be adapted to. EU guidelines define clear aims to be achieved in blood logistics and processing concerning traceability and product quality.

3.1.1 Blood Supply Chain Aspects

Temperature monitoring has to start directly after the donation. Two storage temperatures during lifetime, 20°C and 4°C, are identified. The desired overall temperature life cycle is depicted in Fig. 15.

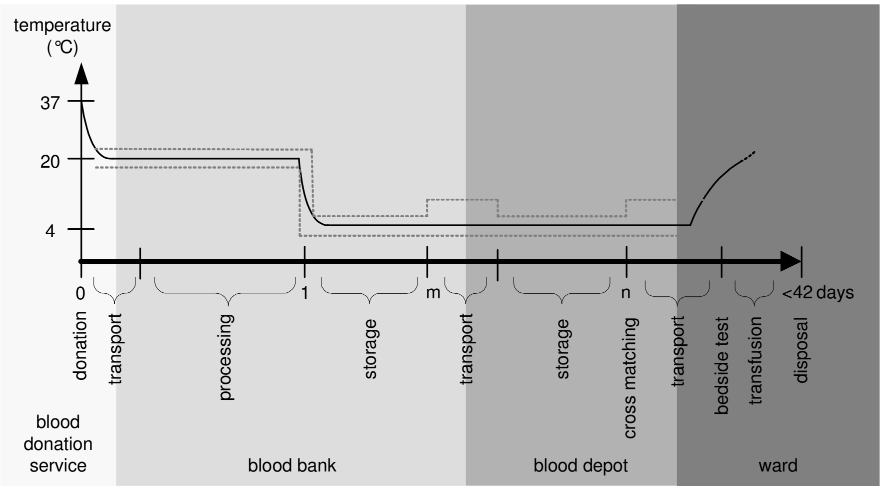


Fig. 15: Permitted blood bag temperature

After donation the blood is cooled down to room temperature; after processing it is stored at 4°C until transfusion. The dotted lines denote the acceptable temperature ranges.

Blood supply spans over several institutions which are strongly dependent on each other while being quite loosely coupled at the moment. A minimum data exchange has to be established in order to fulfil the traceability requirements (see 3.1.2).

Blood bags are handled manually. The interaction with the transponder has to be unobtrusively integrated into the current clinical process by logically accompanying it. The number of times a bag has to be handled should not be increased, by setting the points of interaction accordingly. Temperature checks have to be performed at the interfaces between the institutions, because transport is naturally the most critical phase and the receiver has to control the integrity of the product before accepting it.

3.1.2 Legal Background and Guidelines

Although blood supply is nationally or even regionally implemented it is an issue of European concern. Therefore the European Commission has enacted a series of guidelines:

- 2002/98/EC [EC02]: Setting standards of quality and safety for the collection, testing, processing, storage and distribution of human blood and blood components.
- 2005/61/EC [EC05a]: Traceability requirements and notification of serious adverse reactions and events.
- 2005/62/EC [EC05b]: Certain technical requirements for blood and blood components.

In Austria quality standards for blood donor centres are defined in the "Blutsicherheitsgesetz" (blood safety law) [BSG05]. Other relevant regulations are found in laws on medical documentation, data protection and privacy. In addition there are quality and processing guidelines of associations and institutes, e.g. the Austrian Society for Biotechnology (Österreichische Gesellschaft für Biotechnologie, ÖGBT) and the Red Cross (Österreichisches Rotes Kreuz, ÖRK) have published guidelines on blood serology and transfusion medicine [OGBT00]. Blood processing and treatment is subject to good clinical and medical practices (GCP, GMP): On international level the Pharmaceutical Inspection Convention, an organization for arrangements between health authorities, has worked out a good manufacturing practice (GMP) guide for blood establishments [PICS04].

The core clause about blood temperature monitoring in the EU guidelines is that "after blood collection, the blood bags shall be handled in a way that maintains the quality of the blood and at a storage and transport temperature appropriate to further processing requirements" [EC05b, Appendix 6.2.6]. This means that the blood bags must be verifiably stored and transported at the right temperatures which can only by guaranteed by continuous monitoring.

Moreover they define which requirements on blood bag labelling and which data has to be documented for establishing full traceability: "[…] Every blood establishment has a system in place to uniquely identify each donor, each blood unit collected and each blood component prepared, whatever its intended purpose, and the facilities to which a given blood component has been delivered." [EC05a, 2.3] "[…] All facilities have a system in place to record each blood unit or blood component received, whether or not locally processed, and the final destination of that received unit, whether transfused, discarded or returned to the distributing blood establishment." [EC05a, 2.4] "[…] Blood establishments, hospital blood banks, or facilities retain the data […] for at least 30 years in an appropriate and readable storage medium in order to ensure traceability." [EC05a, 4]

The tracing data [EC05a, Appendix I] [EC05b, Appendix, 6.2] consists of the IDs of the donation service and the donor, the date of collection, the IDs of blood bags and those establishing the connection between blood components and samples. In addition the blood bank must record to which institutions which products have been distributed. The consuming institution has to document the institution which supplied the blood component, the ID of the product, the ID of the recipient and the date of transfusion.

The ÖGBT/ÖRK guideline [OGBT00] also states which documents should be created and archived: The donation service has to justify the donor admission and document donation reactions. The blood bank keeps the laboratory testing results. The transport must be accompanied by a transport document including a temperature documentation. The blood depot: archives information about requests, the recipients, cross-matching results and the disposal of blood bags. The ward keeps a copy of the request, the bedside test results and creates a transfusion respectively haemovigilance report (in Austria: Meldung über unerwünschte Arzneimittelwirkungen (UAW)). A detailed definition of donor related documentation in Austria can be found in the Blutsicherheitsgesetz 1999 §11 [BSG05]. The Arzneimittelverordnung 2005 (drugs regulation) [ABVO05] suggests a nationally unified labelling of blood bags.

The EU guidelines demand certain reliability, security and privacy properties of the employed computer systems, of which "[…] software, hardware and back-up procedures must be checked regularly to ensure reliability, be validated before use, and be maintained in a validated state. Hardware and software shall be protected against unauthorised use or unauthorised changes. The back-up procedure shall prevent loss of or damage to data at expected and unexpected down times or function failures." [EC05b, Appendix 4.5] Furthermore it is necessary "[…] to ensure that all data, including genetic information, collated within the scope of this directive to which third parties have access have been rendered anonymous so that the donor is no longer identifiable. For that purpose, they shall ensure: (a) that data security measures are in place as well as safeguards against unauthorised data additions, deletions or modifications to donor files or deferral records, and transfer of information; (b) that procedures are in place to resolve data discrepancies; (c) that no unauthorised disclosure of such information occurs, whilst guaranteeing the traceability of donations." [EC02, Chapter VII Article 24]

RFID technology is subject to normative regulations too. The 13.56MHz technology lies in the globally free ISM frequency band, although the power radiated by the antenna is not uniformly restricted throughout the world: The European Telecommunications Standards Institute (ETSI) responsible for frequency regulations in Europe restrained it to 4W ERP (effective radiated power); the Federal Communications Commission (FCC) in the US to 3W; and 1W in Japan. The problem with UHF is that there do not exist any common global standard. In Europe the band from 865MHz to 868MHz is used. Within this range three bands with power restrictions from 0.1W up to 2W are defined. RW devices must employ a listen-before-talk scheme or they are limited to short duty cycles. In the US a range from 902MHz to 928MHz at 4W maximum is dedicated to RFID technology; in Japan it is 952MHz to 954MHz at 4W [Eede04].

3.2 Transponder Hardware

The RFID transponder is the core device of the system. Every erythrocyte concentrate bag is equipped with it in order to monitor each bag separately. This chapter defines the minimal features and essential properties of a suitable RFID transponder such as *size*, *battery lifetime* and *temperature logging functionality*. The considerations are based on ISO 15693 technology, however, the majority of concepts is technology independent. The transponder which has been used for prototyping ([KSW06], see 4.3.7] is used as a basis of the discussion. Fig. 16 shows the modules a transponder consists of (respectively its chip contains).

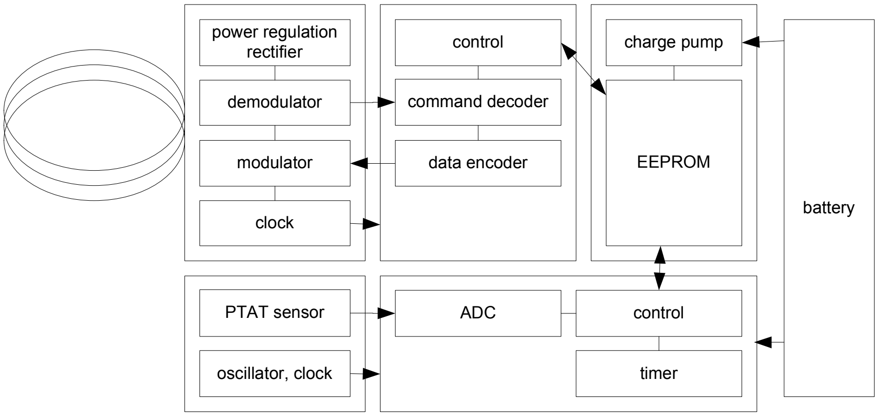


Fig. 16: Temperature measurement transponder
The leftmost modules are the analog interfaces to the antenna and the temperature sensor. The temperature logging modules have their own energy and clock source. (cf. [Opas06])

3.2.1 General Features

The transponder has to be attached to the blood bag, preferably under the primary label, which has a size of about 10x10cm. The transponder must be thin and flexible because blood bags may be folded, e.g. for putting into the slots of a centrifuge. Nevertheless it is not desired that the transponder gets folded too, so it should not be mounted centric which implies that its size must not be greater than credit-card format.

A difficulty arises from transponder recycling: Due to economic reasons the transponder should be used several times, which means that the transponder has to be easily detached while detaching is irreversible in order to prevent tampering. A possible solution is using a flap which is simply torn off as shown in Fig. 17.

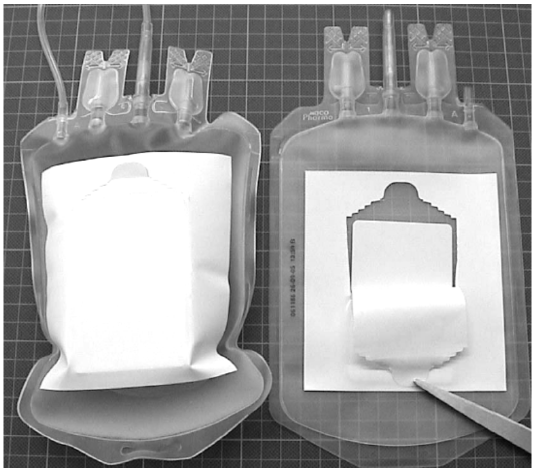


Fig. 17: Transponder mounting and detachment
[Wagn06a]

Another aspect of attaching and packaging is the good heat conductivity from the bag contents to the transponder and the insulation towards the ambience, because the temperature measured on the surface should reflect as good as possible the core temperature. PVC has a low heat conductivity (0.16 $\frac{W}{m}K$) and thus serves as a heat barrier, which on the one hand makes the bag reacting slower on changes but on the other one the temperature measurement less accurate [Zimm05]. So at least the transponder package should have good heat conductivity.

Erythrocyte concentrate has a lower specific heat capacity (0.77 $\frac{kcal}{kg}K$) than water (1 $\frac{kcal}{kg}K$) or whole blood and thus reacts more quickly to changes in temperature [Zimm05]. Tests by MacoPharma [Zimm05] have shown that the measurement yields almost the same values inside the bag and on its surface if the transponder is insulated towards the ambience in the outside case. [Zimm05] suggests insulation over the whole bag as the best solution.

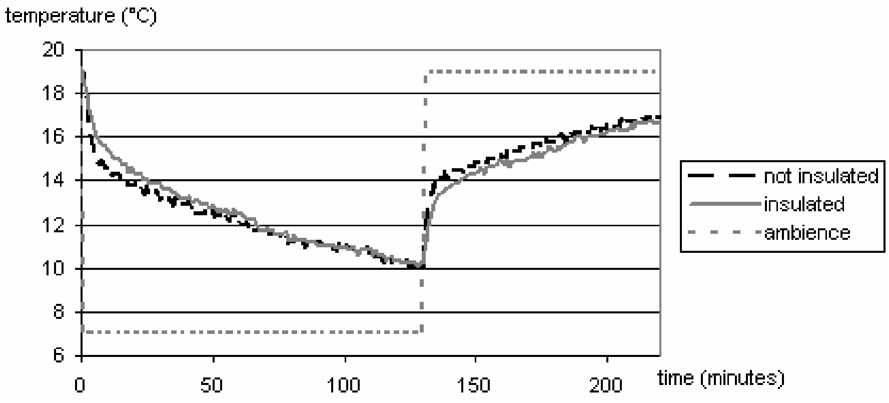


Fig. 18: Surface temperature of a bag
filled with water, measured by insulated (additional 2 mm PVC) and not insulated transponders, when moved between two ambient temperatures (own experiment, cf. [Zimm05])

The transponder memory is used for the blood bag specific information and the temperature data. Setting a minimum to the memory size depends on various aspects being part of the following discussion.

3.2.2 Temperature Logging

The transponder must be able to autonomously perform temperature measurements and stores them until they are read; this is called *temperature logging*. The way the transponder performs the logging should be configurable. The minimum logging features are worked out in this section and it is explained why they are required.

Fig. 19 depicts the general interactions necessary for a transponder to perform the logging. The configuration and the data produced during logging is subsumed under the term *log*. The log is configured and started; then the transponder obtains the measurement data until it is stopped. During logging or afterwards the logging data can be read.

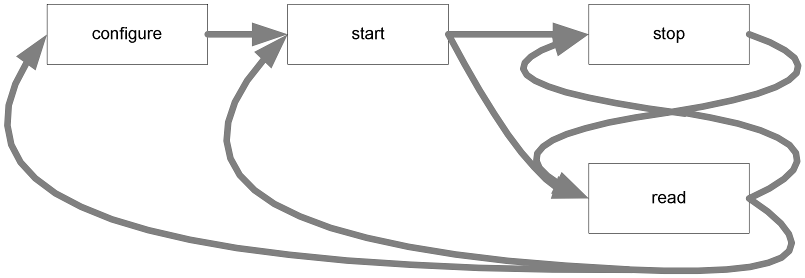


Fig. 19: Logging command cycle

The log is configured and started; the stored measurements can be read during logging and afterwards.

The sensor calibration must be performed by each transponder individually, which is at best performed directly by the manufacturer. For linear transfer function sensors a two-point calibration is sufficient (see 2.3.4). The calculations for the correction of the transfer function can be performed either on chip or by software, the latter implies that the coefficients of the calibration function must be read from the transponder.

The log configuration defines the way the logging is performed. The required parameters are discussed in the following: Monitoring requires periodic sampling. The rate at which the measurements are taken can be defined by the interval between two measurements (with an order of magnitude from seconds up to hours).

The transponder’s memory capacity is restricted. Hence it is essential that some pre-processing, e.g. the decision, when a measurement is stored respectively how or if at all, is performed by the transponder. Thus different logging modes can be defined. The simplest one is storing all values. Normally, one is only interested in exceptional values outside an acceptable temperature range defined by a lower and an upper limit. It would be possible just to store these "bad" values or alternatively the information could be compressed by memorizing only three points [KSW06], i.e. a point when the range is left, one at the extreme value (minimum or maximum) and one when the “acceptable” window is entered again. Fig. 20 illustrates these modes. The log configuration and the information stored about a measurement should allow to associate it with a point in time, i.e. eventually, it should be possible to transform them into a measurement record consisting of the tuple (time, value).

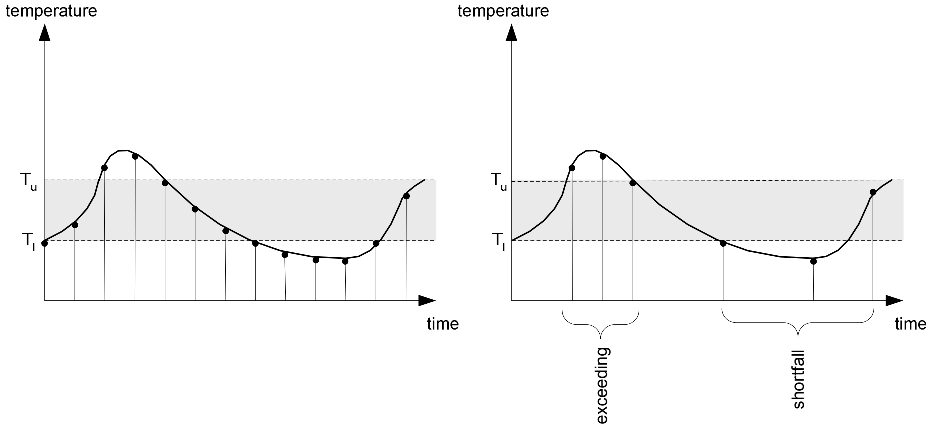


Fig. 20: Logging modes

Logging all values (left); storing only three points for each time the acceptable range (between the dashed lines) have been left.

The choice of the mode depends on the goal to be achieved. If the whole temperature life cycle should be recorded, all values have to be logged. Also digital calibration requires some function which allows unconditional reading of the sensor output. Clearly, this mode needs the most memory space. For monitoring purposes the temperature curve within the allowed range need not be stored. What has to be done with the values outside depends on the information needed by the application, e.g. the duration of the exceeding, the extreme value, or the time-temperature product. The mode which stores only three points for an exceeding allows for deriving this information to a large extent while using little memory space. In this mode the memory occupied is not dependent on the duration of an “exceeding” but only on their number. A problem arises when the temperature oscillates leaving the range and entering it again, each time causing the storage of the maximum/minimum information and thus filling up the memory. This can be tackled by a hysteresis mechanism (see Fig. 21), i.e. for example, an exceeding of the upper limit T_u is recognized when the temperature goes beyond $T_u + \Delta T$ and its end is recorded when the temperature falls below $T_u - \Delta T$.

Another desired function is interrupting a running log, reconfiguring it using other parameters and further continuing. This is needed if several possibly different logs should be run subsequently keeping the data of all logs in memory.

Furthermore it must be decided what to do when memory is full. When continuous monitoring is performed and it is not a problem that parts of the temperature history are lost it is possible to continue in a “ring” overwriting the oldest record. In other cases it might be desirable to simply stop the log when the memory is exhausted [KSW06].

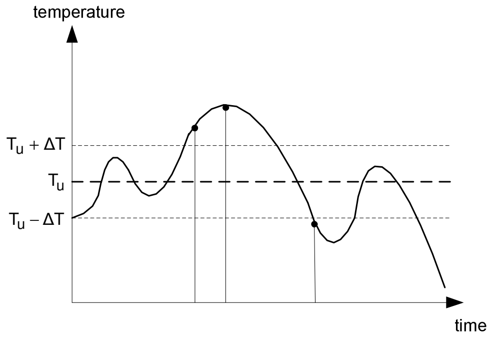


Fig. 21: Hysteresis for suppressing oscillations

T_u is considered to be exceeded when $T_u + \Delta T$ has been surpassed; the temperature is regarded to be within the acceptable range again as soon as it has fallen below $T_u - \Delta T$.

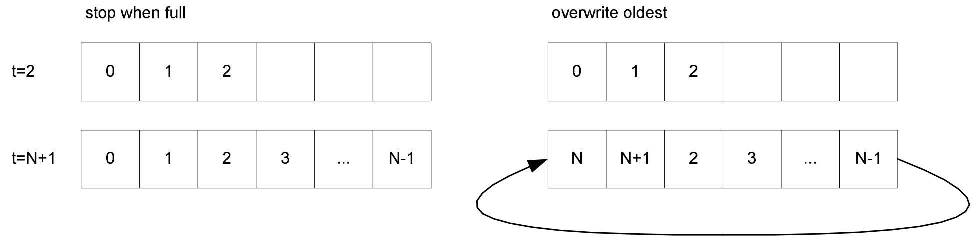


Fig. 22: Memory management

At most the first N measurements are stored (left); the oldest measurements are replaced after the end of the memory has been reached (right).

3.2.3 Basic Functions

Based on the logging functionality, this section defines the functions which must be entirely mapped on the functions of a suitable transponder:

- Identifying the transponder, i.e. reading its UID.
- Initialization prior to first use, i.e. setting transponder specific configuration, e.g. memory settings, and the digital calibration of the sensor.

- Starting the log: The configuration for this log is set and the log is started.
- Stopping the log.
- Reading the log: The whole log data is read, including the state of the log, when it has been started, if it is running, when it has been stopped and the internal timer time; the log configuration parameters and all data necessary for decoding the temperature data, e.g. digital calibration coefficients, and the temperature data itself.
- Writing custom data: This function allows for writing arbitrary information to the transponder, e.g. blood and blood bag data.
- Reading custom data.

Moreover security functionality is desirable in order to prevent from eavesdropping and manipulating data, illegitimate stopping or reconfiguring the log. The following functions are necessary:

- Initializing and configuring security: The information used for the security functions, e.g. keys, passwords, is set.
- Log-in: Authentication is performed and a session with authorization for a subset of functions is opened.
- Log-off: The current session is closed.

The problem of providing state-of-the-art security features on primitive transponders has already been addressed in 2.2.4, which does not imply that the implementation of functions only providing degraded security is useless. Some is still better than none, being aware that security is not fully guaranteed.

3.2.4 Timer

The transponder autonomously performs periodic measurements, therefore a time base on the transponder is needed in order to know when sampling has to be triggered. A power source must be integrated into the transponder which supplies the oscillator and measurement circuit.

A reasonable minimum logging interval is a second, therefore it makes sense that the timer counts seconds. The blood bag monitoring application requires the timer running for 50 days.

$$ld(50 \cdot 24 \cdot 60 \cdot 60) \approx 22.04bit \tag{5}$$

A 24 bit counter runs about 388 days before overflowing. For a 13.56 MHz oscillator a second 24 bit counter is necessary to trigger this timer.

The oscillator cannot be expected to run stably at a frequency, which results in clock jitter in the circuit. Retuning the oscillator can only be performed during interaction with the transponder, i.e. when the blood bag is put into the RW device's field during the blood supply chain. Furthermore it is not expected that a "second" as emitted by the counter has really the duration of a second. The latter property results into a gradually accumulating deviation between the timer's time and real time, called drift. The drift [Kope97] is defined by the relative deviation:

time instances t_0, t_1 with their respective timer times $t_{0,timer} = t_0$ and $t_{1,timer}$

$$d = \frac{t_{1,timer} - t_0}{t_1 - t_0} \tag{6}$$

The maximum acceptable drift is given by the requirement that the absolute deviation has to be smaller than half the log interval at the end of the log (when the log is stopped). For [KSW06] a drift of ±5% is guaranteed, which is far off acceptable considering that a drift of ±1% results in a deviation of 12 hours after 50 days.

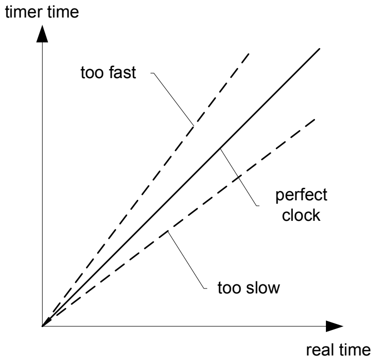


Fig. 23: Real time and drift
(cf. [Kope97])

This problem can be tackled by two methods (cf. [Kope97]): resynchronization and correction. Resynchronization (see Fig. 24) requires interaction with the transponder. A constant is added to the timer in order to make it approximately representing real time again. The calculations can be performed on the transponder or by the host computer system. The first method requires one command at the interface but additional computational resources on the transponder, the second one a command for reading the timer time and one for sending the correction constant.

The timestamps of past measurements remain unaffected and partly wrong after resynchronization. They can be corrected by drift correction (see Fig. 25), which is rather performed by the host computer system because of its computational expense. The current timer time must be read from the transponder and the timestamps are moved accordingly by stretching or compressing the time grid to the real time grid under the assumption of constant drift:

with constant drift d from t_0 to t_n

$$\forall i : 0..n : \; t_i = t_0 + d(t_{i,timer} - t_0) \qquad (7)$$

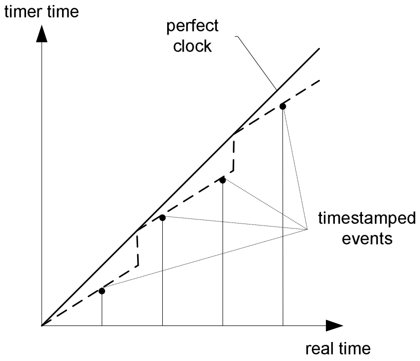


Fig. 24: Resynchronization by offset correction

The timer is synchronized with real time by adding a constant. The timestamps of previous events remain uncorrected.

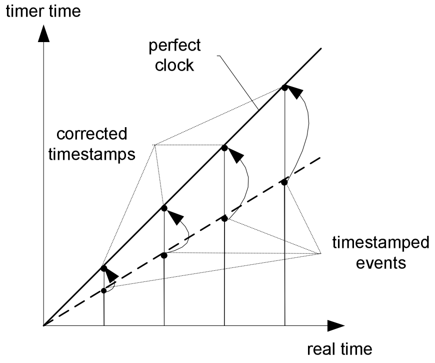


Fig. 25: Timestamp correction
Assuming constant drift, the timestamps can be corrected a posteriori.

3.2.5 Choice of Temperature Measurement Parameters

The temperatures an erythrocyte concentrate blood bag is exposed to range from 2°C to 120°C; during the cold chain between 2°C and 37°C. A measuring range of the sensor from -10°C to 50°C is sufficient. The best accuracy must be achieved between 0°C and 25°C. The desired measurement accuracy is ±0.5°C [Zimm05], normally ±1°C is guaranteed [Tech02]. 0.5°C accuracy means that the encoding of the temperature uses at least 120 values for the range -10°C to 50°C, i.e. at least 7 bits are needed when temperatures outside the range are mapped to the maximum respectively minimum value. But normally, the number of bits used depends on the ADC output which usually spans over the whole sensor output range [Frad04].

The overall accuracy depends on various factors: The intrinsic sensor accuracy, the resolution of the ADC, the accuracy of the calibration procedure and the storage format of the calibration function coefficients and the measurement values themselves:

digital calibration function C with limited precision of the memory representation (rounding function ρ_{memory}) of the coefficients d, k, real temperature T_{real} with sensor accuracy dT and limited ADC resolution by ρ_{ADC}

$$\begin{aligned} C(T) &= f(T, \rho_{memory}(d), \rho_{memory}(k)) \\ T &= C(\rho_{ADC}(T_{real} \pm dT)) \end{aligned} \tag{8}$$

The choice of the logging interval depends on the dynamic behaviour of the whole system consisting of bag contents, bag, sensor and ambience. According to the sampling theorem the interval must be at most half the time needed to reach an unacceptable value and return again into the acceptable range. In order to illustrate this, in Fig. 26 a constant change rate of 0.2°C per minute is assumed as a simplification according to the rule of thumb (see 2.1.3). The acceptable range of 2°C to 6°C actually means permitted permanent storage temperature. If an exceeding of more than 2°C should be reliably detected ten minutes would be a good choice. The optimal interval will have to be found out operationally by a test series with different choices. It is of no use to determine the limits too tight because of the fact that the bag's surface and the transponder are heated up first, thus generating a false alarm.

The memory necessary for storing the measurement data depends on the choice of the measurement mode. Due to the features explained in 3.2.2, the three-point extremum measurement mode is the most interesting for normal operations. If the transponder does not support the hysteresis feature, a filled up memory can be interpreted in a way that there definitely exists a temperature problem, because each extremum means an average duration outside the limits of one logging interval. If the memory size is chosen accordingly a full memory is enough for recommending the disposal of the bag. Using the same argumentation the memory management mode is of no importance since it is only relevant when the memory is full. Using a ring buffer has the advantage that the latest measurements are present which are normally of higher importance in tracing the temperature problem, since temperature problems in the far past should already have been recognized earlier. Thus the size of the measurement memory depends on how many minor temperature problems justify a disposal. The rest of the memory is reserved for custom data.

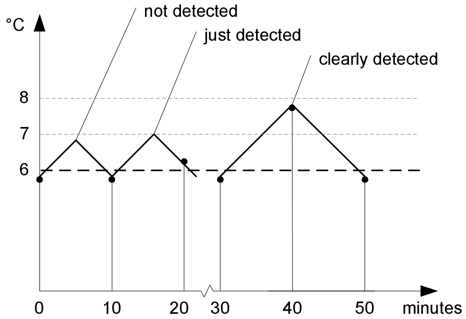


Fig. 26: Choice of the logging interval

The leftmost exceeding remains undetected; the middle one is just over the edge; the rightmost is clearly recognized.

3.2.6 Transponder Communication Time

Every interaction with the transponder consists of two messages: A request by the RW device and the corresponding response by the transponder. In ISO 15693 fast mode this communication is performed at 26.6kbit/s. For the whole communication cycle starting from the initiation of an interaction by the application running on the host computer until receiving the transponder's response by the application, the communication with the RW device, often a serial line, and also the computation overhead of the RW device must be considered. Table 1 shows some experimental figures on these overall communication cycles.

In any case, reading bigger parts of the memory or even the whole memory is impossible on conveyer belts. Normally, the bags are handled manually in the blood application, so it can be assumed that the transponder is not in motion during interaction. Nevertheless, it is important that only small chunks of data are written in order to increase the responsiveness of the application.

Generally, the time for performing the inventory of transponders in the field grows exponentially with the number of transponders [Lee05]. In order to keep the time needed for bulk detection acceptably low only the most important data should be read.

	4 bytes[1]	64 bytes[1]	whole transponder[2]
read	16 ms	141 ms	3922 ms
write	31 ms	312 ms	5235 ms

[1] one command, [2] approx. 1024 bytes, whole command sequence

number of transponders	0	1	2	3	4	5	6
inventory time (in ms)	188	281	281	281	297	375	375

Table 1: End-to-end transponder communication time for read, write and inventory

Naturally, the time needed for multi-tagging increases with the number of transponders in the field. Even if there is no transponder in the field, the anti-collision sequence has to be performed once. (Experimental results with Siemens Moby D10 over RS232 with baud rate 38400)

3.2.7 Battery

For autonomous logging the transponder has to be equipped with an independent energy source; communication is still powered by the field, i.e. the transponder is semi-active. The figures given in brackets in this section apply to a product [Infi04] which has been tested to satisfy all criteria [Ocke06]. This accumulator is based on lithium-cobalt-dioxide ($LiCo0_2$) technology.

The accumulator's size (approx. 1cm²), shape, thickness (<0.36mm) and flexibility must allow the integration into the transponder. For recycling and reuse the accumulator must be rechargeable. The recharging is performed by RF energy charging, i.e. inductively in the field. The number of recharge possible cycles (up to 100000) lies far beyond the transponder reuse count. The necessary battery capacity (up to 300µAh/cm², 85% efficiency) depends on the energy the transponder needs for logging (cf. [Cho05]), the time the logging is active (a maximum of 50 days for erythrocyte concentrates), and loss during storage. Blood bag systems may be stored in the warehouse about one year before being sold, that's why the overall lifetime of the battery being unused for a long time and afterwards in full operation should be at least 1.5 years with a small energy loss per year (1%). As already said, the temperature a bag is exposed ranges from 2°C to 120°C, the battery should survive these temperatures without degradation (-40°C to 150°C). Furthermore it is subject to extensive physical stress discussed in the next section.

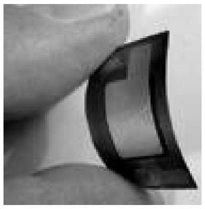


Fig. 27: Foil accumulator
(www.inifinitepowersolutions.com)

There are also ideas implementing sensor-enabled transponders without battery, which scavenge the energy from the electromagnetic fields surrounding us nowadays almost everywhere [Phil05a].

3.2.8 Physical Environment

The transponder has to be mounted on the erythrocyte concentrate bag before the blood bag system is packaged, and is detached after use of the blood product. Therefore the transponder is exposed to the physical stress the bag and bag contents have to undergo during their lifetime.

Before being packaged the whole blood bag system is vapor-sterilized at 120°C and 2bar for 30 minutes. A pasteurization at 85°C for 40 minutes follows [Wagn06a]. During production blood cells and plasma are segregated by centrifugation at 4247g and 22°C for 13.5 minutes [Wagn06a].

Irradiation is a further blood treatment necessary for patients with certain immunodeficiencies in order to reduce lymphocytes [Psch98]. It is performed using Caesium 137 with an energy dose equivalent of 30Gy for 9.8 minutes (1Gray = 1Sievert = 1J/kg energy absorption) [Wagn06a].

Tests (see Fig. 29) [Wagn06a] have been performed whether off-the-shelf passive transponders get along with such environmental conditions. 2.3% have been assessed to be defect at the end of the process.

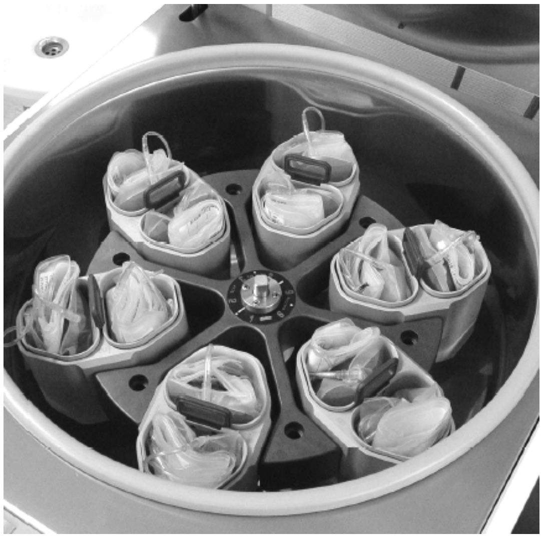


Fig. 28: Blood bag systems in the centrifuge
[Wagn06a]

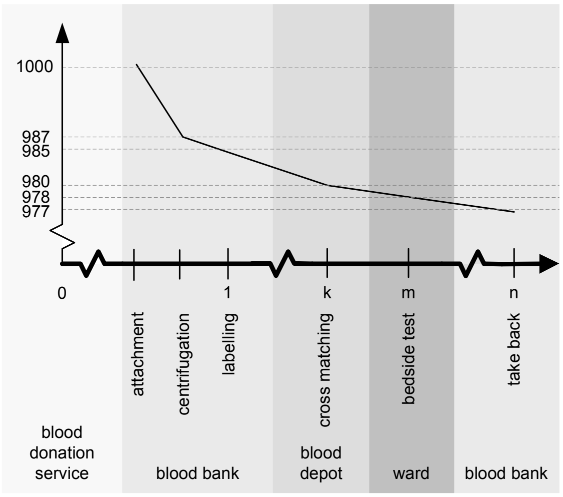


Fig. 29: Passive transponder tests

The biggest increase of defect transponders has been observed directly after centrifugation. The subsequent failures are attributed to irreversible damage by centrifugation which appears later (cf. [Wagn06a]).

The main challenge with semi-active transponders has been the battery so far, which might be solved now using the product [Infi04] which has been tested to be insensitive to 5000g [Ocke06]. Nevertheless the survival of the physical interconnections, the bonding between chip and printed circuits, the antenna and the battery, has to be evaluated and improved in order to increase reliability.

3.3 RW Device and Computational Hardware

The interactions with the RFID transponders must be seamlessly integrated into the current process. Depending on the environment and use case the RW device and computational hardware have to comply to different requirements.

Main criteria are multi-tagging capability and mobility. Bulk detection is necessary for receiving and shipping operations where it should be possible to concurrently interact with several bags. RW devices which provide the full range and are able to manage several antennas must be chosen for this task. During processing or in clinical areas the bags are handled one by one, thus the range can be smaller. However, an RW device's range has to be clearly defined in order to prevent errors because of inadvertently interacting with the wrong transponder lying nearby the antenna. In the laboratories stationary RW devices and standard computers are used. For many operations in the wards mobile RW devices and handheld computers must be employed because e.g. the bedside test has to be carried out at the patient's bed and not in the ward room and therefore operations must not be bound to some fixed workstations. The handhelds must be robust and preferably sealed and sanitizable.

The whole RW device, computational and software infrastructure must be flexible enough to support different RW devices and transponder types at the same time in order to allow possible changes and unhampered growth because of economic, functional, and system evolution and expansion reasons.

3.4 Further Requirements

The computerized systems deployed in the blood supply chain institutions make up an inhomogenous landscape of systems which have to be integrated in order to make an unobstructed flow through the institutions possible. Open and generic means for data exchange with these systems must be applied. The integrity of the information flow has to be guaranteed and access must be restricted to authorized personnel. The blood bags are in intensive interaction with medical and laboratory personnel who have the focus on their primary work, the interaction with the system is done along the way, therefore its use must be easy and natural.

3.4.1 Legacy Systems Integration

The software systems currently in use in the supply chain are dedicated to specialized administration tasks. It is no use and quite unrealistic to create a new system which supports all operations in the entire supply chain. It is rather desirable that the new system is like a line or bus through all institutions where existing and future systems can plug in and interact with its services.

Considering the example of the blood center Graz (see 2.1.3) [Wagn06b], there is a blood banking administration application, eProgesa of MAK-SYSTEM (www.mak-system.com), which performs all tasks ranging from donor and donation administration, laboratory and testing organization and blood bank warehousing. This software suite also includes patient and cross-matching administration support for blood depots. Currently [Wagn06b], there is no automatic blood processing protocol for each blood bag. For accounting an extra application is used. In Styria an electronic request system is installed for requests issued by blood depots. Hospitals which do not have their own blood depot must still send their request using paper forms, in this case the blood samples must anyway be sent physically. The fact that hospitals have their own hospital information systems which are not linked to the blood depot systems implies that hospital wards and blood depots have their separate patient administration applications [Wagn06b].

One principle of integrating these systems is the minimization of interfaces. Incrementally building up the system assures that interaction is minimized to the process points where it is unavoidable. E.g. it could be started with stand-alone applications which implement new functions which do not require communication with existing systems. Interaction is either immediate, or in form of batch updates, e.g. on a daily basis. Data import, export or bidirectional communication is required. The base system must be open to every existing and future system. It need not to change if the administrational systems alter or new systems are installed. An extension of its service should be possible without interfering with existing services. Therefore it should not be tailored and specialized to the existing systems. The use of RFID middleware systems (see 5.2) is encouraged to provide the necessary infrastructure for pushing and pulling the data.

3.4.2 Security

Due to privacy considerations personal data must not be stored on the transponder, but only IDs which can be resolved by authorized institutions. The necessity of encrypting transponder data and setting up a full-featured public key infrastructure is avoided that way. It is of higher importance that the data integrity is guaranteed, i.e. that it is assured that the data read is correct and reliable and has not been manipulated maliciously or non-deliberately. Data integrity consists of two stages: detection and correction.

Data integrity measures (see Fig. 30) span all layers: Checksums for transmission on all links in order to protect against errors introduced by the communication system; and checksums on the transponder data in order to detect transponder memory errors and unintended changes by other systems. In order to detect a malicious manipulation where the checksum is recalculated, it is necessary to store and compare the checksum using a secure information channel forwarding the checksum in parallel to the transponder’s path. This problem could be solved by digital signatures which again require a public key management over the entire process, but though, limited storage space on the transponder poses difficulties. Correction is of minor concern since a blood bag of which the data is proven to be tampered will be definitely discarded considering other physical manipulations which could have been applied. For network connections secure channels, e.g. SSL-based, are obligatory, this applies also for network-enabled RW devices.

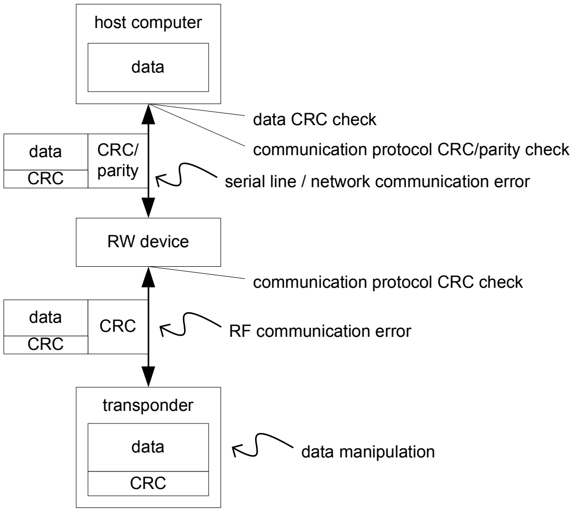


Fig. 30: Data integrity measures

Checksums are a common means for detecting communication errors and non-deliberate data manipulations.

Transponder security features, e.g. authentication and authorization before being allowed to execute certain commands, would provide the most effective protection against tampering. Otherwise data could be read and written by every other RFID system, even accidentally. The transponder should support different permissions (see Table 2) for different types of operations and access to certain memory areas. The simplest way is that the user has to supply an authorization token before being able to perform a command. Of course this method does not offer real security because the tokens are subject to eavesdropping since fully-fledged encryption is hard to be implemented on the transponder due to significant increase of costs and energy demands far beyond current economic viability [Sarm03]. Nevertheless the security credentials must be managed over the whole supply chain, i.e. the security configuration must remain constant or it must be consistently updated over the transponder life cycle.

	everyone	transponder manufacturer	blood bag manufacturer	recycling centre	blood donation service	blood bank	blood depot	hospital ward
identification	X	X	X	X	X	X	X	X
initialization		X	X	X				
calibration		X						
read		X	X	X	X	X	X	X
write		X	X	X	R	R	R	R
start log		X	X	X	X			
stop log		X	X	X		X	X	X

Table 2: Transponder permissions
(R: only for pages which the institution (role) is responsible for)

The data collected in the course of the supply chain has to be reliable, and furthermore appliances are used by many users spread over several institutions, thus unauthorized use must be prohibited. Transponder security goes hand in hand with application-level security. Only certain institutions should be allowed to perform certain operations or write specific data. Even within institutions certain decisive actions should only be allowed to be taken by responsible personnel. Whoever is authorized is accountable too.

Entering passwords or pins is cumbersome especially on handhelds, and they are subject to propagation; biometrics would be a better approach, but as an example fingerprints pose a problem because of often used protective clothing, e.g. gloves. A good solution are employee cards without pins, which make propagation more difficult because other permissions are also bound to them. Access cards are generally reasonable in hospitals for patients, staff and guests, to make hospitals more secure against criminal attacks. An RFID card for every patient would have many advantages in identification and in preventing confusion [Dalt05], but nevertheless still additional checks are necessary.

Another aspect is establishing process security: Every time data is written or a bag is received by the next institution in the supply chain, it is checked by the person in charge and his/her responsibility is recorded by a timestamp and a signature.

Since every security mechanism relies on a secret piece of information, these measures only protect against external intruders. If keys and passwords are propagated due to convenience in daily work even the theoretically best security system could be compromised. Thus overall security includes physical security measures and training to handle the security credentials in a responsible way.

3.4.3 Usability

The system is used by medical and laboratory personnel and has to be designed for easy handling. The terms in the user interfaces must be unambiguous and self-explanatory, the logical course of the dialogs clear, the operations intuitive. It should not prohibit actions, but guide the user and interrupt the routine and warn him/her when sudden non-standard situations emerge. This is particularly important in laboratories and wards where the system is often used in stress situations and important deviations from the routine behaviour are to be taken into consideration.

Special attention has to be paid to the handling of the bags concerning alignment of transponders and RW devices which could easily lead to frustration when not performed correctly. After installation of the system it is important to document best practices in handling the system, e.g. because of manual interaction, the user cannot be prevented to remove a bag during a read or write operation. An interaction with the transponder cannot be done transparently but must be made visible to user.

Designing high usability interfaces is especially difficult with handheld devices which come into use in this kind of application. Handhelds are already successfully used [Sche04] in various clinical practice for administrational purposes, e.g. for looking up drug information and scheduling patient visits. Their greatest advantage is the direct availability at the patient's site and as a reminder instrument for important actions. A problem is still the small size of the screen and the cumbersome data entry. Therefore one should not try to pack a load of information on the tiny screen using small fonts, and data entry by the touch-screen keyboard should be generally avoided. Entries should be rather chosen from lists and numbers entered using up-down numeric fields. The manual entry of critical data should be avoided at all.

A significant factor of usability is performance. Waiting seconds for a response or watching progress bars advancing slowly in routine operations immediately provokes the opinion that the system is of no use. Designing good user interfaces is a very important dimension for the success of a system, since it eventually helps to make the overall process less error-prone.

3.4.4 Fault Tolerance and Failure Recovery

A basic principle of achieving reliability is application modularity [Kope97], i.e. the components (fault containment units) of the system must fail independently without affecting the rest of the system, thus enabling redundancy as a fault tolerance measure:

- When a transponder fails to be accessed, the data solely stored in its memory is lost, and it will have to be disposed like the bag it is attached to (because at least its recent temperature history cannot be retraced). The reasons of the failure can be probably a posteriori inferred by diagnosing the symptoms manifested in the application logs.

- When an RW device fails the problem could be either a hardware failure or a configuration problem, which can be easily identified by diagnosing the logs. Normally, such failures can be quickly settled by the local technical staff by redundancy, i.e. by having spare RW devices and redundant workstations.

- A failure of the RFID software is more severe because its reason is mostly a design fault, i.e. a bug. This is especially bad for tasks which require direct interaction with the transponders. A service outage can only be impeded by redundancy. Usually, several workstations are available for the same task.

- An administration system failure is a big problem for the process. Direct interaction tasks should not be affected by design, e.g. by implementing emergency features with degraded service. Data to be exported to those systems must be cached until they are available again.

A general rule is that blood must not be wasted because of a system failure. The analysis shows that this is especially difficult for transponder failures. The second critical system is the RFID base software, which is mainly threatened when updates are performed or configurations are changed. It must be accentuated that in a hospital the business process continues in spite of system failures. The most important fault tolerance measure is infrastructure redundancy. Computation hardware failures are masked that way which is facilitated by splitting up the application into independent modules for different tasks which can be run on each workstation.

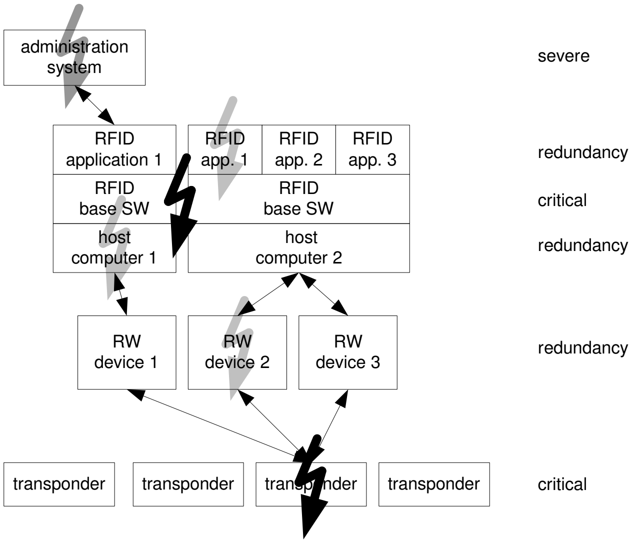


Fig. 31: Failure levels, severity and fault-tolerance measures

A transponder failure is critical because the blood has to be disposed practically. A problem with the RFID base SW is caused by a design or configuration fault which can show its effects in other parts of the system too. Administration system failures affect direct interaction applications which are dependent on data from these systems. The other failures can be tackled by redundancy.

Logging all interactions is an absolute must for maintenance reasons as it is the only means for enabling a posteriori diagnosis. An important design measure is the minimal dependency on links to the administration systems especially for direct interaction tasks. In case of an administration system failure, the data which has to be imported from this systems has to be provided by different means.

Data discrepancies can arise between the transponder data and the information printed on the bag label. This is clearly a human error by the personnel having performed the release of the blood product or a deliberate manipulation, the bag has to be disposed.

Recovery after failure actually consists of maintenance actions, i.e. replacing the failed components in order to maintain the redundancy level, and establishing consistency with the administration systems.

3.4.5 System Deployment and Evolution

An RFID system has to be finely adapted to the customer's needs in a multi-stage deployment process [Flei05]:

First of all a technical proof-of-concept must be performed, which evaluates the core technical implementation of the basic functional requirements and the properties of transponders and RW devices in the respective environment.

In the second stage it has to be shown that the overall function of the system can be fulfilled by installing a pilot which implements a vertical cut through the intended system. During these pilot phases intensive reporting and error tracing must be performed facilitating stepwise improvements of the system. Then the system can be introduced step by step into the whole process. Often old systems cannot be removed at once but have to run in parallel until the entire system is deployed.

During the operation phase the system often has a tendency to grow: More features have to be included, more institutions have to be spanned, and even legacy systems change. System changes have to be applied in the same manner by evaluating first their impact on the process and the running system before full deployment. This requires a scalable architecture which is designed for making changes and extensions manageable. Therefore an RFID based blood temperature monitoring system cannot be expected to use a single transponder type or a single data configuration throughout its lifetime. Even essential hardware and data structure changes must be handled in a plug-in manner and multiple versions have to be supported simultaneously.

Chapter 4

System Design

This chapter discusses the key features of a possible realization. It is argued why certain design and architecture options are preferred. Thereafter we describe how RFID-based temperature monitoring fits into the blood supply chain by examining the use cases which accompany it. The last part presents an RFID temperature monitoring framework, which has been implemented in the course of this thesis in order to demonstrate technical feasibility.

4.1 General Concepts

RFID system architecture is concerned with the structure and relations of tasks and responsibilities between transponders and the computer systems, i.e. which functions and tasks are fulfilled by the transponder and how the computer systems manage the data flow vertically and horizontally. Transponder life cycle management is a topic which comes into play with multiple re-use of transponders. Furthermore it is discussed which data is acquired where and how (during the supply chain).

4.1.1 RFID System Architecture

There are three types of RFID architecture concepts: One extreme uses the transponder for identification only, the other extreme regards the transponder as portable data store and a hybrid approach which replicates the transponder data in the infrastructure. Fig. 32 through Fig. 34 illustrate the three concepts.

EPCglobal item identification and tracking (see 5.2) is based on the first concept [EPC05]. The transponders are initialized once with an ID and remain unaware of what happens to them during the processes, i.e. the transponders do not carry any state. The only information they offer is their ID, and the only information the RFID system is interested are the events generated by moving transponders. This approach is somewhat "minimalist" [Sarm03], but it perfectly addresses the need of large scale and high speed automatic identification. There is no time for reading big amounts of data from a transponder when items are running on a conveyor belt, or a large number of cartons on a palette or items in a carton must be identified within a second. RFID blood bag monitoring does not require large scale identification, therefore this approach misses the real requirements of this application.

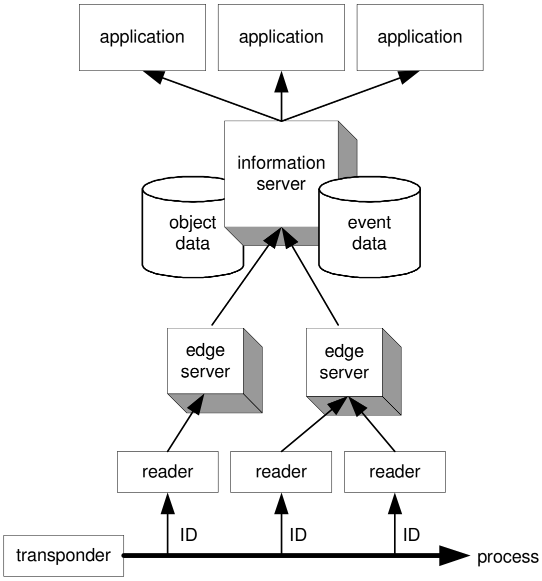


Fig. 32: RFID system architecture for large scale identification applications
As the transponder passes through the process it creates events, which are collected and preprocessed by edge servers, and stored and made accessible to applications by an information server (cf. [EPC05], [Prab05]).

A hybrid system makes use of a database which replicates and backs the transponder data and possibly extends it by further information [Floe05]. The decisive advantage that the transponder data is not totally lost when a transponder turns unreadable is paid by the need of employing consistency measures which guarantee that the information in the database as well as the transponder data are up to date in order that they can be used separately. Furthermore discrepancy resolution has to be applied when both transponder data and database information has been changed concurrently and independently. The backing database can be installed centrally, or the information can be stored locally at each institution and forwarded when the transponder is transported too. The receiving institution has to synchronize physical object arrival and the data import accordingly.

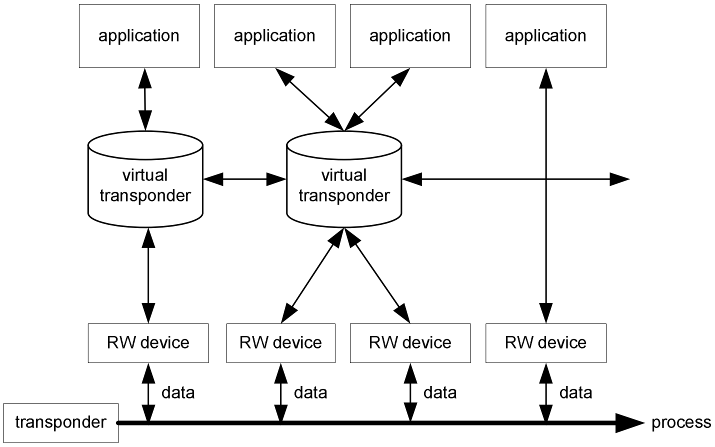


Fig. 33: Hybrid RFID system architecture
The transponder data is replicated in a database as virtual transponder. Applications operate only on the transponder, on its virtual image or on both (cf. [Floe05]).

The third concept is storing the data on the transponder only, i.e. RFID transponders are used as a portable data store; an RFID system interacting with a large number of transponders thus represents a distributed database. In such a system the transponders form an implicit physical data transmission channel which carries the data always exactly to that location where it makes sense, namely directly to the object to which it is linked. It is clear that this is only useful if the data stored on the transponder is insomuch intimately linked to the object that it does not have much value if separated from the object itself and therefore the data loses its value when the object is lost. It would not make much sense cramming central databases with that type of data.

The latter concept is also encouraged by another aspect related to sensor equipped transponders: A sensor performs autonomous data generation recording and makes dynamic properties of its current and past environment readable and accessible. The necessity of storing that data at least temporarily in the transponder memory is self-evident.

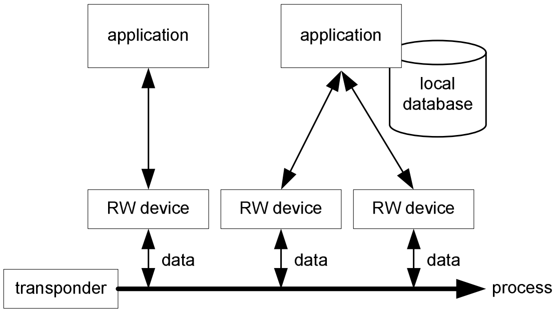


Fig. 34: "Pure RFID" system architecture

This concept goes far beyond the original idea of RFID, namely contactless no-line-of-sight identification. The real value of RFID technology in applications making use of these ideas arises from using transponders as portable memory, computation and sensing devices. This is qualitatively different from normal simple tracking and tracing applications.

Which of the latter two concepts is best suited depends also on transponder life cycle implications, the data stored on the transponder and the following conceptual consideration: On the one hand there are use cases where operations are performed directly in the presence of the physical object. In such cases the portable database property of the transponder can be exploited: Object information is available everywhere, every time. On the other hand there are operations which are performed without having the object. These operations have to be performed on a logical or virtual object representing the real object in the computer system (cf. [Roem04]), which must contain all the information necessary in synchrony with the data on the transponder (see Fig. 35). This case strongly favours the hybrid approach.

An advantage of the transponder-only approach is the minimalization of infrastructure as opposed to providing wireless access to object related data via WLAN. Transponders with large memories are more costly which is negligible regarding the costs for sensor and battery. More severe problems are definitely higher access times and the loss of data when the transponder is defect. Considering the blood monitoring application the transponder can be used as link between inhomogeneous systems, and it increases the interchangeability where no common infrastructure is available. The hybrid approach would require further redundant information channels where the bag is transported physically.

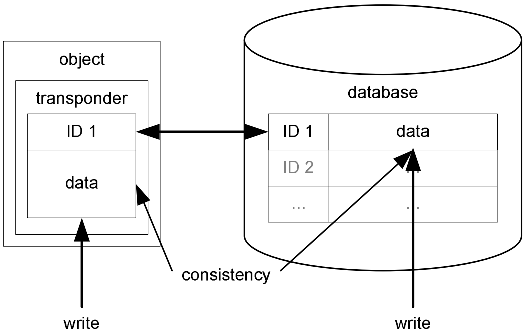


Fig. 35: Physical and virtual object
Consistency has to be maintained between the data on the transponder and in the databases, especially when applications operate on both representations independently (cf. [Roem04]).

Fig. 36 depicts a possible architecture which especially aims at the integration of existing administration systems. The RFID base system separates RFID concerns from the application logic. It feeds data into a general purpose, e.g. publish-subscribe-based middleware communication system (cf. [Arre03]). Administration applications pull and push data to this system. Data for direct interaction tasks is channelled through this system.

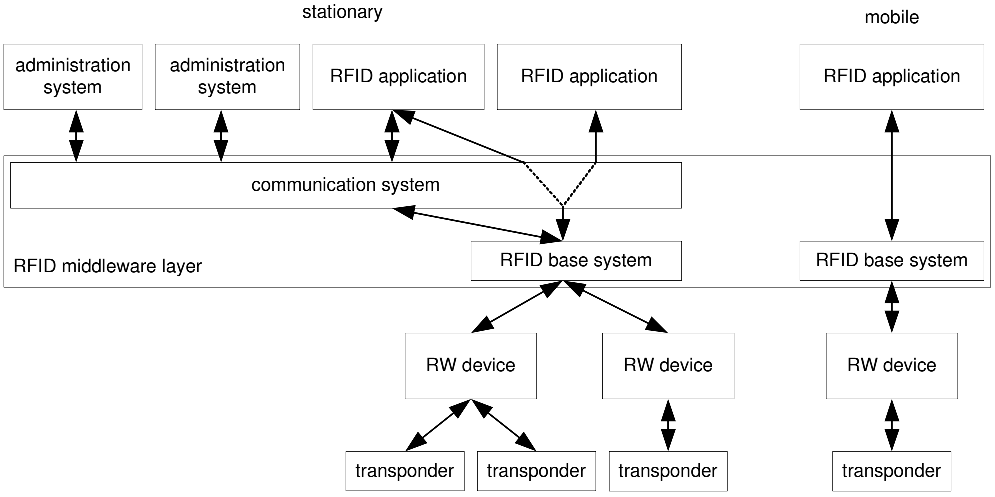


Fig. 36: Generic open modular architecture for RFID integration
(see text)

4.1.2 Transponder Circulation and Recycling

Due to economic reasons the transponders are used several times, i.e. the transponders are collected at the end of the supply chain and prepared for the next cycle. A side effect of recycling is that the supply chain becomes a closed loop which eases reporting and statistics. *A problem is that the principle that a transponder is uniquely linked to an object is violated and thus the use of the UID for identification is restricted.* Of course a transponder is not attached to two blood bags at the same time, but problems arise in administration databases when the UID is used as a key; the bag ID must be used for this purpose. The transponders are collected in the hospital's blood depots which are also the central place for reporting on blood and transfusion issues. A solution for transponder detachment is described in 3.2.1. All transponders, also defect, and supposedly defect transponders must be collected.

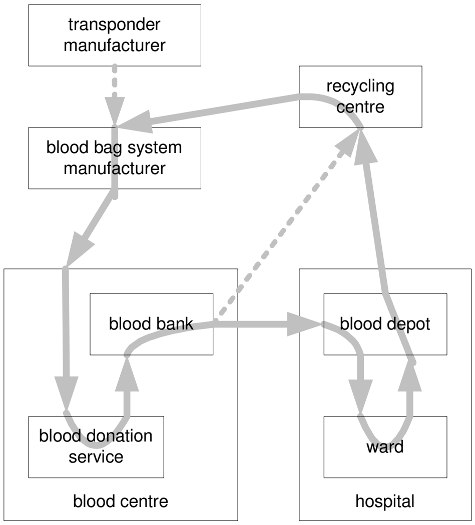


Fig. 37: Transponder cycle
The blood bag manufacturer is provided with new transponders by the transponder manufacturer and reused ones by the recycling centre. The transponders of transfused and discarded blood bags are returned to the recycling centre.

A recycling centre has to be established which is responsible for the transponder life cycle management. A maximum number of cycles which can be guaranteed has to be fixed. A good evaluation must be carried out by experiments first to determine the maximal number.

The recycling centre performs the following tasks (cf. also Fig. 38 and Fig. 39):

- It registers the transponders and counts how often they circulate.
- It checks the transponder's functionality and its further usability and rejects defect entities.
- It decontaminates the transponders and recharges the battery.
- It forwards the transponders to the bag manufacturer.
- It is the central place for reporting technical issues: It obtains information from the blood depots on encountered transponder problems and defects; furthermore it aggregates this information and forwards it to the bag or transponder manufacturer.

The recycling centre is ideally installed at the site of the bag or transponder manufacturer. A very transparent organization of the reporting channels is essential to eliminate the existing problems and to constantly improve the equipment's quality due to the fact that a blood bag must be discarded if its transponder gets defect.

In case of problems the temperature history is analyzed in these blood depots. For the detection of the correlation between the bags history throughout the chain and the temperature chart, important events in the bag's lifetime, as well as begin and end of transport are marked by timestamps.

4.1.3 Data and Data Flow

In the course of the supply chain data which belongs to different categories is generated, collected, and made available to the different applications, i.e:

- *The transponder identifier (UID)* which is permanently assigned at its production.
- *The blood bag identifier* which is assigned prior to donation and is used for identifying the blood bag throughout the supply chain.
- *Blood information data* which subsumes all the medical properties of the bag contents.

- *Temperature measurement data* which represents the temperature history of the bag contents. The data is autonomously generated by the transponder.

- *Operational data* which comprises the data (temporary or accumulated) and which supports the process itself, i.e. it carries information related to the process' state and progress.

- *Tracking data*: data acquired when the bag passes an identification point and consists of the bag identifier, a timestamp, the location and possibly the bag state. It is no use storing tracking data on the transponder.

- *Tracing data*: the totality of data collected during the supply chain for tracing a bag's way back and for finding possible causes of events. It can be used at any position in the supply chain to explore the life story of a given bag.

Table 3 illustrates the different data categories and their properties.

	acquired		stored	
	external	internal	external	internal
UID	fixed			X
blood bag identifier	X			X
blood information	X		O	O
temperature measurements		sensor	O	X
operational data	X		O	O
tracking data	X		X	
tracing data	X		O	O

Table 3: Data categories

The origin of the data and where it is reasonably stored (X mandatory, O optional or alternative).

Due to tightly restricted memory capacity on the transponder the data structure and encoding has to meet certain requirements. We can either assume variable length data and store both the length of an item and its value, or use special symbols as delimiters to separate the values; but in any case a maximum length has to be fixed which must not be exceeded. Therefore the simplest and best way is to use only constant length data items. The grouping of the data into pages is not only advantageous from a modelling perspective (since grouping naturally exists), but also because reading contiguous blocks is faster.

Responsibility	Attribute
blood bag manufacturer	manufacturer ID bag system serial number
blood donation service	donation service ID donation ID donation timestamp & signature
blood bank	blood bank ID blood product type blood group (AB0, Rh(D)) expiry date release timestamp & signature shipping timestamp & signature take back timestamp & signature hospital & blood depot ID
blood depot	receiving timestamp & signature return state return timestamp & signature hospital & ward ID patient ID cross-matching state cross-matching timestamp & signature shipping timestamp & signature take back timestamp & signature
ward	receiving timestamp & signature return state return timestamp & signature bedside test state bedside test timestamp & signature
blood bank, blood depot, ward	final state finalization timestamp & signature

Table 4: Blood information

So, each institution is responsible for the pages for which it is authorized to change the data. Bag related data is physically propagated with the help of the transponder; and the most important information is also printed on the bag's label; furthermore information about the shipped bags is listed in the according transport documents. There is no transfer of personal data, except by IDs which are resolvable by the producing institution. Table 4 lists the proposed set of data stored on the transponder. There are different norms for blood bag data (see 5.3.4). The data chosen here is based on [ICCB04], [EC05a], [EC05b], and operational requirements.

The majority of attributes is written once. In case of cycles in the process the corresponding attributes must be reset. Online data transmission is necessary for administrational purposes, e.g. blood bag orders, i.e. the tasks where the bag is treated virtually.

The collected data on the transponder are used for the following purposes:

- Immediate checking: This is the main advantage of data tagged and of environmentally aware objects. A bag is checked at each interaction point in the process if its state constitutes the precondition of the intended operation. For bulk handling it is necessary to provide an outlining view which shows whether problems are encountered and it allows the inspection of details only in this case.

- Automatic documentation: Medical/laboratory documentation and protocols can be automatically created from a subset of the data. This is an important added value since copying errors can be prevented.

- Reporting: Medical, administrational, technical, and operational statistics/reports can be automatically generated by aggregating the data. The creation of resource consumption, haemovigilance and productivity reports for the management and superordinate institutions is facilitated.

- Tracing: Operational and tracking data allows to a posteriori investigate the life history of a bag in order to detect problems in the supply chain processes. The superposition of the temperature curve and the operational timestamps eases the analyses.

Security and reliability issues are already discussed in enough detail in 3.4.2 and 3.4.4.

4.2 Process Embedding

Process embedding means defining how the system has to fit into the existing processes in order to support the workflow. The first section describes the points of interaction and the operation patterns. The subsequent sections describe the workflow system for the different institutions involved.

4.2.1 System Overview

A point of interaction is a location in the supply chain where information is read from or written on the transponder, or where an operation on the virtual bag is performed. These points define the use cases of the application (see Table 5).

institution	interaction	stationary	mobile	single detection	bulk detection
blood bag manufacturer	testing & initialization	X			X
blood donation service	donor permission	X		X	
	donation finished		X	X	
blood bank	receiving & weighing	X			X
	centrifugation & separation	X		X	
	filtering	X		X	
	labelling & release, finalization	X		X	
	shipping, take-back, finalization	X			X
blood depot	receiving, returning	X			X
	cross matching	X		X	
	shipping, take-back	X		X	
	finalization & reporting	X		X	
ward	receiving, returning	X	X	X	
	bedside test		X	X	
	Finalization		X	X	
recycling centre	reporting & reinitialization	X			X

Table 5: Points of interaction

The bags are always handled manually, i.e. there is no automatic manipulation. The identification is either single or in bulk in cooling boxes. The user interface and the RW device are always in proximity since bag handling, monitoring and triggering actions are usually performed by one person. The possible environments range from mobile donation facilities over laboratories to wards.

The finalization operation is the last write operation on the transponder. The final state indicates what happened to the bag at the end, e.g. is it successfully transfused, or is it discarded due to certain reasons. The reporting system uses the data of the finalized transponders and aggregates it for generating medical and technical reports.

4.2.2 Blood Bag Manufacturer and Recycling Centre

The transponder is mounted as part of the erythrocyte concentrate bag manufacturing process. It is mounted irreversibly detachable under the primary label. The transponder is delivered as already calibrated and tested by the transponder manufacturer or recalibrated and tested by the recycling centre. After the sterilization and the packaging of the bag system, the transponder is once again tested and also initialized. The bag manufacturer and bag information is written to the transponder. The bags are added to the warehouse system. The transponder can be used for identification in warehouse processes, i.e. inventory and commissioning (cf. Fig. 38 and Fig. 39).

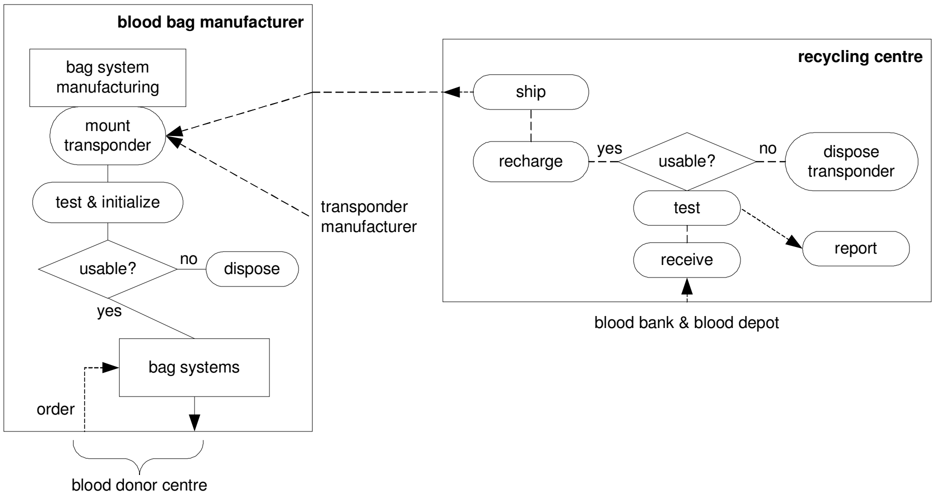


Fig. 38: Blood bag system manufacturer and recycling centre workflow
(see text)

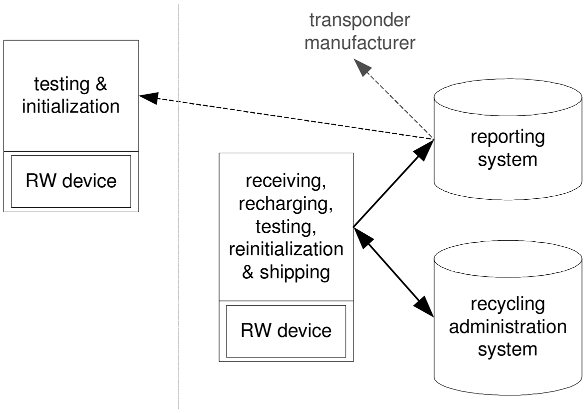

transponder manufacturer
testing & initialization
RW device
receiving, recharging, testing, reinitialization & shipping
RW device
reporting system
recycling administration system

Fig. 39: Blood bag system manufacturer and recycling centre systems (left resp. right); A double-framed RW device has multi-tagging capabilities; see text.

4.2.3 Blood Donation Service

The blood donation service (cf. Fig. 40 and Fig. 41) obtains the blood bag systems from the blood centre. Blood is mostly collected by mobile facilities touring around in companies and public institutions. These facilities are equipped with a computer system for registering donors and donations. The identity of the donor is determined and its suitability is assessed by a questionnaire. If he/she is accepted the donor is registered and the link between donor and donation is established by adding a new donation number for him/her. The donation service identification and the donation number are written to the transponder. The bag system is unwrapped, the bags and probes are labelled in advance; furthermore the bag system is checked for defects and returned to the blood centre if necessary . After the successful completion of a donation the integrity of the donation is checked by the responsible doctor, it is time-stamped and the log is started. Afterwards the bag system is cooled down to room temperature and returned to the blood centre.

4.2.4 Blood Bank

The donor and donation records are imported. When the boxes containing the bag systems arrive, the bags are put on the balance for weighing, the donation data is read from the transponder, data and temperature integrity are checked. During processing the bags are tracked by their UIDs and a process protocol is generated. The number of bags which can be processed in parallel depends on the equipment. After processing, the plasma and erythrocyte concentrate bags are clipped off, the plasma is frozen and the erythrocyte concentrate bags are stored temporarily until the blood analysis results are readily provided by the laboratory systems. The blood data is electronically imported from the laboratory, it is written to the transponder and the labels are printed and sticked on. The data consistency and the temperature integrity are checked before the release is confirmed by a responsible and the log is reconfigured for 4°C and started. Contaminated products are properly disposed. The released bags are stored in a warehouse.

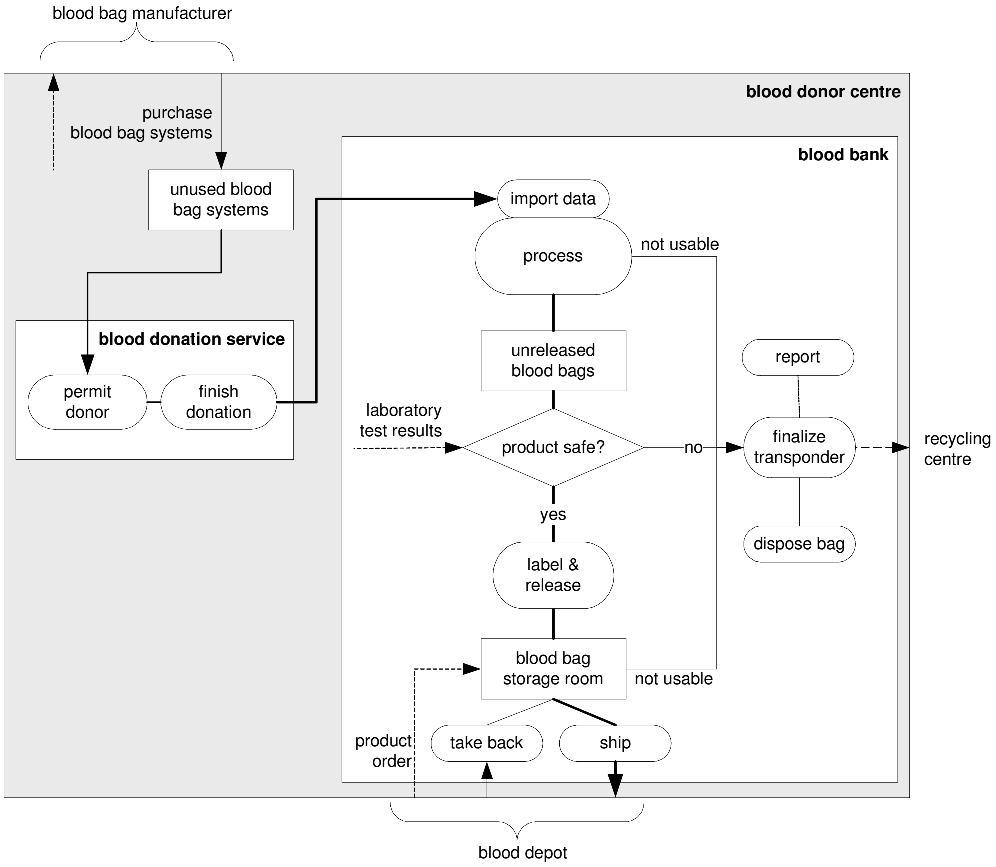


Fig. 40: Blood donor centre workflow
(see text 4.2.3, 4.2.4)

When a request by a blood depot arrives appropriate bags are automatically suggested by the warehouse system, they are taken out of the cooling room, their identity is checked and their integrity confirmed, they are put into cooling boxes, and transport documents are generated. Taking back blood products from blood depots is made possible by temperature monitoring. On receiving it is checked if they can be accepted by controlling their temperature integrity. For all disposed bags the reasons for their elimination, e.g. contamination, bag or transponder defects, are recorded in the reporting system. The transponders are detached and collected and sent to the recycling centre weekly or monthly including a report on technical defects (cf. Fig. 40 and Fig. 41).

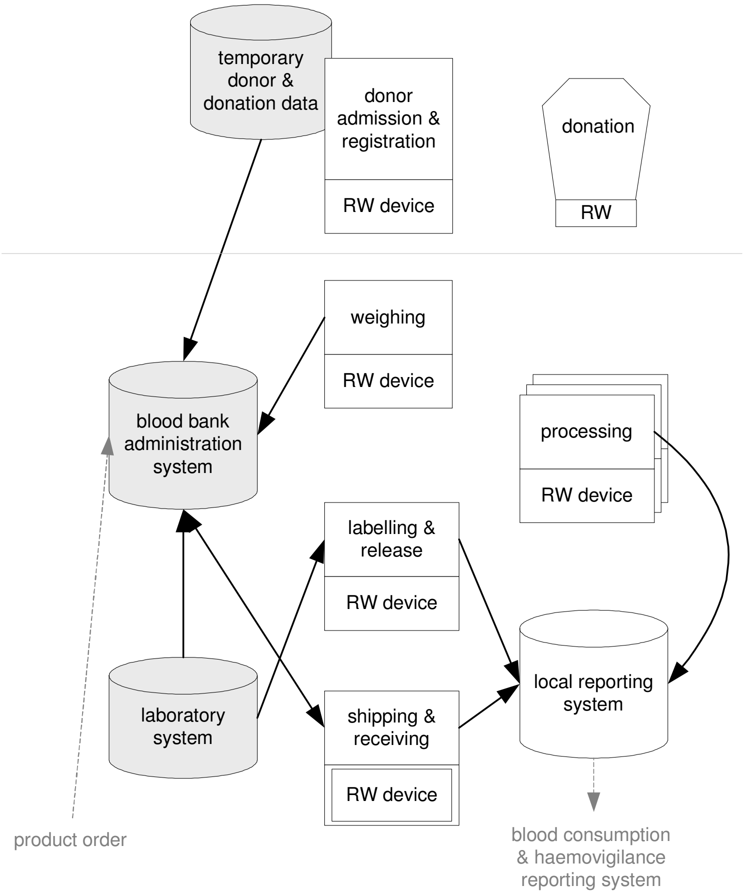


Fig. 41: Blood donation service and blood bank systems

4.2.5 Blood Depot

In our case the warehousing processes in the blood depot are already computer aided. On receiving the transport documents and the shipment are checked against the order by bulk detection. The integrity of the cold chain is confirmed and the necessary data is imported to the local administration systems. Improperly transported and wrongly delivered bags are rejected and returned to the blood bank. After reception of an electronic blood product request from a ward (or a paper-based order from another hospital), the most appropriate bags are reserved for the particular patient for cross-matching in the depot system. As soon as the probes have been received, the bags are taken out, and the patient ID is written to the transponder. In case of emergency, the bags are immediately issued. After cross matching the results are written and confirmed by responsible staff. If an incompatibility is detected the patient ID is reset, the bag is restored, and another bag chosen. This can be repeated as long as available blood probes exist for cross-matching. If the bag has already been issued in advance the ward is notified about the results.

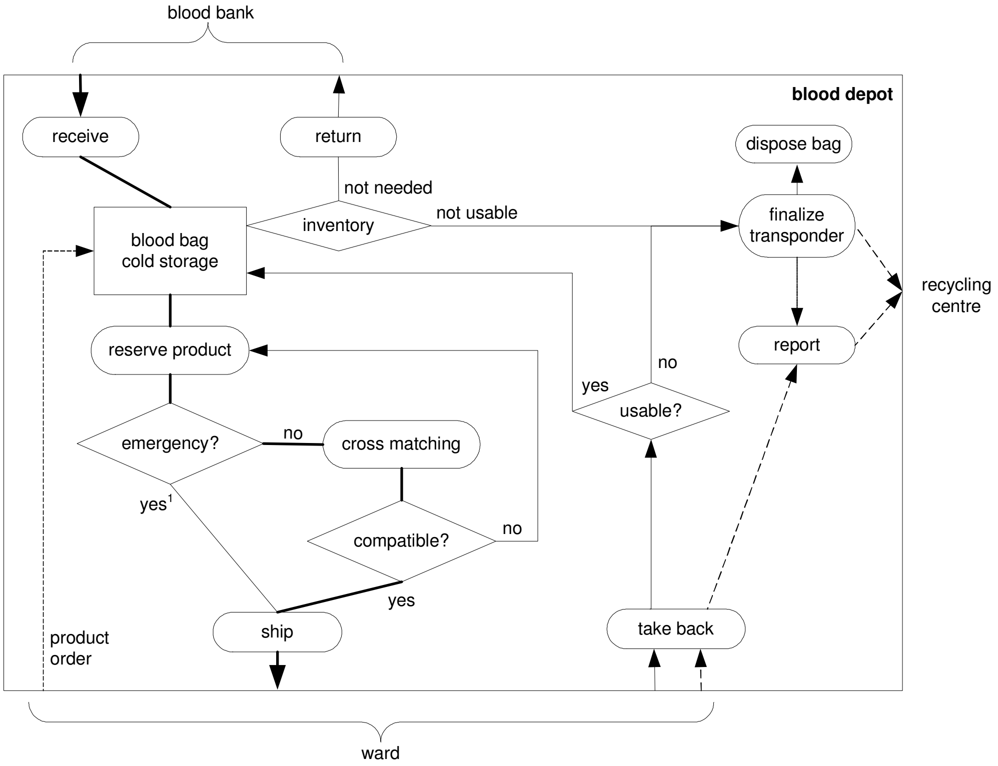


Fig. 42: Blood depot workflow

(see text); [1] Though in case of emergency the bag is immediately shipped, cross-matching is done anyway.

In case that expired or not usable products are found in the depot system, the transponders are finalized and the bags are disposed. Temperature monitoring makes it possible that bags are returned from the wards. It is checked if they are still usable and stored or disposed accordingly. Bags having caused transfusion reactions are analyzed. In case of a successful transfusion only the transponder is returned by the ward. The transponder is read and the data is fed into the reporting system (cf. Fig. 42 and Fig. 43).

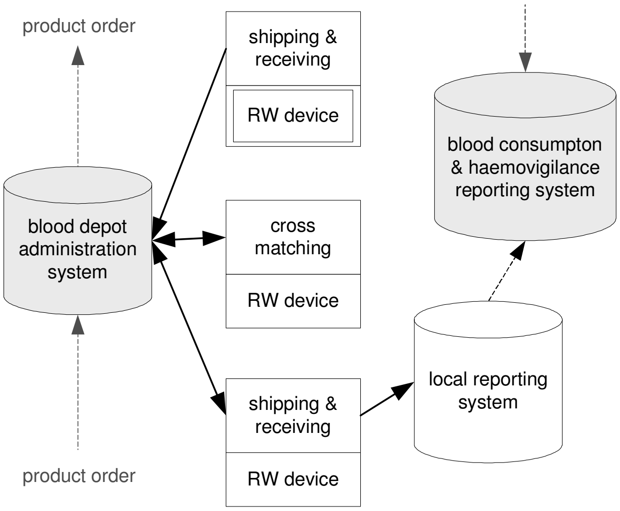


Fig. 43: Blood depot systems

4.2.6 Ward

When a blood bag is needed for a patient, blood probes are taken and sent together with a request to the blood depot. When the bag is received it is checked and its integrity is confirmed. It can be temporarily stored in the transport cooling box. If a bag is not needed or not usable it will be returned to the blood depot.

Before transfusion a bedside test has to be performed: Directly at the patient's bed the doctor responsible for the transfusion checks the bag and decides whether it is still usable. Since mixing up patients and bags often ends up lethally, it must be assured that the right patient gets the right bag. The result of the bedside test is written to the transponder and confirmed; furthermore it is documented in the patient history. Then the transfusion starts. The success of the transfusion is indicated by the final status, e.g. successfully completed, aborted due to transfusion reactions, which is written to the transponder. A transfusion report is created, which is also part of the patient's medical history. In case of reactions or problems all probes are returned to the blood depot (cf. Fig. 44 and Fig. 45).

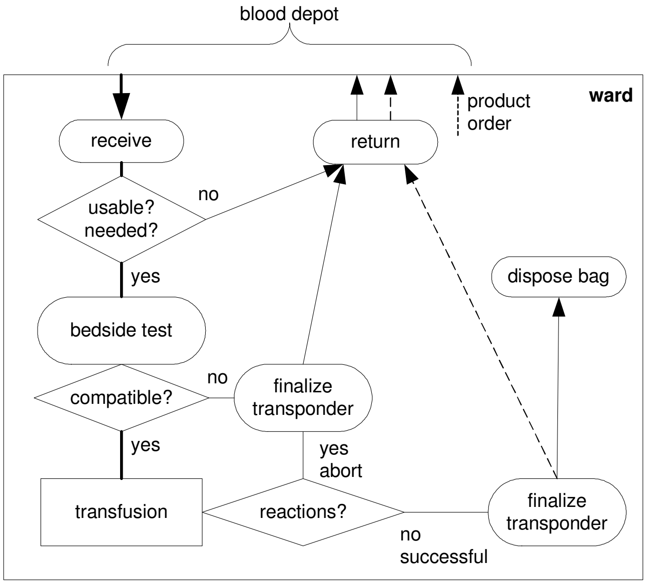


Fig. 44: Ward workflow
(see text)

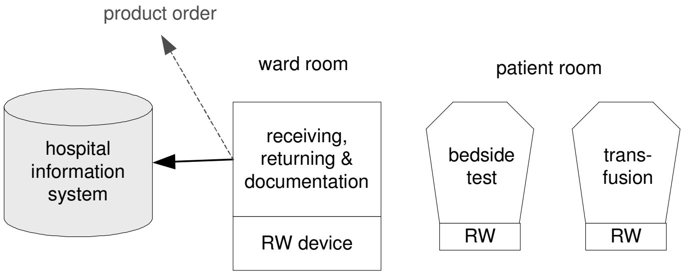


Fig. 45: Ward systems

4.3 RFID Temperature Monitoring Framework

An RFID temperature monitoring framework has been implemented in order to demonstrate the technical feasibility. Essentially, it implements the edgeware layer of the RFID middleware stack (see Fig. 66), and primarily targeted at reusability and quick pilot application development. It realizes the majority of the mechanisms and concepts presented in the preceding chapters.

4.3.1 Tasks

Our framework provides abstractions in order that the application developer need not to deal with low level issues. This enables flexibility and openness for extensions. The abstractions are based on the following three layers:

- RW device communication
- Transponder communication protocol
- Raw data transformation and interpretation

Another important task concerns measurement processing: The timer drift has to be corrected, erroneous measurements must be cleaned up and interpolated, and there are functions for deriving aggregate information from measurements, e.g. extremum information (cf. also 4.3.6).

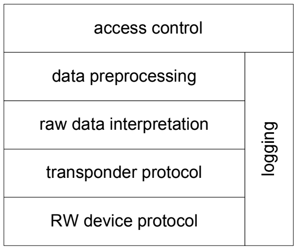


Fig. 46: Framework tasks

Besides the task described above, logging is especially important for the provision of diagnostic information in order to quickly find the source of problems when evaluating a prototype system.

Moreover mechanisms are realized in order to get along and transparently compensate for the deficiencies of the prototyping hardware.

4.3.2 Concepts

The framework provides facilities for accessing transponders and pre-processing transponder data by an edge host or server. It represents the basis for implementing its business logic. It is capable to handle several RW devices for a couple of threads (Fig. 47).

The most important conceptual feature is flexibility and configurability. The framework is *generic* with respect to RW devices, transponder protocols, transponder types, transponder data, and applications. The data model of the configuration is depicted in Fig. 48. Different transponder types the protocols and data configurations are dynamically resolved; so different transponder types and data configurations can be handled at the same time. The resolution process is illustrated in Fig. 49.

The next principle arises from the need of applications being deployed on both, desktop and handheld computers: Portability is ensured by compliance to the *.NET compact framework. C#* is used as programming language.

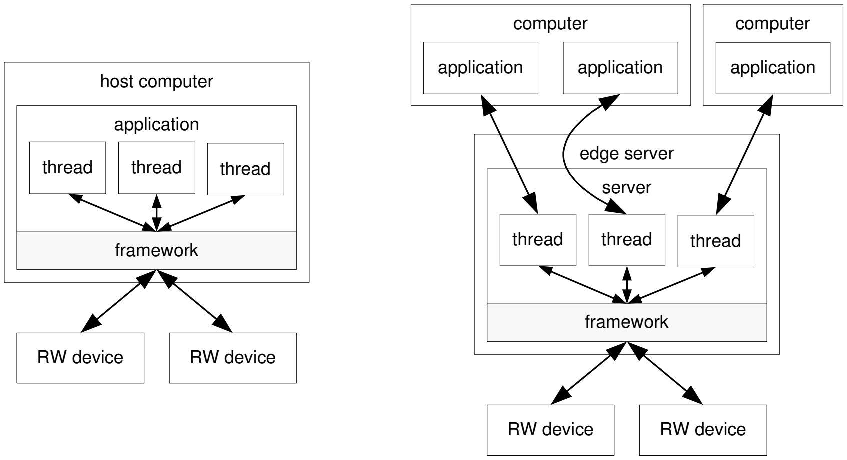


Fig. 47: Framework usage in simple architectures
Left: stand-alone application, right: server application

A concept going along with configurability is extendability. Extension modules can be implemented to support other RW devices, transponder protocols, transponders, and high-level data types. Moreover transponder specific temperature logging features, e.g. new log operations, multiple sensor values or several logs in transponder memory, can be easily supported by extension. Framework-level access control is provided on a thread basis. If a transponder provides security features they can be seamlessly integrated with the framework-level features.

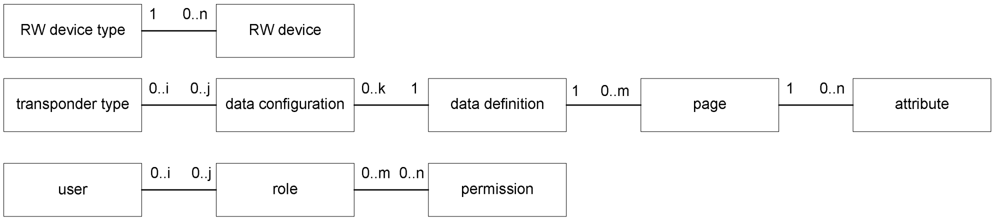


Fig. 48: Data model of the configuration

Interaction with a transponder means interaction with a physical object outside the sphere of influence of the software. That’s why it must be ensured that the developer has full control over its behaviour, i.e. when operations on the transponder are executed. This is also important due to the fact that transponder operations are usually rather time-consuming.

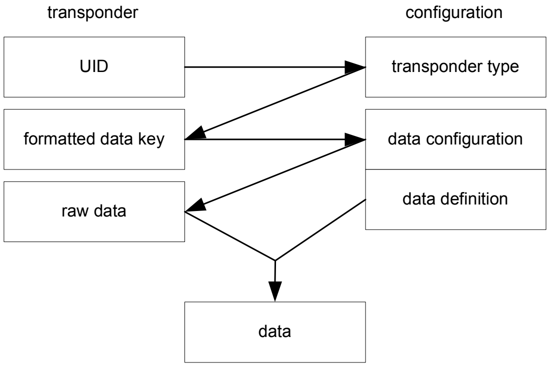


Fig. 49: Dynamic resolution of transponder type and data configuration
The transponder type is identified by its UID. Based on the transponder type and the formatted data key the appropriate data configuration and data definition for raw data interpretation is loaded.

A second aspect arising from the relationships between the physical and the virtual world is data consistency, which originates from write operations. When a write operation results in an error, it must be checked if the data has been written at all, or only partly or even correctly. Commit, verify and rollback mechanisms (see Fig. 50) are provided in order to alleviate implementing transactional semantics for write operations.

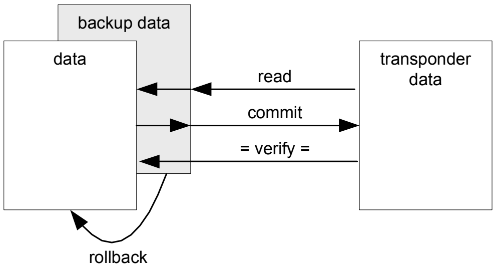


Fig. 50: Transponder data consistency mechanisms

The rollback information always contains the data of the last read or the last successful commit operation.

A feature tackling transient inaccessibility is command re-execution. A command is tried to be retransmitted at random time delays until it is either successfully executed or a maximum number of retries is reached.

Logging debugging information can be enabled for different layers: Exceptions, RW devices, transponder protocol command modules, and transponders.

The modular design of the framework aims at enabling integration of certain modules into bigger middleware systems.

4.3.3 Internal Architecture

The framework is composed of the core system, specialized classes and extension modules (see Fig. 51).

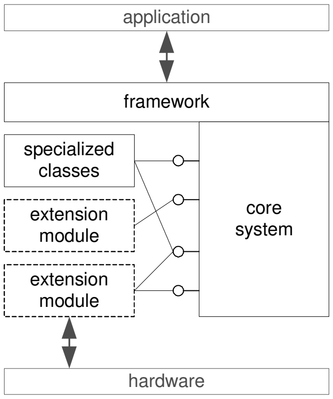


Fig. 51: Framework internal architecture

(see text)

The core system is a collection of abstract classes and interfaces, which are implemented by specialized classes and extension modules, and classes implementing the basic infrastructure and features. It is based on an abstraction of RW devices, protocol command modules and transponders. There are different transponder types forming a hierarchy (see Fig. 52) according to the transponder's functionality. *Raw data transponders* allow binary data to be written. High-level data types can be written on *formatted data transponders*. On the top level we have *temperature measurement transponders.*

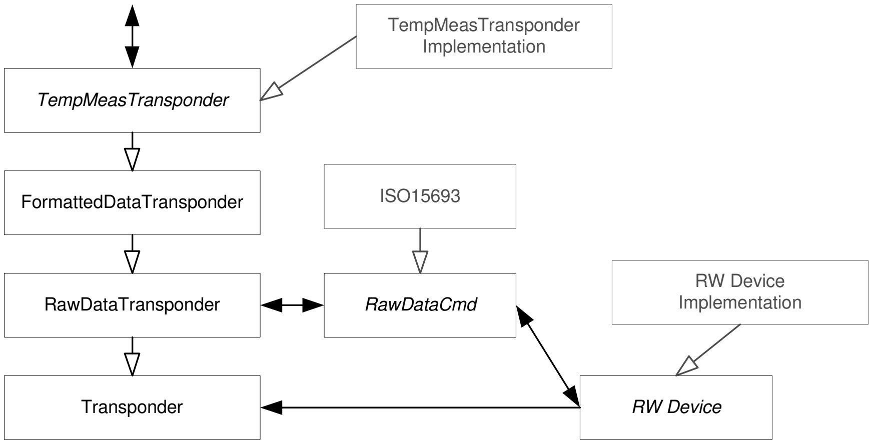


Fig. 52: Transponder hierarchy

The framework defines the interfaces for RW devices, protocols (raw data command modules) and transponders independent of technologies and implements common features in a hierarchic way.

The specialized classes provide an implementation of some abstract classes and interfaces which are commonly used by extension implementations, e.g. the basic ISO 15693 commands.

Extension modules implement abstract classes and interfaces in order to support technology dependent features, e.g. specific RW devices or transponders. An application which only uses the common framework features is absolutely unaware of the extension modules the framework makes use of.

In the course of an application the framework has to be initialized, i.e. the configuration has to be verified and loaded. Performing an inventory on a chosen RW device returns the transponders on which operations can be executed subsequently. The framework core implements the dynamic resolution of configuration which applies for a specific transponder. If the access control features are used the executing thread must be authorized to perform a certain action. This general model of using the framework in an application is illustrated in Fig. 53.

RW device communication proceeds as follows: The RW device is initialized and after a connection has been established, an inventory can be performed. For use in conformity with the ISO 15693 protocol the RW device has to provide methods for selecting a transponder and sending a command. The connection is closed on finalizing the framework.

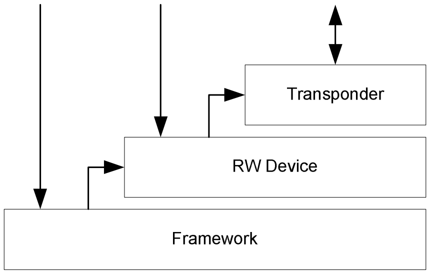


Fig. 53: Using the framework
An RW device is selected via the framework interface; the transponders in its field can be accessed subsequently.

The temperature measurement interface (Fig. 54) provides functions for getting and setting the transponder sensor calibration and the log configuration. The log can be started and stopped, and the log state and the measurements read.

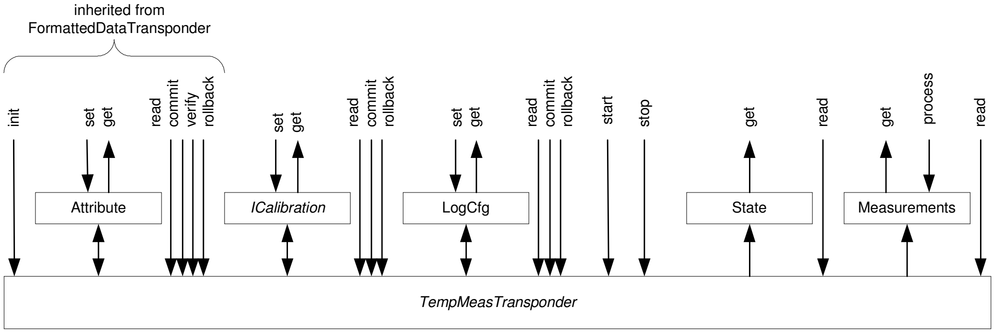


Fig. 54: Temperature measurement transponder interface

The rationale behind the formatted data interface works as follows. Every data configuration is associated with a key identifying it. The ISO 15693 [ISO01b] standard would provide two one byte fields, AFI (application field identifier) and

DSFID (data storage format identifier) to store this information, though the key is stored in the custom memory area for ease and flexibility. The formatted data model enables grouping attributes into pages. An attribute has a fixed length type. Transponder operations are performed pagewise and each page is tagged by a 16 bit CRC.

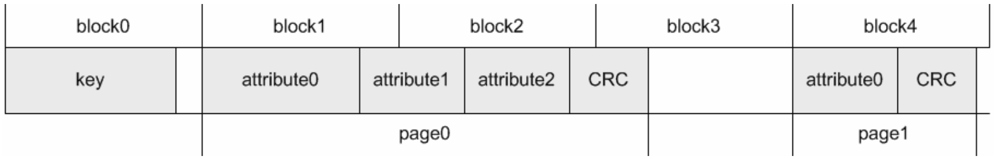


Fig. 55: Transponder data storage

The transponder memory is organized in blocks (usually 32 bit).The formatted data pages are aligned with the blocks. For each page a CRC-16 over the page data is stored.

An XML import/export utility class enables XML-formatted data input/output to/from the transponder classes.

4.3.4 Engineering Aspects

Designing an RFID systems involves the creation of a variety of software modules in the vertical dimension, from low-level protocol and device drivers up to multi-threaded and networked applications.

Prototyping is an important method for solving technical challenges in isolation before starting integration steps. Essentially, a framework consists of a set of interfaces. This is exactly where to start the specification as soon as the technical problems are settled and it is known which information has to be exchanged.

Modular design requires *design by contract*, i.e. the specification defines exactly what a component expects at its interfaces and what its reactions will be, not only on a semantic level but also on a formal level. A method applied in formal verification languages is using pre- and postconditions. A precondition restricts the parameters in order that the postconditions are always fulfilled. The postcondition defines the exact behaviour, i.e. the return value of a function or the state change performed by the function. This method has proved to alleviate implementation and specifying tests decisively.

When the implementation proceeds incrementally, module tests can already be written in parallel by defining test cases using the specification. A tested module represents a reliable building block which forms the basis of continuation. Extendability implies that framework extensions must reliably cooperate with the framework. Therefore extension interface functions are guarded by issuing "programming exceptions" when the preconditions are violated.

The logging features integrated into the framework are actually a good structured instrumentation which can be executed optionally and which is absolutely necessary for testing, debugging and diagnosis in the field.

4.3.5 Test

A problem with testing the framework is that there are inherently stateful entities which make it difficult to achieve a high coverage. An efficient classification of input data is necessary for tackling the combinatorial explosion of test cases. Therefore it is necessary to reduce states during operation wherever possible. For those classes simple module tests can be employed.

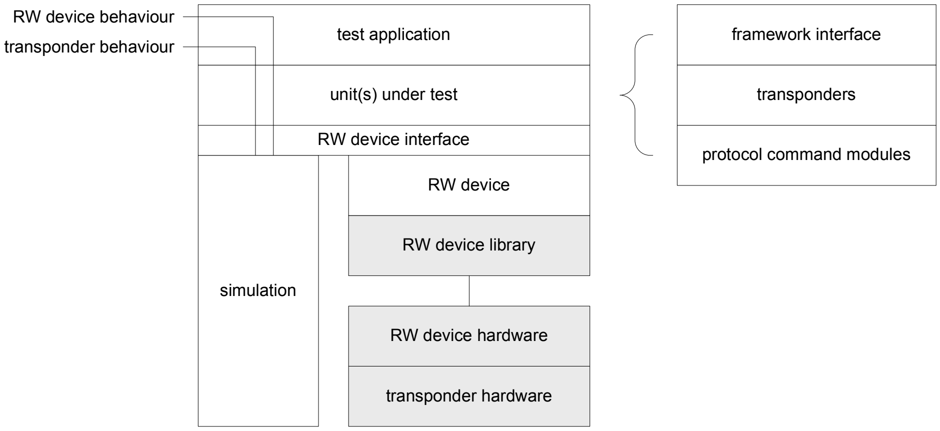


Fig. 56: Test framework
A simulation of the hardware layers allows for testing the effects of hardware errors.

A second issue with RFID systems is that many test cases are related to hardware errors and transient problems of hardware interaction, and thus cannot be reproduced arbitrarily. A simulation model of the hardware components makes these cases testable. There also exist hardware emulators for transponders [Rede05]. In this project a software solution has been chosen covering both the RW device and the transponder. This enables testing the reaction of the software to RW device errors or errors emerging from transponder interaction, as well as transponder errors and transponder data errors. The simple testing framework (Fig. 56) allows to plug-in the simulation model as a special RW device and thus the same test cases for protocol command modules, transponder implementations and the framework interface can be used as for the real hardware.

Besides these automatic tests, semi-automatic tests which demand the user to interact with the hardware have been created to test the most important problems with RW device communication.

4.3.6 Application Development Components

Certain operation patterns are repeatedly used in RFID applications, these blocks are grouped to components which are intended to facilitate application development:

Some RW devices offer a scan-mode which continuously looks for transponders in the field - using software this means inventory polling. Normally, the transponder has to be aligned with the RW device's antenna and then a button is pushed to detect it and perform the corresponding operation. With inventory polling the operation is performed as soon as the transponder is readable.

Bulk detection (see 5.1) requires a sophisticated visualization in order to make it viable under adverse circumstances. Bulk detection consists of several inventory rounds, the detection status of the transponders has to be tracked.

Temperature measurement data encourages a graphical representation by a line chart. Temperatures plotted over the timeline is the adequate visualization of a complete temperature history. Three-point measurements are rather visualized by a compact, intuitive arrangement of the following information: Begin time of the violation (exceeding the allowed range), its extreme value, the duration and the limit which has been violated.

For the prototyping it has been necessary to perform the two-point calibration (see 2.3.4) by myself. A component enables step by step bulk calibration. The transponder's log is initialized and started, the transponders are exposed to the first ambience with constant temperature, after reaching steady state they are exposed to the second one. Then the log is stopped and the automatic detection of the calibration points is performed as follows:

Find measured steady state temperatures $T_{0,sensor}, T_{1,sensor}$ at ambient temperatures T_0, T_1 with

$$\left(\left|T_{0,sensor}-T_{1,sensor}\right|\rightarrow\max\right)\wedge\left(\frac{dT_{0,sensor}}{dt}\rightarrow\min\right)\wedge\left(\frac{dT_{1,sensor}}{dt}\rightarrow\min\right)$$

Time discrete version: N measurements, window length K

$\forall n:0..N-K-1$ calculate $m_n=\sum_{k=n}^{n+K-1}T_k$ and $d_n=\sum_{k=n}^{n+K-1}\left|T_k-m_n\right|$

Find indices n_0, n_1 satisfying the conditions

$$\left(\left|d_{n1}-d_{n2}\right|\rightarrow\max\right)\wedge\left(d_{n1}\rightarrow\min\right)\wedge\left(d_{n2}\rightarrow\min\right) \tag{9}$$

4.3.7 Prototyping Hardware

As prototyping transponders samples of the KSW microtec VarioSens [KSW06] have been used. The VarioSens is an ISO 15693 transponder with an integrated temperature sensor and a foil accumulator as energy source. It provides 1024kbits of memory and the logging features described in 3.2.3.

Fig. 57: KSW microtec VarioSens

For desktop applications the RW devices of the Siemens Moby D series [Siem03] have been used. The Moby D10 is able to handle two antennas, which provide in a tunnel a detection window of about 40x40x70 cm. A device driver is supplied which handles the serial port communication and RW device commands.

Fig. 58: Siemens Moby D10
(www.siemens.com)

A Fujitsu Siemens Pocket Loox with an ACG Handheld Reader (www.acg.de) for the CF slot has been used for mobile applications with a device driver for the Windows^{TM} mobile operating systems available.

Fig. 59: Fujitsu Siemens Pocket Loox equipped with an ACG Handheld Reader

Calibration points have been measured with the help of a commercially available digital multimeter and a thermocouple with a resolution of 0.1°C.

4.3.8 Demo Applications

General purpose demo applications for desktop and handheld platforms for showing the transponder features have been developed allowing the following tasks to be performed:

- Bulk detection.
- Visualization of transponder measurements and data.
- Configuration of the transponder, i.e. the log, the data, including the possibility to store default values.
- Calibration of the sensor.
- Logging transponder interactions on various levels.

Applications for demonstrating the chosen use cases of the blood supply chain have been implemented. As an illustrating example, we describe the bedside test application with the following aims;

- Identify the bag and the patient and check if they match.
- Check if the temperature history is in order. Inspect the details if necessary.
- Write the bedside test result to the transponder and confirm it.

The patient is identified by his/her patient card. The user cannot read the blood bag and the patient card without authentication and authorization by his/her hospital staff card. The confirmation of the result must be done by the entitled responsible personnel. The application flow is depicted in Fig. 60.

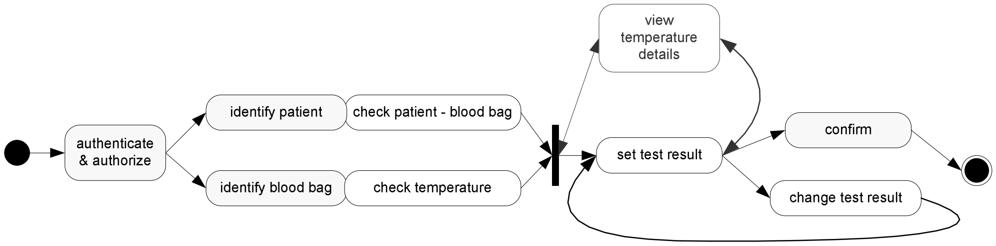
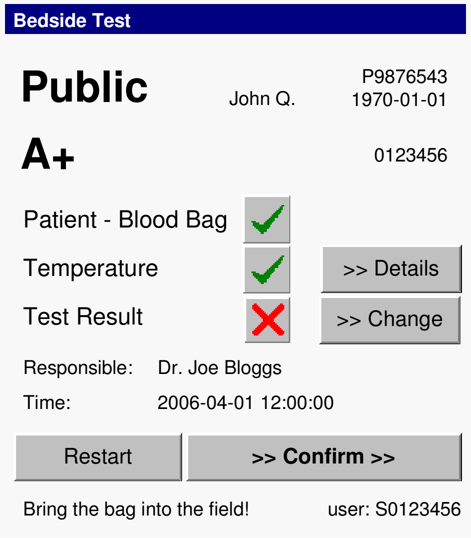


Fig. 60: Action flow of the application
The greyed actions involve transponder interaction.

A screen shot of the confirmation dialog is shown in Fig. 61. All inputs are done by reading transponders or pressing buttons.



Bedside Test

Public John Q. P9876543 1970-01-01

A+ 0123456

Patient - Blood Bag ✓

Temperature ✓

Test Result ✗

Responsible: Dr. Joe Bloggs

Time: 2006-04-01 12:00:00

Bring the bag into the field! user: S0123456

Fig. 61: Bedside test dialog for confirmation of the test result

Chapter 5

Further Aspects

Three major topics which appear when considering an RFID-based temperature monitoring system of blood bags are discussed here: The problem of detecting several transponders in the RW device's field, usually referred to as *bulk detection*; Furthermore RFID middleware and tracking and tracing systems and the usage of their features in the given application; and also the status of standardization throughout the layers of the system are subject of this chapter.

5.1 Bulk Detection

Bulk detection means recognizing several transponders in the RF field of one RW device which is a very useful means for parallelizing operations at the user interface. The intrinsic problems of bulk detection as well as the specific problems with blood bags, e.g. the transmissibility of their liquid content are discussed in this section..

5.1.1 Anti-Collision

Communication with several transponders in the RF field makes a medium access mechanism necessary. In RFID technology normally, TDMA (time division multliple access) is used, i.e. it is communicated sequentially. This is rather easy when a transponder can be addressed for information exchange, but an ”address”, i.e. the transponder's ID, is not known in advance, hence it must be determined during the inventory phase. Therefore anti-collision algorithms are required for getting the appropriate IDs. A detailed description of these algorithms can be found in [Fink03], [Vogt02] and [Lee05].

Generally, we can distinguish two access types: deterministic and probabilistic medium access. In HF systems the ALOHA method is used, which belongs to the latter type. The RW device issues a request and each transponder answers after a random delay. Obviously, collisions are not avoided by this scheme and it needs several rounds for detecting all transponders. UHF systems mostly use a deterministic approach, namely binary tree walking. The RW device requests only transponders with certain UID prefixes to respond. A branch of the tree is no longer pursued if there is one or no transponder found.

ISO 15693 [ISO01b] makes use of framed slotted ALOHA. The RW device sends the inventory command; the response window (frame) is divided into slots which are marked by the RW device by issuing a special pattern (i.e. the EOF signal). The transponder chooses a slot randomly for its response. This eliminates collisions due to the partly overlapping responses. The efficiency of this approach reaches 36.8%, i.e. the number of slots filled with one transponder [Lee05]. A recognized transponder is set mute and the procedure is repeated until there are no more collisions or a timeout is reached. The required number of slots increases exponentially with the number of transponders [Lee05]. Using too few slots yields the majority of them filled with collisions, and obviously using too many results in waste of time.

5.1.2 Practical Problems

Bulk detection requires that all transponders must be recognized, but the number of transponders is normally unknown. The resulting problem is referred to as the false negative read problem [Floe04], because transponders remain undetected due to collisions, interference, and antenna detuning when transponders are to close to each other. In [Vogt02] this problem is formalized and investigated by a Markov model. Each inventory round is regarded to independently return a subset of the present transponders. A detection probability is chosen, e.g. 99% of transponders have to be recognized. An inventory algorithm has been developed which estimates the number of transponders and determines the number of slots dynamically and adaptively. Unfortunately, the predicted results are hard to achieve in practice.

Furthermore, the use of probabilities is not sufficient and appropriate in the application considered here, because with probabilistic anti-collision one can never be sure that all transponders are recognized. The blood bag application poses the problem that all bags have to be recognized which cannot be inferred from having detected all transponders, because a transponder could be defect and does not respond. Moreover the recognition rate depends on the distribution of the transponders in the RW device's field. There are special effects, such that adding a transponder to the field could produce fewer transponders being recognized because of two transponders one or both are not recognized when they lie too close to another.

5.1.3 Solution

Defect transponders cannot respond, therefore even in case of a perfect detection algorithm still there are bags which remain unrecognized. That's why we need an assumption for the blood bag application in order to be able to decide if there are undetected transponders: The number of transponders, i.e. the number of bags, is known.

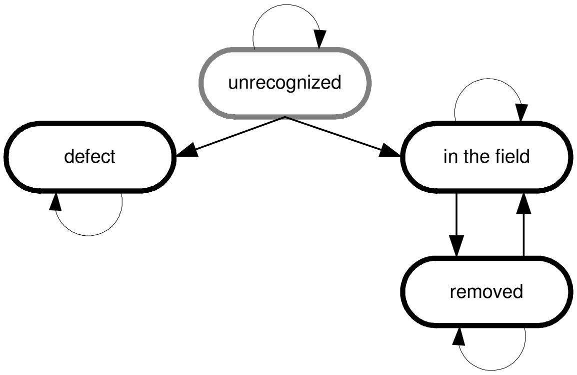


Fig. 62: Bulk detection state chart

Initially, all transponders are unrecognized. In the end, they are classified as detected (in the field or removed from it in the final inventory round) or defect.

Practically, the first attempt, when a transponder is not recognized, is changing the spatial distribution, e.g. by shuffling. Clearly, this method will not succeed if one transponder is defect. A more systematic approach is the iterative physical removal of transponders. If a transponder has already been detected, it must become undetected in the next round. Otherwise it has not yet been recognized and has to be left in the field, and another transponder is chosen. Therefore the unrecognized transponders are never removed from the field. Finally, all removed transponders have been recognized; all remaining transponders have to be checked individually whether they are defect. The detection of transponders follows the states in Fig. 62. In the worst case all transponders are checked sequentially. For probabilistic anti-collision it has to be assumed that each inventory returns an arbitrary subset of transponders in the field. Therefore the decision whether a physically removed transponder has already been detected unfortunately requires user intervention. This procedure could be formulated as follows:

transponders in the field P; $inventory(P) \subseteq P$; initially $|P|=N$; transponder t; predicates $removed(t), recognized(t), defect(t)$

```
$T := inventory(P)$
$do$
$\{$
 $P := P \setminus \{t\}, t \in P$
 $T := T \cup inventory(P)$
 $If\ ((t \notin T) \vee \neg removed(t))\ P := P \cup \{t\}$
$\}$
$while\ ((|T|<N) \wedge (\exists t:T:\neg removed(t))$
$\forall t:T:recognized(t)$
$if(|P|>0)\ \forall t:P:((inventory(\{t\}) = \emptyset) \Rightarrow defect(t))$          (10)
```

5.1.4 Experimental Results

Experiments with the Siemens Moby D10 RW device [Siem03] have been performed. As passive transponders we have Infineon my-d (www.infineon.com), with an allowed range of about 38cm, and KSW microtec VarioSens [KSW06] with a range of up to approx. 30cm due to its higher interrogation field strength (cf. 2.2.2). Bags are filled with 500ml NaCl solution and have showed no effect on the range. The effects of orientation and distance on the field strength are shown in Fig. 63.

The minimal distance between two transponders is about 5mm. At maximum four transponders directly stacked with a minimal distance of 5cm could be detected. When two antennae are arranged in a tunnel the fields add up and increase the total range by approx. 5cm.

A general recommendation for bulk detection is that the transponders' antennae are distributed as uniformly as possible over the RW device's antenna cross section. With blood bags in a box this could look like in Fig. 64. The cooling plates have to be aligned normal to the RW device's antenna.

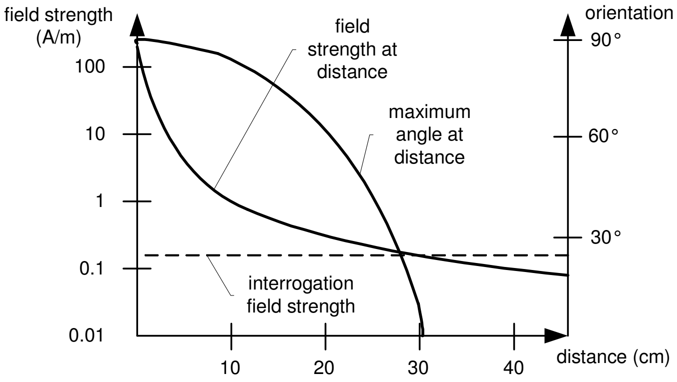


Fig. 63: Field strength and maximum angle
between the antennae over the distance between them for the interrogation field strength H_{min}=150mA/m [KSW06] (cf. [Fink03])

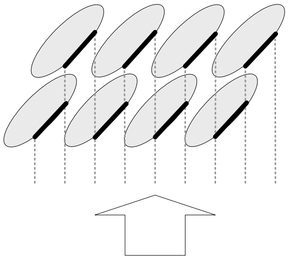


Fig. 64: Blood bag arrangement for bulk detection

5.2 RFID Middleware Systems

This section gives a survey of RFID middleware systems. Most RFID middleware systems are modular, loosely coupled and event-based. Besides the four ubiquitous computing base functions [Scho02], identification, monitoring, localization and notification, management and maintenance aspects play a major role.

5.2.1 RFID based Tracking and Tracing

Tracking means monitoring an object as it passes through the process, whereas tracing is analyzing how an object has passed through the process. One could say, that in the temporal dimension, tracking follows an object's trace in the forward direction, whereas tracing in the backward direction (see Fig. 65).

Existing RFID middleware suites target especially at tracking and tracing tasks in logistics and manufacturing automation. This is monitoring, looking up and tracing shipments, alerting and informing trading partners. Benefits [McFa03] [Flei05] come from optimal route planning, acceleration of loading and unloading operations. Goods are commissioned, transport documents generated, and on receiving charges are checked – all automatically, thus an increase of delivery quality in time and count shall be achieved. Processes can be optimized by analyzing throughput times. Reduction in data entry and the time needed for reconciling missing or wrong shipments, reduction of out-of-stock problems in warehouses, good misplacements, an increase in inventory visibility and theft prevention are expected. Furthermore tracing enables effective product recall. In pharmaceutical industry traceability is often a legal requirement..

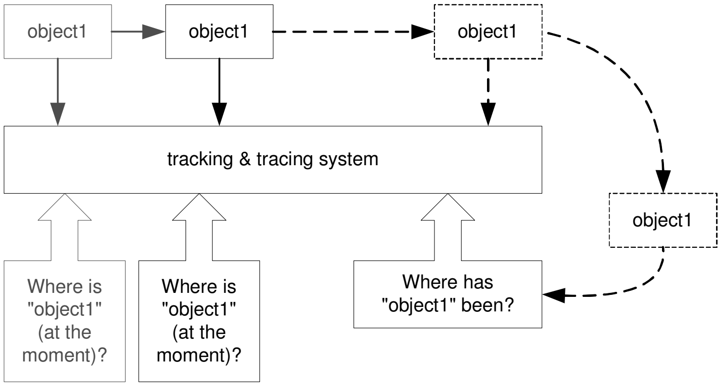

object1
object1
object1
object1
tracking & tracing system
Where is "object1" (at the moment)?
Where is "object1" (at the moment)?
Where has "object1" been?

Fig. 65: Tracking and tracing

The information gathered during tracking the object is later on used for tracing its path back.

5.2.2 RFID Middleware Features

Most RFID middleware systems are driven by the tracking and tracing scenario, which is characterized by an information flow from the "edge" of the network, where the data is collected and subsequently pre-processed, to its centre, where the information is held ready for distribution. The software layers (see Fig. 66) running on the hosts, where the low-level data processing is performed, next to the RW devices are subsumed under the term *edgeware*. *Middleware* means hiding the network, i.e. transparent information exchange over a scalable architecture providing reliability, availability and security; infrastructure management aiming at maintainability; and application specific adaptability by openness, and plug-and-play capabilities.

RFID middleware systems generally consist of the following modules (cf. [Prab05]): Modules abstracting transponders and RW devices, protocols, i.e. for transponder communication and RW device communication. Data processing modules perform filtering, aggregation, correction and caching of data. Filtering means data reduction by selecting events by information of RW device, UID or transponder type or by pattern matching on this information. Aggregation leads to creation of condensed information out of selected groups e.g. by establishing relations between entities, counting events, recording passage by entry-exit-pairs, or joining several RW devices to one logical one [Floe05]. The information exchange system buffers the data temporarily and provides it to enterprise applications over web services, publish-subscribe mechanisms and asynchronous messaging. The whole stack is spanned by management and security features.

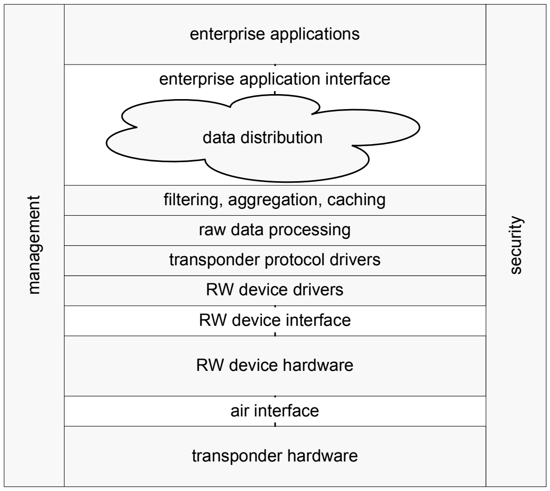


Fig. 66: RFID system layers

The information passes through several layers from the transponder hardware to the enterprise applications and vice versa. The inherent spatial distribution of the infrastructure requires effective management and security mechanisms across all layers (cf. [Prab05]).

RFID middleware systems provide real-time data for operational monitoring and analytical data for reporting to enterprise applications, e.g. ERP (enterprise resource planning) systems. Besides the productive information paths, management, maintenance, and error diagnosis are highly important: A variety of hardware, PCs, handhelds and RW devices have to be administrated in dynamic networks with on-the-fly device registration and configuration, different configurations have to be supported - device firmware updates and software deployment have to be performed centrally without service interruption, and device status and health have to be continuously monitored. It is important from a maintenance perspective that these management services are strictly separated from the business logic. Middleware system often come with development support to easily adapt a system to the application needs, e.g. for building workflow processes.

Initially, RFID solutions were often isolated within companies or only span a few trading partners. EPCglobal (formerly the Auto-ID-Center at the MIT, www.epcglobalinc.com) is an attempt to create an infrastructure reference model for sharing information throughout companies and has developed standards for such a global system [EPC05] [Sarm03]. Although the system does not pose any restriction on the transponder functionality, it is aimed at a reduction of costs by using the most primitive transponders possible which carry only a UID. In essence, it is recorded when a transponder has been detected. The EPCglobal network consists of the following elements: An object naming service (ONS) for querying which decentralized EPC information service (EPC-IS) provides object and tracking information about a given EPC (*electronic product code*). The data can by queried by whatever enterprise application is authorized. The RFID information is acquired from edge servers which implement the application level event (ALE) engine which filters and aggregates events in order to generate business-relevant events to be forwarded upwards.

5.2.3 Examples

This section describes the key features of some chosen commercial and academic RFID middleware systems.

Sun's RFID Network [SunM06] uses three conceptual layers: *sensor, event and business layer*. Sensors are all imaginable data generating devices. The Java System RFID Software is mainly based on Java technologies. The RFID event manager implements an EPC compliant ALE engine; the RFID information server the business-level event (BLE) engine. The Sun Industry Solution Architectures aim at the integration of third party modules. The system is used in a pilot at Narita Airport, Japan, for baggage tracking including an online querying application of the baggage state.

WinRFID [Prab05] is a development by the University of California in Los Angeles (UCLA) . It is a general purpose RFID middleware system based on .NET and structured in five layers: *hardware, protocols, data processing and persistence, web services including management and monitoring, and the applications*. The layers can be adapted to application needs by a rule engine.

RFIDStack [Floe05] is developed at the ETH Zurich. The messaging system is exploited to implement a feedback mechanism for performing filtering directly on the air interface and thus freeing up RW device bandwidth. A second feature is the virtual transponder memory system (VTMS), which provides transponder memory replication and consistency mechanisms.

Effectively, every big integrator offers RFID solutions. There are the explicitly EPC-targeted systems, i.e. OAT foundation suite by OATSystems (www.oatsystems.com), and RFTagAware by ConnecTerra (www.connecterra.com) which are both involved in the EPC standardizing process. More general solutions are IBM's WebSphere RFID Device Infrastructure (www.ibm.com), Oracle Sensor-Based Services (www.oracle.com), SAP's Auto-ID Infrastructure (www.sap.com), which is also used in Metro's Future Store Initiative (www.future-store.org), and systems by Franwell/Globeranger (www.globeranger.com), and Manhattan Associates (www.manh.com). Smaller, but complete systems are Tavis by RF Code (www.rfcode.com), and Savi's SmartChain (www.savi.com). The immense investments and process changes involved with a full-featured RFID solution demand the ability of starting small and expanding it to a big system in order to minimize initial costs.

RFID middleware systems offer the infrastructure on the top of which applications are built and the necessary facilities for gluing existing applications together. Considering the blood supply chain, it can easily take advantage of the general infrastructure features like management and monitoring, as well as conventional tasks like warehousing, receiving and shipping operations. One problem is that the big EPC-targeted RFID systems are not designed for information flow towards the edge and manual handling with direct user interaction.

5.3 Standards and Standardization

There are several attempts to standardize the entire RFID system stack: the transponder-RW device interface, the RW device-host interface, the data structures and encoding and the RW device management. E.g. EPCglobal for tracking applications, which standardizes all from the air interfaces, over the EPC ID data structures, the RW devices, a high-level API, the network facilities, e.g. the ONS, to the reader management (currently in work) [EPC05]. This section surveys the existing standards and assesses where standardization is reasonable and desirable.

5.3.1 Transponder – RW Device Interface

Depending on the RFID technology a variety of standards exists for the air interfaces. ISO 18000 [ISO04c] is the attempt to subsume specifications for all RFID technologies in one standard for item management applications.

The transponder [KSW06], which has been used for prototyping, employs custom commands for the temperature measurement functions. Clearly, all types of operations can be mapped to standard read (send request, receive data) and write (send data, receive acknowledgment) commands, but the internal implementation might be different from “normal” custom memory, because memory containing configurations, measurement state and data are also accessed by the logging logic. Standardization has to pay attention to an efficient transponder-internal implementation. However, the basic properties and functions as digital calibration, log configuration and measurements are worth being standardized, both in data and command structure. Such a standard need not be focused on temperature measurement but can be generically applied to a variety of sensors following the same logging scheme. Moreover e.g. access control features, should be concern of further standardization activities.

5.3.2 RW Device – Host Interface

For the interface between the RW device and the host computer widely accepted standards do not exist yet. There is no standard providing a generic abstraction of RW device operations and data, although this would immensely improve interoperability.

Aspects subject to standardization are: Protocol-independent transponder interaction and data exchange, RW device configuration, health status and firmware update management, and security features on both interfaces. The specifications should be independent of the communication medium used.

An attempt made by the Internet Engineering Task Force (IETF) [Kris05] is the smart lightweight RFID reader protocol (SLRRP) which provides a generic command set for RW device configuration and transponder interaction.

Other trends are intelligent RW devices [Hess06] which replace the edge host computer by performing the data pre-processing and business logic itself, thus providing high-level data at the network interface.

5.3.3 Data Representation

Data representation concerns the data encoding on the transponder as well as the data exchange with the RW device respectively within the middleware system. Such standards are currently in work [Walk04]; they are generally based on ASN.1 (abstract syntax notation, ISO 8824, 8825, and 9834) for encoding transponder data and XML/XSD (XML schema definition, www.w3c.org) for RW device data exchange.

The standards ISO 15961 and 15962 tackle these problems for item identification: ISO 15961 [ISO04a] describes the application interface, i.e. the application-side RW device interface, i.e. the RW device communication by high-level operations performed on the transponder data and the data representation; ISO 15962 [ISO04b] deals with the transponder-side interface. ISO 24752 will define the RW device management interface, ISO 24753 support for sensor functions; the latter two standards are still in work [Walk04].

XML/XSD based data representation has evolved to a widely used for data interchange between distributed applications, because of its flexibility, automatic syntax verification, tagged semantics and easy mapping to relational databases. XML is only reasonable if the data has already been pre-processed; it does not make sense transferring raw binary data over XML. Therefore it is perfectly suited for data transfers above the edgeware layers.

5.3.4 Blood Bag and Measurement Data

Traditionally, Codabar-based barcodes data structures, e.g. as defined by the ABC (American Blood Center, www.americasblood.org), have been employed for blood bag labels, but there have been and there are still proprietary systems in use [Wagn06b]. The ISBT-128 standard [ICCB04] [Ashf02] should unify these systems. It is based on Code 128, which provides more characters and better integrity checks. The ICCBBA administrates databases for looking up the codes' meaning and for registration of institutions.

In the long term, a unification of blood bag labels at least on a European level should be achieved for breaking down the regional barriers for blood supply. In any case a minimum common knowledge among the institutions is required for interpreting the codes.

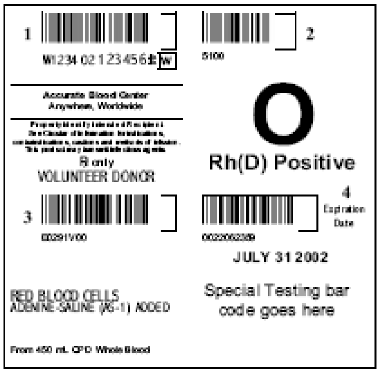


Fig. 67: ISBT-128 barcode label
[Ashf02]

The problem with standardizing measurement data representation is the need to store it as compact as possible and without performing much computation on the transponder. Nevertheless an easily parameterized and standardized procedure for decoding measurement data is desirable.

Chapter 6

Discussion

In this chapter the properties of the solution options are presented, impacts of RFID-based temperature monitoring on the blood supply processes as well as economic aspects and remaining problems. are discussed Finally, a prospect on system extensions and future developments is given.

6.1 Properties

A decentralized solution has been strived for, which minimizes communication, infrastructure, common knowledge and process changes. The use of an RFID transponder as a portable data store allows a maximal degree of decoupling the involved members of the process chain, due to the fact that many operations can be performed locally, even offline. However, an RFID-only approach has decisive impacts on reliability: A defect transponder, i.e with a sensor defect, or which refuses its measurements or data to be read, causes a disposal of the bag it is attached to. This problem cannot be solved by the hybrid approach neither because the most recent temperature history is lost, although previous measurement data is still available in the transponder's virtual counterpart. RFID technology is "pervasive", i.e. it leaves many processes untouched at the surface but provides benefits in the background.

The RFID temperature monitoring framework provides a reference implementation of general concepts related to sensor-enhanced RFID transponders. It is targeted at reusability and deployment in pilot projects.

6.2 Impacts on the Process

Computerized systems become indispensable for their users when they offer them clear benefits. Usability plays a major role, but there is also the effect that – if not exaggerated – the processes become more guided and channelled because a stricter workflow is imposed, which can improve process quality on the whole.

RFID temperature monitoring does not provide a continuous warning capability, i.e. problems are only recognized when it is already too late. The benefits come from the feedback on the process by improving it steadily, the increase in the quality of blood products, and traceability. Automatic identification reduces human-made faults and aims at less confusion of blood products. The time savings due to this automation are also substantial, although there will be some loss in the beginning until RFID interaction is mastered as routine. The closing of the blood chain by the RFID recycling system increases transparency in blood supply and haemovigilance monitoring.

6.3 Economic Aspects

Simple transponders are sold for 0.05€ or less; the price may be two orders of magnitude higher for high-end transponders. The higher the value of the product monitored by the transponder, the less significant becomes the transponder’s price. Although blood is not a cheap resource, single use of transponders is not encouraged. A closed-loop scheme with transponder recycling may reduce the price to a bearable amount. As in any RFID project, one has to start small and think big. Blood supply institutions usually belong to the public health care system which currently suffers from financial problems.

The RFID temperature monitoring system comprises initial costs for the hardware, RW devices, computers, handhelds, and the network infrastructure, for software, the RFID middleware, the development of the applications, and the integration effort, for the process adaptions at the bag manufacturer, and for the recycling centre. Furthermore the users have to be instructed and trained. The running costs consist of transponders, maintenance, and the operation of the recycling centre.

The money and resource savings probably will not be recognizable at the beginning, but after process improvements.

6.4 Open Problems and Prospect

Although the current technology is suitable for the intended tasks, further tests are still required in order to improve the reliability of the transponder, the most critical part of the system.

For establishing nationally and internationally unified systems, it is strongly encouraged to define open standards as quickly as possible in order to channel the system development of different competitors to interoperability. However, the short durability of blood products restricts the geographical expansion of logistic networks in blood supply. Nevertheless future benefits can arise from cooperation efforts amongst regions in emergency situations. Reporting will become significantly easier due to this technology.

Furthermore supply chain transparency allows a better coordination between blood banks and blood depots, and thus tackling another problem, namely the disposal due to expiry which amounts to almost 50% of discard [Parr03].

Chapter 7

Further Applications

RFID-based temperature monitoring is also interesting in other application domains. This chapter gives an overview of the specific problems and properties of four selected fields: Wine, beer, drugs, and sensitive ancient documents.

7.1 Wine Trading

The degradation of the wine quality during storage and transport is directly imputable to temperature exposition.

7.1.1 Goals and Properties

The monitoring of wine bottles during transport, especially by ship from overseas, can support the keeping of the contracted temperature conditions with the carrier and thus improve the quality control of wines.

Wine is usually shipped in 0.75 litre bottles. Quality wines are traded for up to 50€ per bottle. The Austrian wine importer and trader *Wein & Co* [Hamm06] sells 1.6 million bottles per year, the ratio red to white wine is about 40:60. Wine is ideally stored at 12°C ±4°C. Temperature conditions show direct effects on the wine quality. The peak temperatures are critical: If wine freezes the bottle could eventually get broken; continuous coldness leads to the precipitation of tartar, especially for young wines in the first year. Above 30°C the cork may be driven out or the bottle gets broken; furthermore proteins start to excrete. White wines and wines with natural cellar treatment are more susceptible. Moreover the protein stability is dependent on the year and grape. Red wines are less sensitive because of the higher alcohol and tannin content. Red wines are usually stored up to 25 years, white wines up to 10 years.

7.1.2 Scenario

Due to economic reasons monitoring on carton packaging level has to be considered first. Wines from overseas, e.g. Australia, are ordered directly after bottling, i.e. one to three years after vintage. The producer transports the bottles in cartons (six or 12 bottles) to the port where it is temporarily stored. They are shipped in normal or thermo containers (12000 bottles), which takes about 3.5 weeks from South Africa, and five weeks from Chile or Australia to Hamburg. Afterwards they are transported by train to Vienna and by truck to the central warehouse and to the shops.

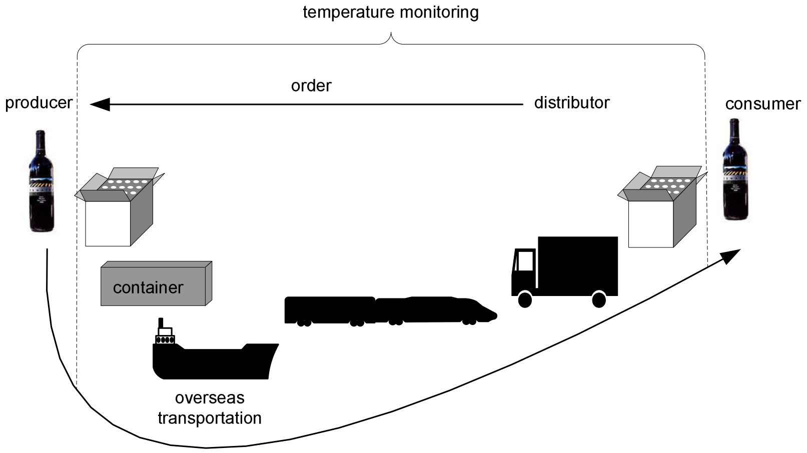


Fig. 68: Wine import from overseas

It is desirable to perform the monitoring on the carton level from the producer to the shop. The warehouse management in the central depot as well as the payment and inventory in the shops makes use of EAN-13 barcodes on cartons and bottles which are either on the product label or sticked on in the central warehouse. Handheld computers are used for performing the administrational tasks [Hamm06].

7.1.3 Discussion

Quality problems provoke discontent of customers. There are no figures about reclamations, but the wine has to be taken back because of economic competition reasons, even if a customer's fault can be proven. The replacement of carton barcodes by temperature monitoring RFID transponders is possible. A recycling system can be established between producers and wholesalers [Hamm06].

RFID temperature monitoring of wines is a promising application because of the clear, well-examined effects of temperature exposition on the quality.

7.2 Beer Kegs

Beer for the gastronomy is shipped in kegs. Beer degrades in quality and loses its flavour when exposed to heat or coldness. Tracking and monitoring beer kegs is a classic closed-loop application because kegs are returnable and reusable.

7.2.1 Goals and Properties

RFID-based temperature monitoring is used to find out problems during transport and to check the quality of returned products for reselling. Furthermore the tracking of the kegs allows for finding out more easily where kegs are lost in the cycle.

The *Ottakringer* brewery [Aroc06] uses 20, 30, and 50 litre stainless steel kegs which are practically indestructible. The value of an empty keg amounts to approx. 80€. Each keg is reused about four times per year employing a deposit system; 80000 kegs circulate in total. Individual kegs are currently not tracked, only pallets are labelled with barcodes for warehousing tasks. Beer should be stored at a constant temperature between 6°C and 12°C for at most three to six months depending on the brand. Quick temperature changes lead to quality degradation by clouding. The kegs are transported without temperature monitoring; the only guidelines are to deliver as quickly as possible in winter below -3°C and not to expose them to direct sun in the summer. There is no information about customer reclamations, but inappropriate storage by the customer is considered to be a problem.

7.2.2 Scenario

Each new keg is equipped with transponder in the brewery. The monitoring is started after filling and stopped on take back. The process chain proceeds as follows: Empty kegs are filled and stored up to 15 days in the brewery. The transport to the customer, mostly gastronomy, is performed by trucks owned by the brewery. The kegs are picked up at the customer and cleaned.

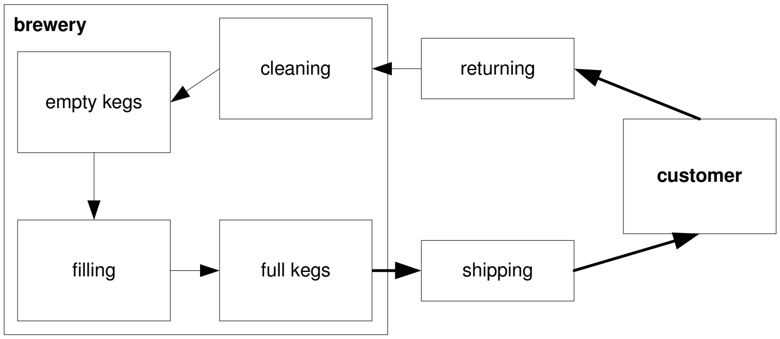


Fig. 69: Keg circulation

Temperature monitoring is performed along the bold arrows.

The following data is stored on the transponder: A circulation counter, the article number, the lot number, the expiry date, and the identification of the customer.

7.2.3 Discussion

Tagging kegs with RFID transponders for identification purposes is already implemented by e.g. Scottish & Newcastle [Pfla02]. Ottakringer also plans to equip all kegs with transponders [Aroc06]. The main problem in this application is that the transponder cannot be read when directly attached to a metal surface; for 13.56MHz technology the distance has to be at least 5mm. Nevertheless the temperature measurement has to be authentic. Moreover, manipulations have to be prohibited and the transponder has to be protected from mechanic stress. Due to the value of a keg, defect transponders have to be replaced.

7.3 Pharmaceuticals

Pharmaceutical products are subject to temperature monitoring by law [AMBO04]; but drug safety does not only involve storage conditions but also protection against counterfeiting which could be tackled by RFID technology.

7.3.1 Goals and Properties

RFID temperature monitoring could enable effective control of carriers and distributors, especially with respect to accepting returned goods.

Generally [AMBO04], all drugs must not be stored outside the range from 2°C to 25°C; some medicaments as vaccines require cooling between 2°C to 8°C. Currently, the cold storage is monitored and single-use loggers are employed during transport for valuable products; but there is no control, guarantee or documentation during storage and transport enforced by law. Usually, the temperature integrity is not even checked by the customers [Döll06].

Drug counterfeiting is an international problem [Flei05], i.e. medicaments with no, weak or even detrimental effects are traded under the brand of well-known pharmaceutical companies. There are lots of methods thwarting counterfeiting which are more or less effective. An RFID-based approach means equipping drug packages with transponders and registering them in a database which enables customers to check the authenticity of the obtained product.

7.3.2 Supply Chain

After production and packaging the drugs are transported to a central warehouse where they are stored up to four month on average. On order by a wholesaler the shipment is commissioned and accompanied by transport documents. Sensitive drugs are carried in a cooling box for short distances and in a cold-storage carrier for long distances. The distributor buffers the products up to one month before they are forwarded to pharmacies and hospitals. Medicaments usually expire after three to five years [Döll06].

7.3.3 Discussion

The effects of temperature affected drugs are not that clear, considering that they are not determinable directly at the product without laboratory analysis. Therefore there does not exist any data on reclamations [Döll06]. The majority of products has to be stored between 8°C and 25°C and are therefore regarded as robust and not sensitive. In these cases the benefits of monitoring are not obvious.

A problem of introducing such a system emerges from the competitive situation. The supplier cannot exert control on its customer because it will change the supplier when, e.g. with respect to returned goods, it is told that it has not kept the contract concerning storage conditions. It is necessary that the responsibility for drug safety is moved towards the customer. A transponder recycling system over the pharmacies would be possible. The customer has to be made aware of drug safety and thus the last control of the temperature has to be performed by him/her when buying a sensitive medicament. Anyway, RFID-based temperature monitoring is a good instrument for the quality control of carriers [Döll06].

A problem within the supply chain is the immense ramification from big shipments to a single product at the customer [Döll06]. Solutions are cheaper transponders for item tagging or stepwise monitoring with copying and forwarding the data where the shipments are split up.

The introduction of continuous temperature monitoring of drugs would be easier and become necessary if enforced by laws.

7.4 Sensitive Documents

Ancient documents, e.g. parchments, require controlled storage and transport with monitoring of temperature and humidity. This is especially important when they are loaned for an exhibition. A transponder supporting the measurement of both, temperature and humidity, has to be employed.

7.4.1 Goals and Properties

RFID-based temperature and humidity monitoring concerning old documents has the following aims and advantages [Hofm06]:

- The climatic monitoring can be performed directly in the object, e.g. between the pages of a book.
- Objects can be permanently monitored while they are transported and on loan.
- It is of good use to check the keeping of the loan contract and to attribute responsibility in case of assurance issues.
- Objects can be prevented from damage and reduction in value.

For example, parchments have to be stored at a temperature between 18°C and 20°C and a relative humidity of 40% to 50%. The conditions should be constant without oscillations. Parchments are destroyed e.g. by embrittlement at low humidity and by microorganisms at high temperatures and high humidity. Temperatures below 16°C and over 22°C, and humidities below 30% and above 60% are considered as critical. Light irradiation poses a problem too. The degradation proceeds gradually and results in a reduction in value which cannot be improved by restauration. The value of parchments ranges from approx. 10000€ up to 1000000€; the *Österreichische Nationalbibliothek* (Austrian National Library) gives between 10 and 20 loans per year [Hofm06].

7.4.2 Humidity Sensing

Humidity means the amount of water vapour in gases [Frad04]. The relative humidity at ambient temperature T is defined as follows:

vapour pressure of the air P_w, maximum vapour pressure P_s

$$H(T) = \frac{P_w(T)}{P_s(T)} \tag{11}$$

Because of the dependency on the temperature, hygrometric sensors are only reasonable in combination with temperature sensor.

Sensor principles are based on the direct proportional change of the dielectric constant of an material to its moisture [Frad04]. Capacitive humidity sensors can be manufactured in thin-film technology, i.e. on chips, and consist of interdigitized electrodes coated with a dielectric layer. Their accuracy is typically ±2% in a range of 5% to 90% relative humidity. Another method is a hygristor, i.e. a humidity dependent resistor of nonmetal conductors, which can also be integrated using thin-film technology. The capacitor resp. resistor is included in a oscillation circuit and its change of capacitance and/or resistance which results in a frequency change is registered with the help of a counter.

7.4.3 Scenario

An application scenario is monitoring parchments on loan. When e.g. a museum requests an exhibit for its expositions, a loan contract is agreed on, where the climatic conditions for transport and the exhibition area are fixed. The loanibility of the object is checked and, if necessary and possible, measures are taken to establish it. The parchment is put into a passe-partout and a frame and is wrapped. The transponder can be put into the passe-partout or the frame. An art shipping agency is charged with the transport. At the exhibitor it is unwrapped and positioned in the exposition area. In case of valuable objects the conditions are controlled on the spot by the ÖNB. After the exhibition which normally lasts about three months the object is returned and a condition report is worked out in order to check whether the contract has been kept.

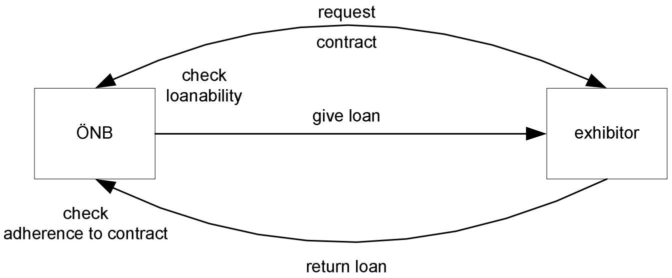


Fig. 70: Loaning procedure by the Österreichische Nationalbibliothek

7.4.4 Discussion

The monitoring of the transport conditions is especially important when the object is shipped per plane. At the moment there exists an object catalogue, but there are no computerized systems yet for the administration of the stock and the loans. An interesting application is storing a loan temperature and humidity history of an object, including where, when, the shipping company, etc. This would support fixing the duration the object is banned after an exposition and possibly defining extra-conditions if there has been a problem with an exhibitor in the past.

Barcodes are already in use for some object types, but they will eventually be introduced for all, although there are problems with the attachment, i.e. glues. This would be the same with transponders which must not contain substances which cause chemical reactions with the object.

The storage rooms are under climatic control, but however, monitoring directly on or in the object in storage rooms would have significant advantages because the conditions are often different in shelves, especially with respect to humidity. Battery lifetime might pose a problem because there is currently no annual inventory or control of the object conditions. Active transponders will have to be used because permanent storage condition monitoring aims rather at automatic alerting than tracing back problems.

Monitoring of sensitive documents does not exhibit direct economic benefits because the costs for restauration are negligible; the aim is rather preserving the value of the stock and ancient artworks.

Chapter 8

Conclusion

The feasibility of a system for RFID-based temperature monitoring of blood bags has been discussed. The supply chain has been analyzed and the technical and functional requirements on the transponder have been defined. There are still partly open issues concerning the physical reliability of the transponder as a whole which will have to be evaluated. A solution for integrating the transponder into the bag system which enables authentic measurement and transponder reuse at the same time has to be chosen in practice.

RFID-based temperature monitoring has many advantages as acquiring a continuous temperature history of each blood bag separately and closing the supply chain, thus enabling efficient reporting and tracing. Different approaches to RFID system architectures have been discussed, especially those which exploit the full functional range of RFID technology.

RFID-based temperature monitoring of blood bags is feasible from the technical perspective as soon as reliability problems of the transponders have been solved. The introduction of the system is a long-term process which is accelerated by legal pressure concerning traceability and quality.

RFID-based temperature monitoring of blood bags is a high-end application which boosts an innovative technology. By setting a proof-of-concept, it could path way for other sensor-related applications in ubiquitous computing.

References

[ABVO05] Verordnung über Arzneimittel aus menschlichem Blut. BGBl. II Nr. 187/2005, Vienna, 2005.

[AMBO04] Arzneimittelbetriebsordnung. BGBl. II Nr. 479/2004, Vienna, 2004.

[Aroc06] G. Arocker, and M. Ruth, personal correspondence, Ottakringer Brauerei AG, Vienna, Austria, May 2006, e-mail: gottfried.arocker@ottakringer.at, michael.ruth@ottakringer.at

[Arre03] D. Arregui, C. Fernström, F. Pacull, G. Rondeau and J. Willamowski. STITCH: Middleware for Ubiquitous Applications In *Proceedings of the Smart Objects Conference*, Grenoble, May 2003.

[Ashf02] P. Ashford. An Introduction to ISBT 128. ICCBBA 2002. Available from: `www.bloodct.org/ISBT/ICCBBA%20-%20An%20Introduction%20to%20ISBT128%202nd%20edition.pdf`

[BMSG02] Bundesministerium für soziale Sicherheit und Generationen, Abt. VIII/D/21. Mindeststandards für Blutdepots. Vienna, 2002. Available from: `www.bmgf.gv.at`

[BSG05] Blutsicherheitsgesetz. BGBl. I Nr. 44/1999 Änderung durch BGBl. I Nr. 63/2005, Vienna, 2005.

[BSI04] Bundesamt für Sicherheit in der Informationstechnik. Risiken und Chancen des Einsatzes von RFID-Systemen. Bonn, 2004.

[Cho05] N. Cho, S. Song, J. Lee, S. Kim, S. Kim and H. Yoo. A 8-µW, 0.3-mm² RF-Powered Transponder with Temperature Sensor for Wireless Environmental Monitoring. In *IEEE International Symposium on Circuits and Systems*, 2005.

[Dalt05] J. Dalton and S. Rossini. Using RFID Technologies to Reduce Blood Transfusion Errors. White Paper by Intel Corp., Autentica, Cisco Systems, and San Raffaele Hospital, Sept. 2005. Available from: www.cisco.com/global/IT/local_offices/case_history/rfid_in_blood_transfusions_final.pdf

[Döll06] H. Döller, personal correspondence, Merck Austria GmbH, Vienna, Mai 2006, e-mail: hannes_doeller@merck.at

[EC02] European Commission. 2002/98/EC Setting standards of quality and safety for the collection, testing, processing, storage and distribution of human blood and blood components. Brussels, 2002.

[EC05a] European Commission. 2005/61/EC: Traceability requirements and notification of serious adverse reactions and events. Brussels, 2005.

[EC05b] European Commission. 2005/62/EC: Certain technical requirements for blood and blood components. Brussels, 2005.

[Eede04] H. van Eeden. Europe Needs New RFID Regulations. *RFID Journal*, June 7th, 2004. Available from: www.rfidjournal.com/article/articleview/974/1/82

[EPC05] EPCglobal Inc. The EPCglobal Architecture Framework. Jul. 2005. Available from: www.epcglobalinc.org/standards_technology/Final-epcglobal-arch-20050701.pdf

[Fink03] K. Finkenzeller. *RFID Handbook: Radio-Frequency Identification Fundamentals and Applications.* John Wiley & Sons, Chichester, 2003.

[Flei05] E. Fleisch, and F. Mattern (Ed.). *Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis.* Springer, 2005.

[Floe04] C. Floerkemeier and M. Lampe. Issues with RFID Usage in Ubiquitous Computing Applications. *Pervasive Computing*, Lecture Notes in Computer Science, Vol. 3001, pages 188-193, 2004.

[Floe05] C. Floerkemeier and M. Lampe. RFID middleware design – addressing application requirements and RFID constraints. In *Proceedings of the joint conference on Smart objects and ambient intelligence: innovative context-aware services: usages and technologies*, Grenoble, pages 219-224, 2005.

[Frad04] J. Fraden. *Handbook of Modern Sensors – Physics, Designs and Applications.* 3rd Edition, Springer, New York, 2004.

[Gyge05] T. Gyger, H. Grossmann and D. Lanz. Sensoren – die Sinnesorgane technischer Systeme. *Bulletin SEV/VSE*, pages 23-29, Nov. 2005.

[Hamm06] G Hammer, personal correspondence, Wein & Co Handelsges.m.b.H., Vienna, Austria, Mai 2006, e-mail: gerhard.hammer@weinco.at

[Hess06] E. Hess. RFID Readers Meet Gen 2 Compliance. *Integrated Solutions*, May 2006. Available from: www.integratedsolutionsmag.com/Articles/2006_05/060505.html

[ICCB04] ICCBBA. ISBT 128. Technical Specification 2.1, 2004. Available from: www.iccbba.com/Technical%20Specification,%20Version%202.1.0.pdf

[Infi04] Infinite Power Solutions. LiTE*Star The Solid-State Thin-Film Rechargeable Battery. Available from: www.infinitepowersolutions.com/data-sheets/ battery_specifications.pdf

[ISO01a] International Organization for Standardization, International Electrotechnical Commission, "ISO/IEC 14443 Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards", Geneva, 2001.

[ISO01b] International Organization for Standardization, International Electrotechnical Commission, "ISO/IEC 15693 Identification Cards – Contactless Integrated Circuit(s) Cards – Vicinity Cards", Geneva, 2001.

[ISO04a] International Organization for Standardization, International Electrotechnical Commission, "ISO/IEC 15961 Information Technology – Radio Frequency Identification For Item Management – Data Protocol: Application Interface", Geneva, 2004.

[ISO04b] International Organization for Standardization, International Electrotechnical Commission, "ISO/IEC 15962 Information Technology – Radio Frequency Identification For Item Management – Data Protocol: Data Endoding Rules and Logical Memory Functions", Geneva, 2004.

[ISO04c] International Organization for Standardization, International Electrotechnical Commission, "ISO/IEC 18000 Information Technology – Radio Frequency Identification For Item Management", Geneva, 2004.

[Kope97] H. Kopetz. *Real-Time Systems, Design Principles for Distributed Embedded Applications*. Kluwer Academic Publishers, 1997.

[Kris05] P. Krishna, and D. Husak. Simple Lightweight RFID Reader Protocol. Internet Engineering Task Force, SLRRP Working Group, Aug. 2005. Available from: datatracker.ietf.org/public/idindex.cgi?command=id_detail&id=12560

[KSW06] KSW VarioSens Command Set 0.9. KSW Microtec AG, Dresden, 2006.

[Kurz05] M. Kurz. Klinische Anwendung von RFID bei Blutprodukten. Universitätsklinik für Blutgruppenserologie und Transfusionsmedizin, Allgemeines Krankenhaus Wien, 2005. Available from: www.isst.fraunhofer.de/deutsch/ download/17804_MKurz-RFID-bei-Blutprodukten.pdf

[Lee05] S. Lee, S. Joo and C. Lee, An Enhanced Dynamic Framed Slotted ALOHA Algorithm for RFID Tag Identification. In *The Second Annual International Conference on Mobile and Ubiquitous Systems (mobiquitous): Networking and Services*, pages 166-174, 2005.

[McFa03] D. McFarlane and Y. Sheffi. The Impact of Automatic Identification on Supply Chain Operations. *International Journal of Logistics Management*, Vol. 14, No. 1, 2003.

[Mich01] L. Michalski, K. Eckersdorf, J. Kucharski, and J. McGhee. *Temperature Measurement.* 2nd Edition, John Wiley & Sons, Chichester, 2001.

[Nova05] Novatech Research. *Liquid Control Unit*. Vienna, 2005. Available from: www.novatechresearch.com

[OBIG04] Österreichisches Bundesinstitut für Gesundheitswesen. Hämovigilanz Jahresbericht 2004. Vienna, 2004. Available from: www.oebig.at

[Ocke06] U. Ockenfuß, personal correspondence, Schweizer Elektronik AG, Schramberg, Germany, Mar. 2006, e-mail: ulrich.ockenfuss@seag.de

[OGBT00] Österreichische Gesellschaft für Biotechnologie und Direktorium Richtlinien in der Blutgruppenserologie und Transfusionsmedizin für das Blutspendewesen des Österreichischen Roten Kreuz. Vienna, July 2000. Available from: www.galp.at/de/dwnld/6402_ RiLiTeil4.pdf

[Opas06] K. Opasjumruskit, T. Thanthipwan, O. Sathusen, P. Sirinamarattana, P. Gadmanee, E. Pootarapan, N. Wongkomet, A. Thanachayanont, and M. Thamsirianunt. Self-Powered Wireless Temperature Sensors Exploit RFID Technology. *IEEE Pervasive Computing,* Vol. 5, No. 1, pages 54-61, Jan.-Mar. 2006.

[Parr03] A. Parr. Absatzmöglichkeiten für Software-Applikationen zur Administration von Blutprodukten sowie Einschätzung des erzielbaren Einsparungspotenzials. Österreichisches Bundesinstitut für Gesundheitswesen, Vienna, 2003.

[Pfla02] A. Pflaum. *Edition Logistik Band 3: Transpondertechnologie und Supply Chain Management, Elektronische Etiketten – Bessere I-dentifikationstechnologie in logistischen Systemen?* Deutscher Verkehrsverlag, Hamburg, 2002

[Phil05a] M. Philipose, J. Smith, B. Jiang, A. Mamishev, and K. Sundara-Rajan. Battery-Free Wireless Identification and Sensing. *IEEE Pervasive Computing*, Vol. 4, No. 1, pages 37-45, Jan.-Mar. 2005.

[Phil05b] T. Phillips, T. Karygiannis, and R. Huhn. Security Standards for the RFID Market. *IEEE Security and Privacy*, Vol. 3, No. 6, pages 85-89, Nov.-Dec. 2005.

[PICS04] Pharmaceutical Inspection Convention and Pharmaceutical Inspection Cooperation Scheme. GMP Guide For Blood Establishments. Geneva, 2004. Available from: www.picscheme.org/indexnoflash.php?p=guides

[Prab05] B. Prabhu, X. Su, H. Ramamurthy, C. Chu, and R. Gadh. WinRFID – A Middleware for the enablement of Radio Frequency Identfication (RFID) based Applications. University of California, Los Angeles, Wireless Internet for the Mobile Enterprise Consortium, 2005. Available from: www.wireless.ucla.edu/rfid/winrfid/

[Psch98] W. Pschyrembel, and O. Dornblüth. *Klinisches Wörterbuch*. H. Hildebrandt (Ed.), 258th edition, Walter de Gruyter, Berlin, New York, 1998.

[Rana05] D. Ranasinghe, K. Leong, M. Ng, D. Engels, and P. Cole. A Distributed Architecture for a Ubiquitous RFID Sensing Network. In *Proceedings of the 2005 Intelligent Sensors, Sensor Networks and Information Processing Conference, Melbourne, Australia,* pages 343-347, 5-8 Dec. 2005.

[Rede05] R. Redemske, R. Fletcher. The Design of UHF Tag Emulators with Applications to RFID testing and Data Transport. In *Proceedings of 4th IEEE Conference on Automatic Identification Technologies*, Oct. 2005.

[Roem04] K. Römer, T. Schoch, F. Mattern and T. Dübendorfer. Smart Identification Frameworks for Ubiquitous Computing Applications. *Wireless Networks* Vol. 10, No. 6, pages 689-700, Nov. 2004.

[Sarm03] S. Sarma, S. Weis and D. Engels. RFID Systems and Security and Privacy Implications. In *Proceedings of the International Conference on Security in Pervasive Computing*, Boppard, pages 454-469, Mar. 2003.

[Sche04] A. Scheck-McAlearney, S. Schweikhart and M. Medow. Doctors' experience with handheld computers in clinical practice: qualitative study. *British Medical Journal*, Vol. 328, May 15th 2004.

[Schl03] E.Schloegl, R. Reisner, H. Goldenits, G. Schwondra, and M. Bernhart. Blood Product Tracking using RFID-Labels: impact on product handling and haemovigilance data acquisition. *Blood Banking and Transfusion Medicine*, Suppl. 1, 2003, 1, 1, 280.

[Scho02] T. Schoch and M. Strassner. Wie smarte Dinge Prozesse unterstützen. *Ubiquitous Computing, HMD 229 - Praxis der Wirtschaftsinformatik*, pages 23-31, Feb. 2003.

[Schr05] V. Schröter, and C. Bothur. Transponder identifizieren Blutspende. *ident*, 10. Jahrgang, Nr. 5, pages 32-33, 2005

[Siem03] Siemens Automation and Drives. Moby D SLG D10 Technische Daten. Available from: `www.automation.siemens.com`

[SunM06] Sun Microsystems. Sun Java System RFID Software 3.0. Feb. 2006. Available from: `www.sun.com/software/products/rfid/`

[Tech02] TechnoPuce. Hémo-Tag, une avancée technologique pour la sécurité transfusionnelle. Available from: `www.technopuce.com`

[Vogt02] H. Vogt. Multiple Object Identification with Passive RFID Tags. In *Proceedings of the IEEE International Conference on Systems, Man and Cybernetic,* Volume 3, 6-9 Oct. 2002.

[Wagn06a] T. Wagner, and G. Lanzer. RFID in der Transfusionsmedizin. Speech held at the Smart Card Solutons Day 2006, Mar. 23th 2006. Available from: `www.siemens.at/scs-day/pages/downloads/1_RFIDinderTransfusionsmedizin.pdf`

[Wagn06b] T. Wagner, personal correspondence, Department of Transfusion Medicine and Blood Serology, Medical University of Graz, Austria, Mar. 2006, e-mail: thomas.wagner@meduni-graz.at.

[Walk04] E. Walk. Aktuelle Situation der RFID Standards für die Logistik. In *Ident Jahrbuch 2004*, pages 48-53, Rödermark, 2004.

[Want04] R. Want. Enabling Ubiquitous Sensing with RFID. *Computer*, Vol. 37, No. 4, pages 84-86, Apr. 2004.

[Weis04] S. Weis, S. Sarma, R. Rivest and D. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. *Security in Pervasive Computing*, Lecture Notes in Computer Science, Vol. 2802, pages 201-214, 2004.

[Will06] William Laboratories. Safe-T-Vue® Non-Reversible Temperature Indicator For Blood Safety. Available from: `www.williamlabs.com`

[Zimm05] J. Zimmermann. Blood Components Temperature Measurement. MacoPharma SA, Tourcoing, 2005.