



FAKULTÄT FÜR **INFORMATIK**

Requirement Evaluation and Prototype Implementation of an Electronic Triage Tag Framework

MASTER THESIS

For the obtainment of the academic degrees

Master of Science

Within the academic study

Medical Informatics

Submitted by

Edin Srdic

Matriculation number 0425106

At the
Faculty of Informatics of the Vienna University of Technology

Supervision:
Advisor: Thomas Grechenig
Assistance: Wolfgang Schramm

Vienna, 12th January 2011

(Signature author)

(Signature advisor)



MASTER THESIS

Requirement Evaluation and Prototype Implementation of an Electronic Triage Tag Framework

For the obtainment of the academic degree

Master of Science

Performed at

Institute of Computer Aided Automation

Research Group for Industrial Software (INSO)

Vienna University of Technology

Supervised by

Thomas Grechenig

under the guidance of

Wolfgang Schramm

By

Edin Srdic

0425106

Othmargasse 25/56, 1200 Wien

Affidavit

I hereby declare that I wrote this thesis on my own and without the use of any other than the cited sources and tools and all explanations that I copied directly or in their sense are marked as such, as well as that the thesis has not yet been handed in neither in this nor in equal form at any other official commission.

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Vienna, 12th January 2011

Edin Srdic

Acknowledgement

“Acquiring knowledge in company for an hour in the night is better than spending the whole night in prayer.” (Prophet Muhammad)

First of all I want to thank God for supporting and guiding me every day, for my wonderful family and all the material and nonmaterial blessings. Particularly I want to thank:

- My supervisor Univ.-Prof. Dipl.-Ing. Dr. techn. Thomas Grechenig for his helpful advice.
- My supervisors Dipl.-Ing. Christopher Dräger and Dipl.-Ing. Dr. Wolfgang Schramm for their patience with me and their constant assistance.
- My parents Hazim and Zevkija for their caring support during years of study and my whole life.
- Everyone who helped me to finish this diploma thesis especially my fiancée Aida, my friend Volkan, my sister Edina, my cousin Nermin.

Abstract

Many medical areas such as diagnose, treatment and patient care benefited from the application of IT-infrastructure ranging from complex architectures to small monitoring devices providing better access to information, more efficient data exchange and increased data processing. The goal of this thesis is to bring these benefits to the field of emergency care. Triage is a process during emergency care which aims at maximizing the provided care in a situation where the available resources are limited by diagnosing injuries and categorizing patients into groups to determine the priority for treatment and transport. Our intent is to increase the quality and amount of medical care for patients in such situations by introducing electronic Triage Tags to increase the efficiency of the entire triage process. Hence, this thesis evaluates the core requirements and deduces a framework for an electronic Triage Tag, utilizing RFID tags and a client/server approach based on wireless communication. Information gathering is performed by the mobile triage devices with integrated RFID reader. Finally, the thesis presents a simple proof of concept application.

Kurzfassung

Viele medizinische Bereiche wie Diagnose, Behandlung und Patientenpflege profitierten durch den Einsatz von IT-Infrastrukturen, die von komplexen Architekturen zu kleinen Überwachungsgeräten reichen, wodurch ein besserer Zugang zu Informationen, effizienterer Datenaustausch und erhöhte Datenverarbeitung gewährleistet werden können. Das Ziel dieser Arbeit ist es, diese Errungenschaften auch im Bereich der Notfallversorgung umzusetzen. Triage ist ein Prozess während der Notfallversorgung, bei der die vorhandenen Ressourcen begrenzt sind und rasch in oftmals unübersichtlichen Situationen optimale Hilfestellungen zu erbringen sind. Durch Triage soll diese Notfallversorgung deutlich effizienter gestaltet werden, indem Verletzungen diagnostiziert und die Patienten in Gruppen kategorisiert werden, um die Priorität für Behandlung und Transport zu bestimmen und klar darzustellen. Diese Arbeit evaluiert die Kernanforderungen und leitet daraus ein elektronisches Triage Tag System ab, das RFID Tags und einen Client/Server Ansatz basierend auf drahtloser Kommunikation verwendet. Informationen werden durch die mobilen Triage Geräte mit integriertem RFID Lesegerät erfasst. Abschließend wird eine Prototyp-Konzeptanwendung vorgestellt.

Contents

Contents.....	I
List of Figures.....	IV
List of Tables.....	VI
1 Introduction	7
1.1 Overview.....	7
1.2 Field of Application of Triage	10
1.2.1 Triage in Emergency Departments (ED)	10
1.2.2 Military (Battlefield) Triage.....	12
1.2.3 Triage in Disaster Situations	13
1.2.4 Categorization of Patients	14
1.2.5 The START System	15
1.3 Triage Workflow	17
1.4 Triage Tag	19
1.4.1 Examples of Triage Tags	19
1.5 Motivation for the Electronic Triage Tag	22
1.5.1 Limitations of the Conventional Triage Tag.....	22
1.5.2 Benefits of the Electronic Triage.....	23
1.6 Mobile Triage Device	25
2 Requirements of Medical Equipment	26
2.1 Definition of a Medical Device (Medical Equipment).....	26
2.2 General Requirements.....	26
2.3 Design of Medical Devices.....	30
2.3.1 Essential Requirements	30
2.3.2 Reliability of Medical Equipment.....	31
2.3.3 Balancing Usability and Complexity of Medical Equipment	32
3 Related Work	33
3.1 Related Projects	33
3.2 Related Studies	34
3.3 Open Source Software for RFID Emulation	37
3.3.1 Fosstrak Project	37
3.3.2 RifiDi Project.....	38
3.3.3 RadioActive	38
3.4 EPCglobal Network.....	38
4 Definition of the System Architecture	41
4.1 Workflow in the Electronic Triage System.....	41

4.2	Use Cases	44
4.3	Technical Requirements for the RFID Middleware	50
4.3.1	Information Consistency	51
4.3.2	Lost Update Problem.....	51
4.4	System Requirements.....	53
4.5	Technical Requirements of the RFID Tag and RFID Reader.....	54
4.5.1	Requirements of the RFID Tag	54
4.5.2	Requirements of the RFID Reader.....	56
4.6	Security Aspects	58
4.6.1	Aspects of RFID Security	58
4.6.2	Anonymity and Availability Requirements Conflict.....	61
4.6.3	RFID Security Mechanisms.....	62
4.6.4	Data Integrity Solutions	63
4.6.5	Data Security Solutions	67
4.6.6	Disposal of RFID Tags	73
4.7	System Architecture of RFID Triage	74
4.8	Near Field Communication (NFC) - Triage	76
4.8.1	Differences between NFC and RFID	77
4.8.2	NFC Applications.....	78
4.8.3	Modes of Operation.....	79
4.8.4	Communication Modes.....	82
4.8.5	The Contactless Communication API.....	83
4.8.6	Secure Element (SE).....	84
4.8.7	Impact on the Requirements of the Electronic Triage System.....	86
5	Implementation	89
5.1	Fosstrak Framework	89
5.2	Fosstrak Reader	89
5.2.1	Reader RP/RM Core	91
5.2.2	Reader RP Proxy	92
5.2.3	Reader RP Client	93
5.3	Implementation of the Triage Interface	94
5.3.1	Configuration.....	96
5.3.2	Implementation.....	100
5.3.3	Data Storage	103
5.3.4	Documentation	109
6	Discussion and Future Work.....	112
6.1	Open Issues.....	113
7	Summary.....	115
7.1	Introduction	115
7.2	Requirements of Medical Equipment	116

7.3	Requirements Analysis	116
7.4	Implementation	118
7.5	Discussion and Future Work.....	119
	References.....	120
	Appendix A.....	i

List of Figures

Figure 1-1: Hospital based triage organization [HoBu07].....	11
Figure 1-2: Prehospital disaster triage organization [HoBu07]	13
Figure 1-3: Operations of a Disaster-Medical-Aid Center	15
Figure 1-4: The Modified Simple Triage and Rapid Treatment System	16
Figure 1-5: Workflow in triage [InSo08].....	18
Figure 1-6: Smart Tag (by courtesy of [TsAs09])	20
Figure 1-7: METTAG (by courtesy of [MeMa09])	20
Figure 1-8: New Jersey Disaster Tag (by courtesy of [StOf09])	21
Figure 1-9: All Risk Triage Tag (by courtesy of [DiMa09])	21
Figure 3-1: Roles and interfaces in the EPC Network.....	39
Figure 4-1: Workflow in RFID Triage System [InSo08]	41
Figure 4-2: Sequence diagram visualizing emergency treatment.....	43
Figure 4-3: Rough overview of the use cases for an emergency person	44
Figure 4-4: Use case diagram of the RFID triage system.....	48
Figure 4-5: Information flow between emergency personnel and server	50
Figure 4-6: Lost update problem	52
Figure 4-7: Interference during transmission.....	63
Figure 4-8: Parity determination of a byte by multiple XOR operations	64
Figure 4-9: LRC checksum.....	65
Figure 4-10: CRC checksum.....	67
Figure 4-11: Mutual authentication procedure between transponder and reader	69
Figure 4-12: Authentication procedure based upon derived keys	70
Figure 4-13: Attempted attacks on a data transmission.....	71
Figure 4-14: Encrypting the transmitted	71
Figure 4-15: Stream cipher realized by one-time-pad	73
Figure 4-16: System and network architecture [InSo08].....	74
Figure 4-17: NFC Data transmission [FiK110]	76
Figure 4-18: NFC – Active Mode [FiK110].....	79
Figure 4-19: NFC – Passive Mode – Reader Emulation [FiK110]	80
Figure 4-20: NFC – Passive Mode – Card Emulation [FiK110]	81
Figure 4-21: NFC Communication Modes (by courtesy of [NeFe10])	82
Figure 4-22: Anatomy of Contactless Communication API (by courtesy of [EnOr10])	84
Figure 4-23: Card Emulation Activity Notifications (by courtesy of [EnOr10])	85
Figure 4-24: Typical Elements of a Java Card Application (by courtesy of [EnOr10])	85
Figure 5-1: Fosstrak Reader architecture.....	90
Figure 5-2: The Fosstrak HAL implementation	92
Figure 5-3: Reader RP Proxy.....	93
Figure 5-4: Reader RP Client and EventSink module	94
Figure 5-5: Triage Interface and the Fosstrak modules	95

Figure 5-6: Start the Fosstrak Reader	96
Figure 5-7: Start the Reader RP Client	96
Figure 5-8: Start the Triage Interface	96
Figure 5-9: Connect to the reader	97
Figure 5-10: Type-length-value format	104
Figure 5-11: Add a new tag to the reader	109
Figure 5-12: Move the tag over the antenna	109
Figure 5-13: Triage Interface	110
Figure 5-14: Injury editor of the Triage Interface.....	111

List of Tables

Table 1-1: Severity of injury	16
Table 4-1: Use cases of the RFID triage system.....	47
Table 4-2: Lost update	53
Table 5-1: Type definition for data storage on the RFID tag	108
Table 5-2: Type-length-value	108

1 Introduction

The application of IT embedded in medical care influences the future outlook of the medical sector in a positive way. Better access to information, more efficient data exchange, increased data processing capabilities allowing real-time and on-line diagnostics, simulation of results and stimulation of distributed decision-making processes are all results that are opening up new opportunities in the practice of medicine.

Many medical fields such as diagnose, treatment and patient care benefited from the application of IT-infrastructure. Better performing medical instrumentation, more efficient diagnostic systems, improved medical components and IT technology ranging from complex architectures to small monitoring devices are directly benefiting the medical sector. The goal of this thesis is to bring these benefits to the field of emergency care. The next chapter provides a short overview about this thesis.

1.1 Overview

Triage is a process during emergency care which aims at maximizing the provided care in a situation where the available resources are insufficient for medical treatment of all patients. One of the goals of triage is to diagnose critical injuries requiring lifesaving treatment in the shortest possible time. To this end patients are categorized into groups to determine their priority for treatment and transport to definitive care facilities.

The word “Triage” is derived from the French word “trier”, meaning to sort out. The French military were the first to use it in the Napoleonic Wars in the 18th century, when victims were classified and sorted according to the urgency of their conditions with the intention to determine the medical treatment priorities.

The purpose of the military was to provide care to the casualties, so that the soldiers could return as soon as possible to the front. Therefore combat Triage was directed by the adage: “the best for the most with the least by the fewest”. This meant that critical casualties requiring extensive resources received delayed medical care. Triage described the first-aid treatment of battle casualties in collection stations at the front before their evacuation to hospitals located behind the lines.

The major objective of military triage is to sort who can be returned to the front immediately, who needs treatment before returning to duty and who will not be able to return to active duty. This takes place in geographically dispersed areas by personnel with varying levels of expertise. The military experience has useful application for civilians working in disaster situations. Triage in disaster situations and emergency departments must be conducted with the purpose of doing the greatest good for the largest number of

people. While military and civil triage have the same goals they use different methods and processes. [HuJe03]

Triage is a procedure used by emergency personnel to distribute the limited medical resources to the injured people in a mass casualty situation. Thereby emergency personnel attach Triage Tags to the injured people. Triage tags are used to

- Classify the degree of the injury and determine the transport order of injured people to the hospitals
- Store and provide information about the casualty incident to publish to special facilities or to use for decision making like medical resource procurements.

Although the usage of triage tags and paperless digital system is growing, the current state of documentation of triage activities remains poor making research in the actual performance of triage difficult [VaGr03]. Up to now triage is operated manually with conventional paper triage tags, radiophones and check lists. This leads to failure (Chapter 1.5.1), inaccuracy and delay in information transmission when the state and the scale of the casualty incident should be published to involved facilities or used for decision making. Patient information must be collected manually and written down on the conventional Triage Tag. Information from the conventional tags can be stored electronically for statistical and analytical work resulting in a media break. This media break can lead to failures and wrong information caused by human errors like typing, read or operating errors.

The priority of emergency personnel is to treat the injured people efficiently because after a civilian disaster it may be appropriate to use the insufficient resources for those most likely to survive.

To aid the emergency personnel in the triage process and to avoid some of the drawbacks of conventional triage tags in this diploma thesis we propose a triage system using RFID tags (silicon chips with IDs, radio frequency functions and some additional logic and memory) which are attached to the conventional paper triage tags. RFID readers supply power to the RFID tags (passive) through radio frequency communication and read/write information from/on the tag. The RFID tags recommended in our diploma thesis are passive and have 1 kb of rewritable memory.

Emergency personnel use mobile devices equipped with an RFID reader. Mobile devices are used for the collection of patient information and identification of the injured person by the unique ID of each RFID tag. The RFID tag is embedded to the conventional paper triage tag.

The main differences which evolve by applying an electronic triage system using RFID tags compared to paper triage are:

- a) The information of the injured person can be stored on the RFID tag because of the rewritable memory of the RFID tags.
- b) Mobile devices combined with wireless communication allow collecting the needed information of injured people quickly via the network. Input method using mobile devices allow less error prone read/write features. Input rate is improved by automating the information of the emergency personnel and reducing the information which must be input in the early phase of triage to the injury level and the hospital.

This RFID triage system addresses important challenges for ubiquitous computing. These challenges are:

- Availability:
The emergency personnel must be able to input information about the patient anytime in the triage process, even when the network is not reachable.
- Confidentiality:
The electronic triage system must ensure that patient information is accessible only authorized emergency personnel providing information security.
- Low Latency:
The information about injured people must be quickly collected and viewed by the control center.
- Input Rate:
The time to input the patient information must be optimized to a minimum.
- Data Integrity:
The information of injured people should not be lost or changed after being acquired. In this context consistency and accuracy of the stored patient information must be provided by the system.

In this diploma thesis we outline a solution for these challenges by analyzing the workflow and optimizing the network usage by following approaches:

- Availability is assured by the storage of the information of the injured people on the RFID tag and using it as local buffer.
- Confidentiality is assured by the security measures applied to the electronic triage system on different layers.
- Latency is lowered by defining minimum wireless communication areas in the paths of the triage workflow.

- Input rate is improved by using mobile devices allowing easier input methods and automating information storage.
- Integrity is assured by mechanisms in the middleware being responsible that patient information is consistent, updated constantly and provided for the control center.

This chapter gave a short introduction about triage. In the following sections of chapter 1 the field of application of triage and the motivation of an electronic triage system are specified. In chapter 2 the requirements of medical equipment are described. Related work in chapter 3 presents similar projects to this diploma thesis and the open source software RFID emulation from the Fosstrak project used in our work. In chapter 4 the requirements of the RFID triage system and the electronic triage tag are defined. Chapter 5 documents the technical implementation of the Triage Interface for the mobile triage devices. Finally chapter 6 discussion and chapter 7 summary conclude this diploma thesis by defining open issues and further work.

1.2 Field of Application of Triage

Today triage is used to organize the medical care available during disasters and mass casualty situations, and in emergency departments and urgent care centers.

Triage in health care facilities, triage on the battlefield and triage at the disaster site differs in both requirements and functions from each other although sharing the same purpose.

1.2.1 Triage in Emergency Departments (ED)

Emergency Department (ED) use of triage systems began in the early 1960s, when the demand for emergency services outpaced available emergency resources. Emergency department space, equipment, and personnel were not adequate to handle the explosive increase in the number of emergency department visits. [IsMo07]

As the use of EDs increased and the waiting times became longer, the triage process evolved as a way of effectively separating patients requiring immediate medical attention from those who could wait. Figure 1-1 shows a generic layout for hospital-based triage (EMS, emergency medical service). [HoBu07]

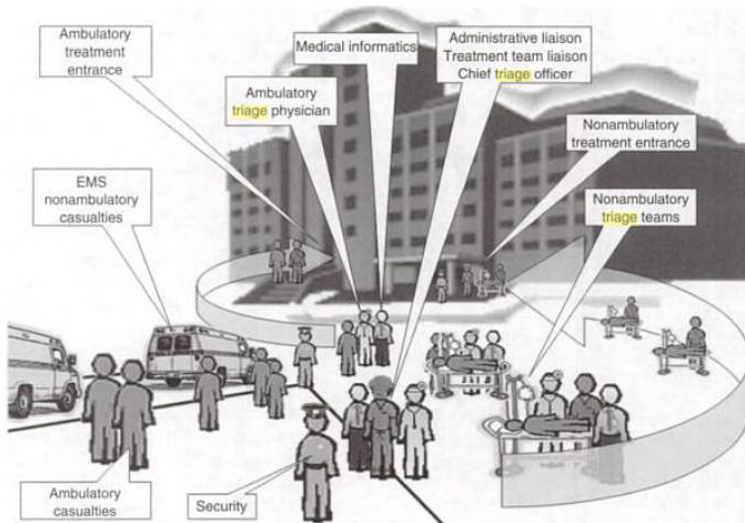


Figure 1-1: Hospital based triage organization [HoBu07]

The primary goals of an effective ED triage system are to:

- Quickly identify those patients with emergent, life-threatening conditions
- Regulate the flow of patients through the ED
- Provide direction to visitors and other health care professionals [VaGr03]

An efficient triage system increases the quality of patient care delivered, shortens the length of a patient's stay, and decreases patient waiting time by combining immediate assessment and interventions.

EDs in the United States generally use a 3-level system, although 5-level systems are gaining acceptance as they prove themselves to be more reliable. Countries, such as Canada, Spain, the United Kingdom, and Australia, have already adopted 5-level systems for ED use. The Emergency Severity Index ranges the patients into 5 groups from level 1 (most urgent) to level 5 (least urgent) on the basis of acuity and resource needs and uses the number of resources a patient needs. The Manchester Triage Scale, used widely in Great Britain, uses algorithms based on the patient's chief complaint to determine the triage level. The Canadian Triage and Acuity Scale (CTAS) uses an extensive list of clinical descriptors to place patients in one of 5 triage levels. Each level has an associated time required for physician assessment, with all level 1 patients needing to be treated immediately. These methods have good, but not excellent reliability, making it unclear whether these are incorrect systems, whether those using them are not up to the task, or whether nonmedical criteria are influencing some decisions. [IsMo07]

1.2.2 Military (Battlefield) Triage

Military physicians were the first to implement formal systems of triage to determine treatment priorities for wounded soldiers. Military triage has several distinctive features. The triage officers and treating professionals are typically members of a military service, and the patients are usually also military personnel. As military personnel, these health care professionals and patients may have obligations, allegiances, and expectations that are not shared by other health care professionals or by the general public. For example, military personnel typically give up certain rights and liberties and assume an obligation to obey their superior officers' orders. Military personnel may also be willing to accept life-threatening assignments according to, in part, the expectation that they will receive optimal medical care if they are injured in the line of duty. Furthermore, in addition to the internal medical objective to act in the patient's best interest, external objectives related to accomplishing a strategic or military mission may influence military triage systems. These systems may, for example, define which patients they may treat, such as combatants and civilians injured by their actions, and whom they may not, typically all other civilians. [IsMo07]

Triage decisions must often be modified when casualties are being transported from an "unsecure location". In a military setting, this may occur during the evacuation of casualties from a combat zone where the transport vehicle may represent a very attractive target for enemy attack. In paramilitary situations (e.g., postwar), civil unrest, looting and lawlessness can develop and patient transport vehicles may become targeted for theft, hijacking or destruction. When moving multiple patients from such an area, time can be critical for ensuring the safety of the vehicle and transport personnel.

In military firefight situations, medical care for the injured soldier begins at the scene with treatment administered by other soldiers trained in "combat lifesaving". Specialized medics are available to provide care for the North Atlantic Treaty Organization (NATO) combat units. Transport of battle casualties to the next level of care by personnel without medical training is referred as casualty evacuation (CASEEVAC). [WiGr07] An example of this is the transport of a patient by a combat helicopter returning from the battlefield. A medical evacuation (MEDEVAC) occurs when patients are transported in a medically configured helicopter, by trained medical personnel, with varying levels of resources at the associated medical treatment facilities (MTFs). [WiGr07]

There are five "levels of care" recognized by NATO for the management of battle casualties. [WiGr07] In the NATO system, the lowest level of support and treatment occurs at level I and the highest is level V. An increase in the level of care corresponds with expanded availability of resources in the NATO system. Surgical services are available at the different levels. These include are rudimentary medical treatment facili-

ties (MTFs), known as Battalion Aid Stations (BAS) or Shock and Trauma Platoons (STP), U.S. Army Forward Surgical Team (FST), the U.S. Air Force Mobile Field Surgical Team (MFST), U.S. Navy Casualty Receiving Treatment Ships (CRTS) and the U.S. Marine Corps Forward Resuscitative Surgical System (FRSS). [WiGr07]

1.2.3 Triage in Disaster Situations

The goal of triage in disaster situations is to quickly move from patient to patient and rapidly assess and classify the injured in terms of urgency and necessity of care. In addition triage may involve providing some basic life saving or stabilizing measures, but it is not meant to be the time at which definitive care is provided. Another difference between triage in a disaster situation and triage in a hospital setting is that the time to definitive care is unknown in a disaster situation.

A medical disaster creates demands that overwhelm the capacity of the local health care system; at least some demands cannot be satisfied. Therefore triage is used to determine who will receive treatment immediately or delayed and who will not receive treatment. Depending on the expected number of casualties and the severity of their injuries, the geographic area involved, and the expected arrival time of additional resources, criteria used for triage after natural or manmade disasters may vary. Hence, to come to the optimal disaster triage decisions, triage officers also need accurate information about the cause and extent of the disaster, as well as the location, capabilities, and functional status of nearby health care facilities. Moreover they need rapid patient assessment skills and knowledge of triage systems. Figure 1-2 shows the basic organization of prehospital triage (EMS, emergency medical service). [HoBu07]

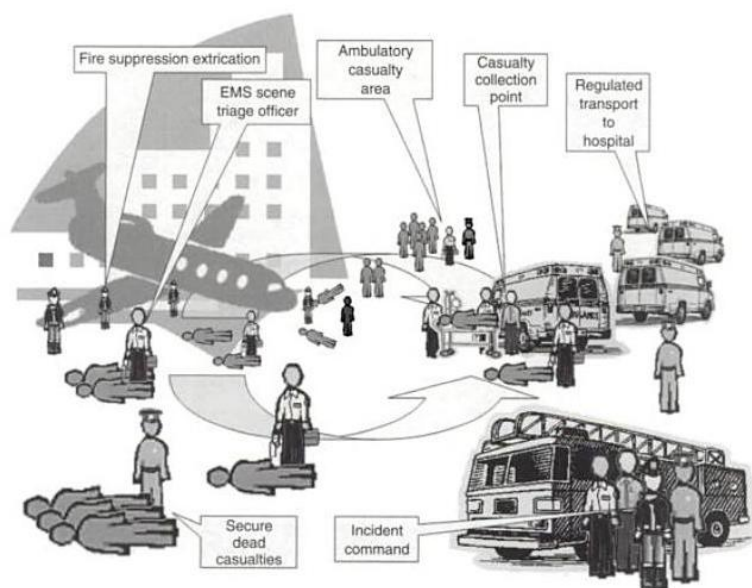


Figure 1-2: Prehospital disaster triage organization [HoBu07]

Triage in a disaster situation is only one part of an overall organizational approach that requires preplanning. Probably the most important goal of triage is to diagnose critical injuries requiring lifesaving treatment in the shortest possible time. For this purpose patients are categorized into groups to determine their priority for treatment and transport to definitive care facilities. A variety of formats have been used, most of them have three to five categories.

1.2.4 Categorization of Patients

The World Medical Association has recommended that clinicians categorize disaster victims with a general approach that has been adopted worldwide in some form and which involves the following triage criteria: [IsMo07]

- a) Priority 1 (“immediate”) – red triage tag
Those who can be saved but whose lives are in immediate danger, requiring treatment immediately or within a few hours
- b) Priority 2 (“delayed”) – yellow triage tag
Those whose lives are not in immediate danger but who need urgent but not immediate medical care
- c) Priority 3 (“minimal”) – green triage tag
Those requiring only minor treatment
- d) No Priority (“expectant”) – black triage tag
Those whose condition exceeds the available therapeutic resources, who have severe injuries such as irradiation or burns to such an extent, and degree that they cannot be saved in the specific circumstances of time and place, or complex surgical cases that oblige the physician to make a choice between them and other patients
- e) No specific triage tag
Those who are psychologically traumatized and might need reassurance or sedation if acutely disturbed (no specific triage tag)

Health care providers are coordinated into teams capable of delivering medical care immediately after a disaster situation. The goal of these teams is to stabilize the condition of patients in the field and then facilitate their transport to local hospitals or predestinated evacuation sites.

Dead or expected to die patients (black) and minimally injured victims (walking wounded, green) are identified. Those considered requiring immediate (red) or delayed

care (yellow) are further evaluated like outlined in Figure 1-3 [ScKo96]. Patients with at least a 50 percent probability of survival if treated receive care. All victims are periodically reevaluated. Once their condition has been stabilized, patients are evacuated to nearby hospitals or casualty-collection points.

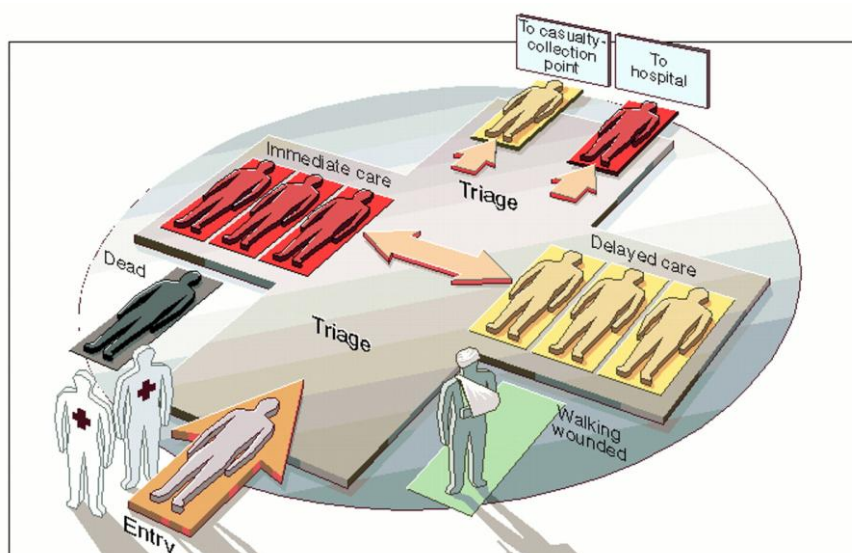


Figure 1-3: Operations of a Disaster-Medical-Aid Center

These activities which rely on making a rapid assessment (taking less than a minute) of every patient, determining which injury categories the patient should be in are standardized in different schemes. One of them is the START System.

1.2.5 The START System

Many experts agree that the START (simple triage and rapid treatment) system using the assessment of respirations, perfusion, and mental status is the best strategy [DeDr02]. This system supports the emergency personnel deciding which patients should be transported immediately, which can wait, and which patients are "unsalvageable".

Color coding schemes are generally used to identify the severity of injury and the category of treatment or evacuation into which the patient should be included. Although the use of color triage tags has been described, another practical option is to write the color code on the forehead of the patient with a marker for instance. It is important that all the participating people in patient care and evacuation understand and use the same color scheme.

Color	Priority	Description
Red	1	May survive if given immediate simple life saving measures
Yellow	2	Should survive if given care within a few hours
Green	3	Walking wounded: minor injuries that do not require rapid care
Black	4	Deceased or severely injured patients unlikely to survive

Table 1-1: Severity of injury

Injured patients are placed in one of the four color groups listed in Table 1-1 depending on the severity of their injuries [DeDr02].

Patients who can walk are identified first and receive first-aid measures only. Afterwards the triage nurse moves quickly to individual patients, assessing respiration, circulation status, and mental status according to the algorithm shown in Figure 1-4 [ScKo96]. Patients considered to need immediate care (red) are assessed and treated before those whose care can be delayed (yellow).

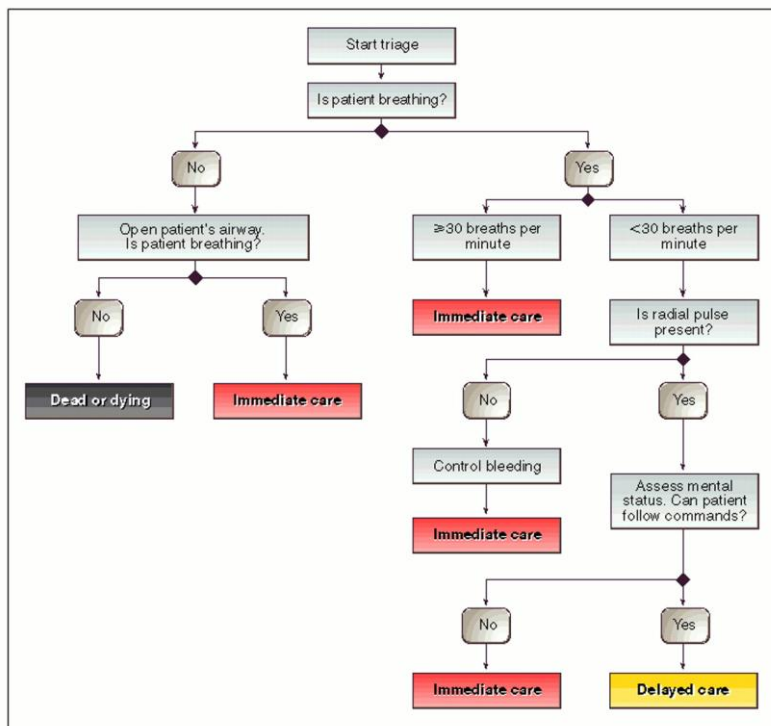


Figure 1-4: The Modified Simple Triage and Rapid Treatment System

1.3 Triage Workflow

In the following section the workflow of triage operated by emergency personnel will be described as well as the challenges for ubiquitous computing in the context of an electronic triage system. Triage is a practical application that requires urgent and continuous improvement since we are facing massive casualty incidents.

Current triage is done in the following sequence without using an electronic triage system by the emergency personnel (Figure 1-5). [InSo08]

- a) *Arrival*: Emergency personnel arriving first to the incident site establish a first-aid area, which is a safe place for first-aid near the incident area. Besides they establish a control center, which is the command center for the triage.
- b) *Primary triage*: Once the incident site is secured the emergency personnel enter the incident site and the primary triage by identifying the injury level in about 30 seconds. They attach the triage tags to the injured people representing the injury level.

During primary triage the emergency personnel try to write as much as possible from the following information to the tag:

- Time of input
 - Name and category (doctor, emergency medical technician) of the emergency personnel
 - Age of the injured person
 - Sex of the injured person
 - Injury level
- c) *Collection*: Injured people are moved to the first-aid area.
 - d) *Secondary triage*: In the first-aid area the injured people get a medical treatment. Besides that the secondary triage is performed by collecting following information if possible and writing the information down on the triage tag.
 - Name of the injured person
 - Phone number
 - Address
 - Updated information from the first triage

- e) *Hospital determination*: Before the patient leaves the first-aid area the target hospital must be determined. This information is written down on the triage tag and a carbon copy of the triage tag is left to the emergency personnel of the control center.
- f) *Transport*: When a transport vehicle arrives at the first-aid area the injured people are transported to the selected hospital. In the ambulances additional patient information is written on the triage tags.
- g) *Return to disaster site*: Emergency personnel being in the hospital and collecting information of the transported injured people. The transport vehicles return from the hospital to the incident site again and repeat the transportation of the injured people to the hospital. On returning the transport vehicle delivers the carbon copy of the triage tag from the hospital to the control center.
- h) *Update information at control center*: In the control center the information of the carbon copies of the triage tags are collected and reported to the search and rescue teams. This information is used, e.g., for decision making. [InSo08]

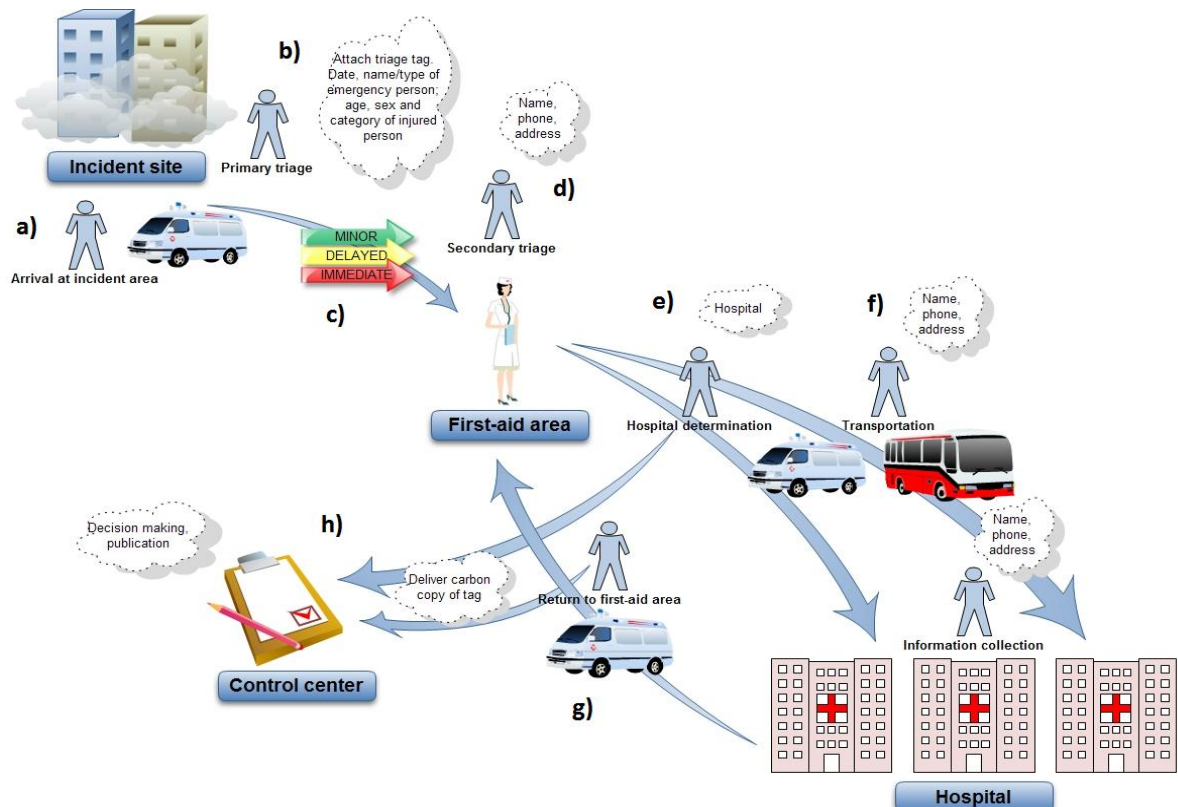


Figure 1-5: Workflow in triage [InSo08]

By using a wireless network combined with the RFID technology for the electronic triage media breaks can be avoided because input information can be collected through the

network, even if emergency personnel do not directly or indirectly give a triage tag to the person who is responsible for collecting the information. But, this stands on the assumption that information once acquired can be reached in a destination in the network for a long time. This assumption does not always hold in ubiquitous computing. Therefore data integrity and low latency in the semi-reachable network remains one of the challenges in ubiquitous computing.

The approach of this diploma thesis is the storage of patient information on the RFID tag to improve availability, while most of the RFID applications in the literature store only the ID on the RFID tag referencing patient information. However, the requirements in surroundings of insufficient network infrastructure are also discussed in mobile and ad hoc networks with a requirement for quick deployment.

1.4 Triage Tag

The identification of victims is an ever-present problem that occurs with multiple-patient incidents. After the victims are initially assessed, it is essential that they are identified as whether they require immediate care or whether they can wait for care. A variety of triage tags have been developed across the world to provide this identification. [HoBu07]

The triage tag should be easy to write on, weatherproof and it should be able to be secured directly to the victim, not to the clothing of the victim. Moreover it should store some information about the patient, at a minimum, name, age, gender, injuries, medical problems, field interventions, hospital destination, transportation agency, emergency medical service unit number, and of course the triage category. Space for some other information or checklists should be provided according to the requirements of the emergency care system of each individual facility, community or country.

Above all the triage tag must be easy to understand and easy to use while writing and reading patient information. Otherwise the tag will remain just a colorful decoration on the victim.

1.4.1 Examples of Triage Tags

Within the scope of the research of this diploma thesis we investigated the following 4 types of triage tags:

a) Smart Tag

The Smart Tag (Figure 1-6) has unique folded design which means that effective triage is quick and simple, but most importantly it allows casualties to be re-

triaged without having to replace the tag. It has been adopted as the standard triage tag for the states New York, Connecticut, Philadelphia, Boston and Nevada.



Figure 1-6: Smart Tag (by courtesy of [TsAs09])

b) METTAG (Medical Emergency Triage Tag)

The most common triage tag is the METTAG (Figure 1-7), which uses a combination of colors (black, red, yellow, green), priorities (0, I, II, III), and icons (cross/dagger, rabbit, turtle, ambulance crossed out) all on the same tag. The colors immediately identify the priority and urgency of the victim's situation. The dagger means the victim is dead; the rabbit means hospital care is urgently needed; the turtle indicates no urgency but hospital care needed; and the crossed-out ambulance means only first aid and no hospital care is needed.

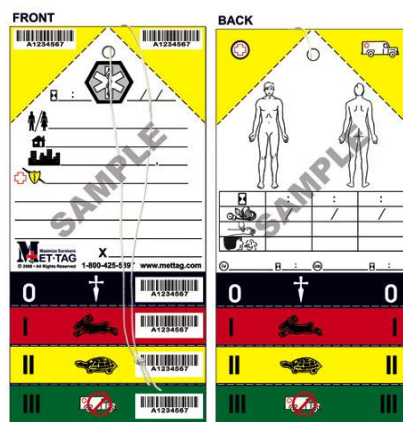


Figure 1-7: METTAG (by courtesy of [MeMa09])

c) New Jersey Disaster Triage Tag

The New Jersey Department of Health developed a new and unique triage tag to address the current and future needs of the disaster scene management. The New Jersey Disaster Triage Tag (Figure 1-8) is designed to make up for some of the shortcomings of the METTAG. It is two-sided, has basic three components (Tear Off Sections, Main Body, Peel-off Stickers) and includes the START scheme.

Personal Property / Evidence Tag
 Attach stub or seal inside personal property or evidence bag.
 Patient Destination and Transport Unit: Remove this stub after arrival of health care team and attach to patient care report.

PEEL AND STICK TO PATIENT CHART

STATE OF NEW JERSEY

PERSONAL PROPERTY / EVIDENCE TAG

REPERATIONS
 R: Yes No P: Pulse 2 Sec M: Mental Status Can't Do

Move ANYONE ambulatory **MINOR**
 No Respiration after head tilt **DECEASED**
 Respiration 0-30 **IMMEDIATE**
 No radial pulse or Capillary refill over 2 Seconds **IMMEDIATE**
 Unable to follow simple commands **IMMEDIATE**
 Everyone else **DELAYED**

HAZARD AUTO INJECTOR 1 2 3 4 5 6 7 8 9 10

VITALS
 Time: B/P: Pulse: Resp: O₂ Sat:

Medications
 Time Medication Dose Route

IV Location On Solution Rate Always Adjunct

DECEASED
IMMEDIATE LIFE THREATENING INJURIES
DELAYED NON-LIFE THREATENING INJURIES
MINOR MINOR INJURIES
UNINJURED DOCUMENTED BY PERSONNEL

STATE OF NEW JERSEY

PERSONAL PROPERTY / EVIDENCE TAG

State of New Jersey
 DISASTER TRIAGE TAG

PERSONAL PROPERTY / EVIDENCE TAG

REPERATIONS
 R: Yes No P: Pulse 2 Sec M: Mental Status Can't Do

Move ANYONE ambulatory **MINOR**
 No Respiration after head tilt **DECEASED**
 Respiration 0-30 **IMMEDIATE**
 No radial pulse or Capillary refill over 2 Seconds **IMMEDIATE**
 Unable to follow simple commands **IMMEDIATE**
 Everyone else **DELAYED**

HAZARD AUTO INJECTOR 1 2 3 4 5 6 7 8 9 10

VITALS
 Time: B/P: Pulse: Resp: O₂ Sat:

Medications
 Time Medication Dose Route

IV Location On Solution Rate Always Adjunct

DECEASED
IMMEDIATE LIFE THREATENING INJURIES
DELAYED NON-LIFE THREATENING INJURIES
MINOR MINOR INJURIES
UNINJURED DOCUMENTED BY PERSONNEL

VICTIM DEMOGRAPHICS
 Sex: Male Female Unavailable
 Age: DOB: Minor Unavailable
 Name:
 Address:
 City: St: Zip:
 Phone:
 SSN:
 Religion:
 Tribe: Other:
 Tent: Other:
 Tans: Other:

Figure 1-8: New Jersey Disaster Tag (by courtesy of [StOf09])

d) All Risk Triage Tag

The All Risk Triage Tag (Figure 1-9) is manufactured by Disaster Management Systems (DMS) is the standard tag of several states including Florida and California. It has adapted START triage, mass decontamination procedures, patient care criteria and evidence tagging into a simple and effective tool. The information stored on the All Risk Triage Tag is the basic information for the implementation of the prototype of this diploma thesis.

CONTAMINATED

Personal Property Receipt / Evidence Tag
 Evidence Tag: R1234567
 Destination:
 Via:

ALL RISK TRIAGE TAG
S L U D G E M
 AUTO INJECTOR TYPE: 1 2 3
 AUTO INJECTOR TYPE: 1 2 3

REPERATIONS
 R: Yes No P: Pulse 2 Sec M: Mental Status Can't Do

Move the Wailing Wounded **MINOR**
 No Respiration after Head Tilt **MORGUE**
 Respiration - Over 30 **IMMEDIATE**
 Perfusion - Capillary Refill Over 2 Seconds **IMMEDIATE**
 Mental Status - Unable to Follow Simple Commands **IMMEDIATE**
 Otherwise **DELAYED**

VITAL SIGNS
 Time: B/P: Pulse: Respiration:
 Time: Drug Solution: Dose:

PERSONAL INFORMATION
 Name:
 Address:
 City: St: Zip:
 Phone:
 Comments:

CONTAMINATED

EVIDENCE

MORGUE **MORGUE**
 Patients: **Non-Breathing**
IMMEDIATE **IMMEDIATE**
 Life Threatening Injury Life Threatening Injury
DELAYED **DELAYED**
 Non Life Threatening Injury Non Life Threatening Injury
MINOR **MINOR**
 Wailing Wounded Wailing Wounded

Figure 1-9: All Risk Triage Tag (by courtesy of [DiMa09])

1.5 Motivation for the Electronic Triage Tag

The current state of documentation of triage activities remains poor, while the usage of triage tags and paperless digital system is growing.[VaGr03] This makes the research in the actual performance of triage difficult because only the documented results of triage decisions can be evaluated with correctness. Research on electronic triage is marginal, while most studies in this field cover the triage in EDs and not the triage in disaster situations.

This diploma thesis compares our proposed electronic triage tag to the conventional triage tag and outlines that the electronic triage tag can be adopted more efficiently. All required information is prepared and stored electronically. Thus the information can be forwarded to a central unit (e.g., a mobile control center). A chip (rather a transponder) upgrades the conventional triage tag. Data is read and written by a read/write device which is connected to the central unit via a wireless connection.

The electronic triage tag is not a static and disconnected information repository. Real-time information about patients and their status is critical to the overall management of field medical care by the command center. Because of the known and limited availability of resources (such as on-scene providers, ambulance locations, and area hospital capacities) medical command must coordinate timely information on the number of casualties and their needs. Moreover real-time information is critical to determine the appropriate patient destination, depending on the type of injuries and the capabilities of the receiving facilities.

The sequential interdependence described above highlights the importance of information transfer in a disaster scenario. Actions in the field, such as triage, transport and treatment of victims, finally impact hospital resources and capabilities. On the other side real-time information on hospital and health care resources has an important impact on disaster response management and field care of victims. Still this information is mostly not available and is hampered by the lack of a global communication and information system at the disaster scene.

1.5.1 Limitations of the Conventional Triage Tag

Most medical facilities use conventional paper triage tags. Some of them use bar codes to provide a unique identification for the patients' information; nevertheless the conventional tags have many limitations.

- The space for recording medical data or additional information about the patient is limited (e.g., if the emergency person writes down long comments about the patient the space on the conventional triage tag might be insufficient)

-
- The “tear off” format of tags only allows unidirectional changes in victim condition (change for the worse)
 - The tags can be corrupted, destroyed or lost which means that patient information is lost partially or entirely
 - The tags might contain unreadable handwriting resulting from the stress situation for the emergency personnel
 - The manual count of the injured people (e.g., deceased) is prone to human error
 - Media breaks caused by the manual transmission of patient information from the conventional tag to electronic documentation is a source of error
 - The tags do not discriminate between victims categorized under the same color
 - The tags inefficiently monitor and locate victims
 - The tags are static and disconnected information storages without any real-time information about the victim

1.5.2 Benefits of the Electronic Triage

The complex work processes and communication patterns exhibited in emergency medicine may be effectively managed through the use of information technology. These tools must be evaluated within the work environment to understand their effects on work flow, information flow, and patient safety. The usage of electronic and conventional triage systems is growing, but the research in this field is not adequate.

The results of studies and researches like [LeFr06], [DoBu07] and [B1Bu05] show that electronic triage has positive effects. Efficient work and communication processes are essential for the management of time-critical activities in the ED and in a disaster situation. Information technologies are being developed and integrated into the triage workflow to meet these demands; however, few studies have quantified their impact on work processes and clinical outcomes.

Study of the impact of effects of computerized triage on nurse work behavior outlines that triage times did not change significantly after the CTA (computerized triage application) was introduced. Patient chief complaint, age, acuity score and nurse experience did not impact triage times. After CTA implementation the number of tasks each triage nurse performed and the average duration of interruptions decreased significantly. [LeFr06]

Study of comparing a novel computer triage program with standard triage tries to determine the agreement between a computer decision tool and memory-based triage. There was significant discrepancy by emergency personnel using memory-based triage when compared with a computer tool. The results of the study show a considerable down-triaging of patients without using the computerized tool. Triage decision support

tools can mitigate this drift, which has administrative implications for the triage workflow. [BlBu05].

The electronic triage system is designed to assist those performing triage by displaying the modifiers for each complaint that define the criteria for each triage level. These systems are not intended to replace clinical judgment and should not be permitted to promote total dependence. The goal is to develop trustworthy systems that permit and even encourage overrides when indicated by clinical judgment. Moreover, these clinical overrides can be used to adjust the source reference used to develop the system. The principles of iterative feedback, clinical efficiency, end-user sensibility and implementer flexibility have ensured success of such computer information systems. [DoBu07]

The main advantages of an electronic triage system compared to a conventional triage system are:

- Mobile triage devices (Chapter 1.6) combined with wireless communication allow collecting the needed information of injured people via the network by sending the information to a central server.
- Input method using mobile triage devices allow less error prone read/write features compared to handwriting
- Input rate is improved by automating the information of the emergency personnel and hospital addresses
- Real-time access to the patient information which is critical to the overall management of field medical care is provided by the wireless data transmission and the storage of the information on a central unit

The main disadvantages are:

- There is a strong dependence on the IT infrastructure. Wireless network might not be available or can crash anytime and mobile triage devices are at risk to become defective by hardware errors.
- The acceptance of the electronic triage system by emergency personnel cannot be assured. Gathering patient information might be less intuitive or slower than with the conventional triage tags. These uncertainties about the acceptance and prosperity of the electronic triage system can be reduced through the results of studies or field trials.

1.6 Mobile Triage Device

The mobile triage device is a handheld scanner carried by emergency personnel and used for information collection. It allows textual data input combined with a touch screen. This provides suitable usage by the emergency personnel.

The mobile triage device is equipped with an RFID reader and a wireless communication interface. Its graphical interface allows the emergency personnel to input information of the injured person.

After that the information is saved to the RFID tag and sent to the server through the wireless network. If the wireless connection is disconnected, the information is stored on the mobile triage device and will be sent to the server when the wireless connection is established. There is information which will be automatically inserted by the mobile triage device like the date/time or name/category of the emergency personnel.

Emergency personnel use the mobile triage device designed for the usage in the first three phases;

- primary triage
- secondary triage
- hospital determination

2 Requirements of Medical Equipment

The electronic triage system architecture consists of different components necessary for the collection of patient information. The mobile triage device with an integrated RFID reader is used by the emergency personnel in the early stages of triage. It has a significant role in the information collection process of the electronic triage and as such has to be regarded as a medical device. Thus we must define general requirements as basic principles for a medical device. For this reason we have to define what a medical device is.

2.1 Definition of a Medical Device (Medical Equipment)

Various medical device directives define a medical device as follows:

“any instrument, appliance, apparatus, material or other article, whether used alone or in combination, including the software necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of:

- Diagnosis, prevention, monitoring, treatment or alleviation of disease
- Diagnosis, monitoring, alleviation of or compensation for an injury or handicap
- Investigation, replacement or modification of the anatomy or of a physiological process
- Control of conception

And which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means.” [RiFr06]

The mobile triage device meets the demands for monitoring an injury and controlling the conception; hence we can define the general requirements for a medical device in the next section.

2.2 General Requirements

All medical devices carry a certain degree of risk and could cause problems in specific circumstances. Many of these problems cannot be detected until extensive market experience is gained. Component failure of the mobile triage device can be unpredictable or random. The current approach of device safety is to estimate the potential of a device becoming a hazard that could result in safety problems or harm. This estimate is identified as risk management.

- Risk Management Process
- Essential Performance
- Expected service life

- Equivalent safety for medical equipment or medical systems
- Medical equipment parts that encounter the patient
- Normal condition and single fault condition for medical equipment
- Components of medical equipment

a) Risk Management Process

The risk management process consists of a series of steps that, when undertaken in sequence, enable continual improvement in decision-making concerning the basic safety of medical devices. It is activity directed towards the evaluation, alleviation and monitoring of risks.

Hazard is a potential for an adverse event, a source of danger. Risk is a measure of the combination of:

- The hazard
- The likelihood of the occurrence of the adverse event
- The severity of overall impact [MiCh03]

Risks are due to accidents, natural causes and disasters as well as intentional attacks from someone. There are different possibilities how to manage the actual situation like:

- Transferring the risk to another party
- Avoiding the risk
- Reducing the negative effect of the risk
- Accepting some or all of the consequences of a particular risk

The manufacturer of the medical equipment or the medical system should make judgments relating to basic safety and essential performance of the medical equipment, including the acceptability of risks, taking into account the generally accepted state of the art, in order to determine the likely suitability of medical equipment to be placed on the market for its intended use. ISO 14971 [InOr09] specifies a procedure for the manufacturer to identify hazards associated with a medical device and its accessories; to estimate and evaluate the risks associated with those hazards; to control those risks, and to monitor the effectiveness of that control.

The manufacturer should assess risks resulting from the fact that individual system components have been integrated into one electronic triage system. This assessment includes all aspects of the information exchanged between the system

components. The potential risk related to the integration of these components (electrical or non-electrical) into the medical system, need to be considered. The risk management process results in a set of records and other documents like the risk management file. Compliance of the risk management process is checked through inspection of the risk management file.

The risk management process complying with ISO 14971 should be performed before the creating prototype of the medical device to prevent safety problems or harm. Compliance is checked by inspection of the risk management file. The requirements of a national standard referring to inspection of the risk management file are considered to be satisfied if the manufacturer has: [OeOe04]

- Established a risk management file
- Established acceptable levels of risk
- Demonstrated that the residual risks are acceptable

b) Essential Performance

An essential performance problem exists when the feature or function is either absent or its characteristics are degraded to a point that the medical equipment or the whole system is no longer usable for its intended purpose.

With regard to which features and functions of a piece of medical equipment or the whole system might be essential performance, it is easiest to begin by thinking of the medical equipment or the whole system as a “black box”. To achieve its intended purpose, the “black box” must provide specified features and functions that, if they were absent, the patient, operator and others would be exposed to harm.

c) Expected service life

The expected service life of medical equipment or a medical system is determined by the responsible organization manufacturing the medical device. Usually it should not be any longer than the expected service life which was defined by the manufacturer (e.g., in terms of years of service or number of uses), but it can be longer in particular instances.

The manufacturer has to determine the expected service life as a part of the risk management process. This information is part of the risk management file.

d) Equivalent safety for medical equipment or medical systems

These requirements address particular risks but alternative means of addressing these risks are acceptable if the manufacturer can justify that the residual risks after applying the alternative means are equal to or less than the residual risks after applying the requirement of a national standard that addresses the particular risks.

e) Medical equipment parts that encounter the patient

There are two different types of equipment parts; applied parts and parts that are simply considered as the enclosure. Parts that encounter the patients can present greater hazards (e.g., electrification or burn) than other parts of the enclosure. Therefore the applied parts are subject to more strict requirements (e.g., for temperature limits and for leakage current).

A part that unintentionally comes into contact with an unconscious, anaesthetized or incapacitated patient can present the same risks as an applied part the necessarily has to contact the patient. Besides that, a part that an active patient could reach out and touch can present the same risk to the operator like it presents to the patient.

The risk management process includes an assessment of whether parts (falling outside of the definition of applied parts) that may possibly come into contact with the patient shall be subject to the requirements for applied parts.

f) Normal condition and single fault condition for medical equipment

Single fault safe is a characteristic of medical equipment that assures freedom from unacceptable risk during its expected service life.

The requirement that medical equipment is “single fault safe” effectively puts a lower limit on the probability of occurrence of harm from a hazard. If this probability is achieved then the risk of the hazard is acceptable. In all cases where this discussion refers to the severity of probability of a hazard, it is intended to refer to the probability or severity of the harm resulting from that hazard.

g) Components of medical equipment

All components which could cause a hazard shall be used in conformity with their specified ratings unless a specific exception is made in the risk management process or a national standard. The reliability of components that are used

as means of protection shall be assessed for the conditions of use in the medical equipment. They should confirm to one of the following points:

- The applicable safety requirements of the relevant IEC/ISO standard (ISO 14971). [InOr09]
- Where there is no relevant IEC/ISO standard, the requirements of a national standard have to be applied. [OeOe04]

2.3 Design of Medical Devices

In the European Union there are directives and laws like the Medical Devices Act which is based on the fundamental requirement that medical devices may only be allowed freedom of movement within the European Economic Area if they conform to the essential requirements (Directive 93/42/EEC). [EuUn09]

2.3.1 Essential Requirements

The essential requirements are a set of criteria which a medical device must fulfill if it is to be freely traded on the European Union internal market. The essential requirements of a medical device are:

- The safety
- The technical performance
- The medical performance

The conformity assessment procedure (Directive 93/42/EEC) is used to provide evidence that concerning safety and technical performance are satisfied, while the medical performance is approved by the clinical assessment.

The essential safety requirements include (among others):

- A general requirement for safe design
- The minimization of risks from contamination
- Compatibility with materials with which they are likely to come into contact
- The minimization of hazards of infection and microbial contamination
- Provision of sufficient accuracy (for devices with a measuring function)
- Protection against radiation
- Adequate product marking
- Adequate user instructions

Besides that there are administrative requirements for the manufacturer which say that the manufacturers must typically:

- Comply with the essential requirements
- Demonstrate design verification
- Carry out a risk assessment
- Demonstrate clinical evidence of the effectiveness of the device
- Implement a procedure for post market surveillance
- Complete a Declaration of Conformity
- Maintain a file of technical information about the product

2.3.2 Reliability of Medical Equipment

Main factors that decrease the operational reliability of the electronic triage system must be concerned during design in order to control and maximize system reliability. Hence, early failures can be eliminated by a systematic process of controlled screening and burn-in of the components, assemblies and the device. Wearout failures can be eliminated by undertaking timely preventive maintenance on the device, with adequate replacement of affected components. Stress-related failures can be reduced by providing adequate design margins for each component and the device. [RiFr06]

Reliability assurance provides the theoretical and practical tools which help you to evaluate the functionality of a component or device with a certain confidence:

- Establishing reliability in design by use of failure-free or failure-tolerant principles
- Verifying reliability by well-designed test procedures
- Producing reliability by proper manufacturing processes
- Assuring reliability by good-quality control and inspection
- Maintaining reliability by proper packaging and shipping practices
- Assuring operation reliability by proper field service and appropriate operations and maintenance manuals
- Improving reliability throughout the life of the device by information feedback on field problems and a system to address these issues [RiFr06]

These requirements can be consulted for the definition of a structured approach to the life cycle of a medical device.

The effect of a reliability program on medical devices provides a structured approach to the product development process. The techniques improve the quality of the device over a period of time and reduce development time and cost. They assure regulatory requirements are achieved and give confidence that regulatory inspections will produce no deviations. Using different reliability techniques decreases warranty costs and increases customer acceptance [RiFr06]. These techniques also reduce the risk of liability by assuring that safety was the main concern during the design and development process.

2.3.3 Balancing Usability and Complexity of Medical Equipment

The market pressure brings the manufacturer to add extra features to a medical device, while they disregard the user-interface designer's rule: 20 percent of a device's functions will be used 80 percent of the time. [MiWi95]

In the cases of advanced electronic and computer-based medical devices there is a proliferation of features, because adding extra features is relatively inexpensive, requiring only a few more lines of software code rather than additional hardware components in condition that hardware infrastructure supports the feature. Many nurses using advanced electronic and computer-based medical devices say that they have too many features. [MiWi95] Nevertheless most of them want the manufacturer to provide most of the optional features. [MiWi95]

Hence we arrive at the conclusion that there is a big priority and a key role in user-interface design. The ease of learning is the key attribute of usability attributes, but a device that is initially easy to learn to use may not be the easiest to use in the long run.

3 Related Work

This chapter provides an overview of thematically relevant work for the electronic triage system. Related studies are mentioned to provide an overview of the existing literature of the research which is remaining poor in the field of electronic triage. Some mentioned projects are implementing the electronic triage tag with a similar technology and presenting the advantages and disadvantages of this solution.

The practical part of this diploma thesis is the implementation of a prototype interface for the mobile triage device. We investigated some open source RFID simulation software for this implementation of the simulator.

3.1 *Related Projects*

The article [FrLe05] describes an integrated software–hardware system (MASCAL) designed to enhance management of resources at a hospital during a mass casualty situation. MASCAL uses active 802.11b asset tags to track patients, equipment and staff during the response to a disaster. The system integrates tag position information with data from personnel databases, medical information systems, registration applications and the US Navy’s TACMEDCS triage application in a custom visual disaster management environment [FrLe05].

The main difference between the MASCAL project and my diploma is that MASCAL seeks to facilitate the resource allocation decisions, avoid patient flow bottlenecks and maximize system capacity and throughput at military and civilian hospitals, and the electronic triage system of my diploma thesis work is applied at the disaster area. Nevertheless the fundamental architecture of the MASCAL project will be relevant for my diploma thesis. Besides that the MASCAL project uses passive RFID tags for the storage of patient information.

Most localities and facilities applying the triage system use conventional paper triage tags. Some of these tags have bar codes to provide a unique identification for an injured person. The article [LePa05] ascertains the limitations of the conventional tag and describes the design and development of an electronic triage tag. The “tear off” format of tags only allows unidirectional changes in patient condition (worsening). The tags are not weather resistant, and are hence easily marred or destroyed [LePa05]. The focus of the article [LePa05] is on the design of an Intelligent Triage Tag (ITT) developed as part of the Wireless Internet Information System for Medical Response in Disasters project (WIISARD) using 802.11 (WiFi) wireless-based technologies to coordinate and enhance care of mass casualties.

The Advanced Health and Disaster Aid Network (AID-N) project designs a hardware and software architecture of the electronic triage system. The decentralized electronic triage and sensing system uses low power, electronic triage sensors to monitor the vital signs of patients and provide location tracking capabilities [MaGa06]. This article identifies the limitations of the conventional paper triage tag. Paper tags inefficiently monitor and locate patients, have limited visual feedback and do not aid in locating a particular patient in a sea of patients with the same triage color tags. When a commander needs to tally the number of patients triaged under a certain color, the manual count is prone to human error. Finally, paper tags do not distinguish between patients categorized under the same color. Two patients categorized as critical (red) have the same priority, even if one patient's vital signs designate him to be much worse than the other [MaGa06].

The conventional tag is static and disconnected information repository. Real-time information about the injured persons and their status is significant for the management of the field work. Medical command must coordinate timely information on the number of casualties and their needs with the known availability of resources, such as on-scene providers, ambulance locations, and area hospital capacities. Real-time information is also critical to determining the appropriate patient destination, depending on the type of injuries and the capabilities of the receiving facilities [LePa05].

3.2 Related Studies

Many countries [ElMe07] recognized the need for an efficient triage system and different algorithms have been developed around the world like in Canada (CTAS, Canadian Triage Assessment Scale) [ThDo00], Australia (Australasian Triage Scale) [CoLe04], the United Kingdom (Manchester Triage Scale) [VeSt08], Europe (ESI, Emergency Severity Index) [ElMe07]. The research in the field of electronic triage systems is poor; nevertheless there are studies relevant for this diploma thesis.

The purpose of study "The Australasian Triage Scale: Examining Emergency Department Nurses' Performance Using Computer and Paper Scenarios" [CoLe04] is to examine emergency nurses' performance using triage scenarios characterized by type of patient population (adult versus pediatric) and mode of delivery (paper versus computer). A combination of paper-based (script alone) and computer-based (script plus still photographs) triage scenarios were used. Of the 28 scenarios used, half were written and half were computer based. Within each subgroup, there were 7 adult and 7 pediatric scenarios. Participants were asked to allocate an Australasian Triage Scale category for each triage scenario. One hundred sixty-seven participants completed a total of 2,349 adult scenarios, and 161 participants completed 2,265 pediatric scenarios. Sixty-one percent of the triage decisions made by the nurses were "expected" triage decisions, 18% were "undertriage" decisions, and 21% were "overtriage" decisions. Nurse triage allocation decisions for the scenarios containing still photographs delivered by comput-

er demonstrated a higher average agreement percentage of 66.2% compared with the average agreement percentage of 55.4% using paper-based (text-only) scenarios. [CoLe04] The mode of delivery appeared to have an effect on the nurses' triage performance. It is unclear whether the use of simple still photographs used in the computer mode of delivery resulted in a higher incidence of expected triage decisions and, thus, improved performance. The use of cues such as photographs and video footage to enhance the fidelity of triage scenarios may be useful not only for the education of triage nurses but also the conduct of research into triage decision-making. [CoLe04]

The objective of the study "Comparison of Mass Casualty Incident Triage Acuity Status Accuracy by Traditional Paper Method, Electronic Tag, and Provider PDA Algorithm" [BuLy07] was the evaluation of the accuracy of triage using an embedded algorithm in a wireless electronic system compared to traditional methods of triage. The Wireless Internet Information System for Medical Response in Disasters (WIISARD) [BuLy07] project uses wireless technologies, including 802.11, mesh-networking, instantaneous data transfer and geo location to coordinate patient tracking and care from field to hospitals. The conducted comparative trial during a multi-casualty incident (MCI) drill comparing the Wireless Internet Information System for Medical Response in Disasters (WIISARD) system to traditional paper tracking of casualties. There were two parallel response teams, both of which consisted of professional emergency responders. The control using the traditional paper technology and the experimental using the WIISARD wireless system, both receiving 50 identical matched patients. The WIISARD group could perform automated triage using a personal digital assistant (PDA) or they could perform manual triage using an electronic triage tag (iTag). The "Gold Standard" for the patient triage status was determined a priori and written into patient scenarios that should have led to the appropriate triage status (Immediate, Delayed, Walking Wounded, Morgue) with strict application of the START (Simple Triage and Rapid Assessment) triage algorithm. There were three groups analyzed: Control-manual, WIISARD-PDA, and WIISARD-iTag. They were able to retrieve 76% of scenarios for the control group and 92% of scenarios for the WIISARD group, 17 scenarios using the PDA, 28 scenarios using the manual entry into the iTag. The control manual group had 73.7% accuracy when compared to the gold standard. The WIISARD-PDA group had 72.2% accuracy and the WIISARD-iTag group had a 67.8% accuracy when compared to the gold standard ($p = 0.09$) which shows that there was no significant difference in accuracy between the 3 methods of triage acuity determination in this MCI drill. [BuLy07]

The objectives of the study "Data collection on patients in emergency departments in Canada" [RoBo06] were to determine the use of electronic patient data in Canadian EDs, the accessibility of provincial data on ED visits, and to identify the data elements

and current methods of ED information system (EDIS) data collection nationally. Surveys were conducted of the following 3 groups:

- a) all ED directors of Canadian hospitals located in communities of >10 000 people
- b) all electronic EDIS vendors
- c) representatives from the ministries of health from 13 provincial and territorial jurisdictions who had knowledge of ED data collection.

The results of the study were the following: Of the 243 ED directors contacted, 158 completed the survey (65% response rate) and 39% of those reported using an electronic EDIS. All 11 EDIS vendor representatives responded. Most of the vendors provide a similar package of basic EDIS options, with add-on features. All 13 provincial or territorial government representatives completed the survey. Nine (69%) provinces and territories collect ED data; however the source of this information varies. Five provinces and territories collect triage data, and 3 have a comprehensive, jurisdiction-wide, population-based ED database. 39% of EDs in larger Canadian communities track patients using electronic methods. A variety of EDIS vendor options are available and used in Canada. [RoBo06] The wide variation in methods and in data collected presents serious barriers to meaningful comparison of ED services across the country. The majority of information regarding ED overcrowding in Canada is anecdotal, when the collection of this critical health information is so variable. According to [FoBo06] there is an urgent need to place the collection of ED information on the provincial and national agenda and to ensure that the collection of this information consistent, comprehensive and mandatory. [RoBo06]

The study “The effect of training on nurse agreement using an electronic triage system” [DoBu07] describes the inter-rater agreement and manual overrides of nurses using a CTAS-compliant (Canadian Triage and Acuity Scale), web-based triage tool (eTRIAGE) for 2 different intensities of staff training. This prospective study was conducted in an urban tertiary care ED. In phase 1, eTRIAGE was deployed after a 3-hour training course for 24 triage nurses who were asked to share this knowledge during regular triage shifts with colleagues who had not received training ($n = 77$). In phase 2, a targeted group of 8 triage nurses underwent further training with eTRIAGE. In each phase, patients were assessed first by the duty triage nurse and then by a blinded independent study nurse, both using eTRIAGE. Inter-rater agreement was calculated using kappa (weighted κ) statistics. In phase 1, 569 patients were enrolled with 513 (90.2%) complete records; 577 patients were enrolled in phase 2 with 555 (96.2%) complete records. Inter-rater agreement during phase 1 was moderate (weighted $\kappa = 0.55$; 95% confidence interval (CI) 0.49–0.62); agreement improved in phase 2 (weighted $\kappa = 0.65$; 95% CI 0.60–0.70). Manual overrides of eTRIAGE scores were infrequent (approximately 10%) during both periods. [DoBu07] Agreement between study nurses and duty triage nurses, both using eTRIAGE, was moderate to good, with a trend toward im-

provement with additional training. Triage overrides were infrequent. Continued attempts to refine the triage process and training appear warranted. [DoBu07]

3.3 Open Source Software for RFID Emulation

The practical part of this diploma thesis is the implementation of a prototype for the mobile triage device and the terminals for the collection of patient information. Thus we require software emulating the RFID technology. Beside the simulation of RFID readers and RFID tags this open source software should imply an RFID middleware for the coordination of the readers.

3.3.1 Fosstrak Project

Fosstrak is an open source RFID software platform implementing the EPC network [EpIn09] specifications. It is intended to support application developers and integrators by providing core software components for track & trace applications.

Radio Frequency Identification (RFID) technology has a lot of potential to improve patient tracking processes and the storage of patient information. To realize the full potential of RFID, an IT infrastructure is required that manages readers, filters and aggregates raw RFID data, but also facilitates data exchange among the components of the electronic triage system.

The Fosstrak project consists among others out of 2 components being relevant for the electronic triage system:

- The RFID Reader which identifies RFID tags and exposes its functionality through the Reader Protocol (RP) and Reader Management Protocol (RM).
- Filtering and Collection Middleware which is responsible for the coordination of readers and the filtering and collection of RFID readings. [FoOw09]

Besides that the Fosstrak project includes the Fosstrak HAL project. The objective of the Fosstrak HAL project is to define a hardware abstraction interface that is used to access RFID readers and implement it for various reader devices and reader simulators. The HAL Simulator allows simulating RFID readers with more antennas and creating RFID tags. By dragging the tags over the reader antenna the user can simulate the reading of an RFID tag.

For the mentioned reasons we decided to use the Fosstrak project framework as the RFID software emulation for the practical part of this diploma thesis. Before we came to this decision we analyzed other open source software which came into consideration to be used but did not fulfill all needs for the practical part of the diploma thesis.

3.3.2 Rifidi Project

Rifidi is an open source tool allowing the development of an RFID system with software components and removing the dependency on hardware and infrastructure similar to the Fosstrak project.

The Rifidi project allows creating virtual RFID architecture with software defined RFID readers, RFID tags, and RFID events that behave like their real-life counterparts. [RiSo09]

The big disadvantage of the Rifidi project is the absence of middleware responsible for component coordination and for the collection and filtering of the read RFID data.

3.3.3 RadioActive

The RadioActive Foundation [RaFo09] is a group of projects with the mission to develop quality RFID applications and to promote the use of RFID technology. RadioActive is an open source suite of RFID applications with a focus on the EPC network (see also chapter 3.4) and consists of the subprojects Graviton and Fusion. [EpIn09]

The Graviton project implements the hardware sensor layer of an RFID deployment. It contains a reader simulator, an implementation of the Reader Protocol and Reader Management standards.

The Fusion project is a generalized middleware system that takes RFID input and adds contexts necessary to add meaning to that raw sensor input.

According to the EPC network documentation, the middleware is responsible for:

- Managing various readers
- Gathering tag readings from the readers
- Filtering, aggregation and counting of tag data [RaFo09]

The reason why we did not chose RadioActive as RFID emulation software is the development status of the project which is still in the planning stage.

3.4 EPCglobal Network

The EPCglobal Network is a set of technologies that enable immediate, automatic identification and sharing of information on identifiable items. The EPCglobal Network is usually used to share product data between trading partners but the specifications and infrastructure of the EPCglobal Network are convenient for the electronic triage system.

Basis for the information flow in the network is the Electronic Product Code (EPC) [EpIn09] of each item which is stored on an RFID tag. The EPC can be used to identify

patients, is written to and read from RFID tags using the air communication protocols also defined by EPCglobal.

The EPC Information Services (EPCIS) is a standard designed to enable EPC-related data sharing within and across facilities. This data sharing is aimed to enable all network participants a common view of object information. At the EPCIS each facility designated who has access to its dynamic information. [FoOw09]

The RFID tag contains the EPC, which can be read and written using the air communication protocols which are defined by EPCglobal. [EpIn09]

The EPC infrastructure builds the Tag Data Standard and the air interface protocols and consists of a number of roles and interfaces. These roles and interfaces need to be deployed within an organization in order to process an EPC tag in a correct way (EPC-compliant). The EPC Network does not specify individual components which have to be implemented. Moreover it defines the roles and interfaces which must be implemented illustrated on Figure 3-1: [FoOw09]

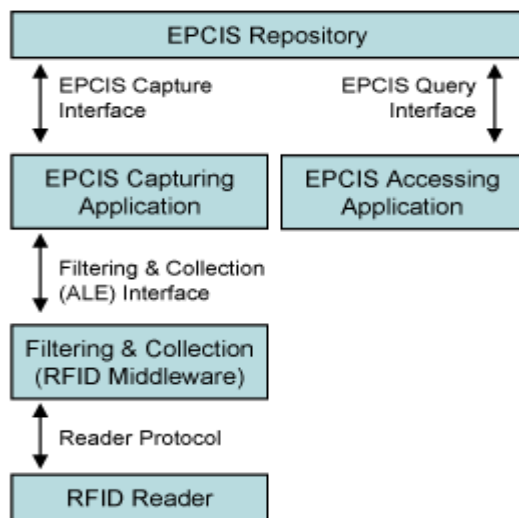


Figure 3-1: Roles and interfaces in the EPC Network

The architecture of the EPC Network is comprised of a number roles and interfaces:

- The RFID Reader - identifies RFID tags and exposes its functionality through the Reader Protocol (LLRP and RP) and Reader Management Protocol (RM).
- Filtering and Collection Middleware - is responsible for the coordination of readers and the filtering and collection of RFID readings. It generates Application Level Events (ALE) for higher layers.

- The EPCIS Repository - is used to store EPCIS events that are generated by interpreting RFID readings. Its functionality is exposed via the Capture and Query Interface.
- EPCIS Capture and Query Applications obtain RFID readings from the middleware and transform them into EPCIS events that are then saved in the EPCIS Repository. These events can be queried by an EPCIS Query Application. [FoOw09]

4 Definition of the System Architecture

The requirements for the electronic triage system must ensure that critical information collected in the field is communicated to receiving personnel quickly and accurately. All patients and emergency personnel must be registered and identifiable. The electronic triage system must ensure that patients and emergency personnel are accounted for at all times without over reliance on manual, error prone, processes. The collected information relevant to situational management and decision support must be integrated into a central unit and available over a single application for the command center. In case of system or network failure the electronic triage system must have contingency capabilities.

4.1 Workflow in the Electronic Triage System

By applying the RFID technology into the triage workflow the triage system implicates the change that instead of writing and collecting the conventional paper tags, emergency personnel read the information of each injured person from the RFID tag, input the information of each injured person to the mobile triage device and then write it on the RFID tag.

Figure 4-1 demonstrates the workflow in the RFID Triage System with electronic triage tags and mobile triage devices using the wireless communication. [InSo08]

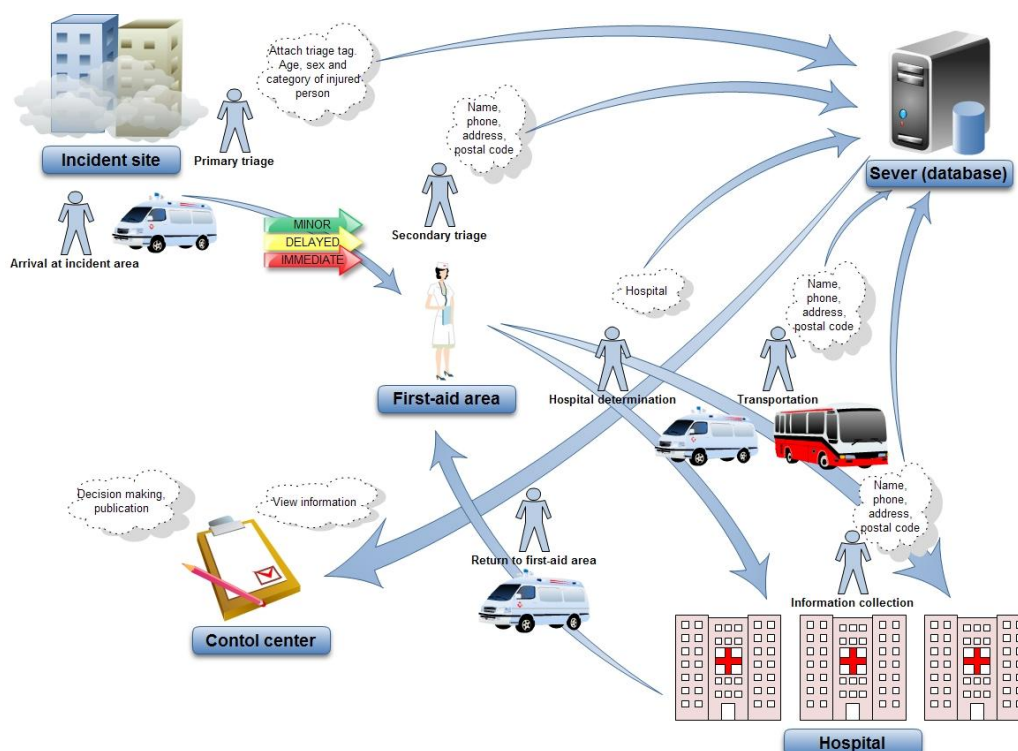


Figure 4-1: Workflow in RFID Triage System [InSo08]

In the following section the usage of the electronic triage system by emergency personnel in different stages of triage will be described.

The emergency person being responsible for primary triage inputs the information of each injured person by the mobile triage device which writes it on the RFID tag. At the same time the emergency person attaches the triage tag with the RFID tag to the injured cuts the triage tag off to the right color. In the background the mobile triage device sends the information of the injured person, written to the RFID tag, to the server as soon as the wireless network is available.

The emergency person being responsible for secondary triage reads the information of each injured person from the RFID tag through the mobile triage device and changes or adds the information to the RFID tag by interviewing the injured person.

The emergency person being responsible for hospital determination selects the hospital to which the injured person must be transported by the mobile triage device and writes the information to the RFID tag.

The emergency person being in an ambulance/transport vehicle or in a hospital has the same duties like the emergency person being responsible for secondary triage with the difference that he/she has not the mobile triage device but a notebook PC with keyboard and mouse and an RFID reader. Except that the emergency person can record the time needed to carry the injured person to the hospital.

The emergency person in the control center can browse the patient information. The information is stored on the server and can be visualized by using web browser software for instance. Then the emergency person can inform different facilities like the emergency control center in the municipality or the search and rescue teams. The information of the injured people is stored on the server providing the information to the control center terminal for instance through HTTP protocol. [InSo08]

The following sequence diagram shows the collaboration of the emergency personnel and the standard treatment of an injured person using UML version 2 (Figure 4-2).

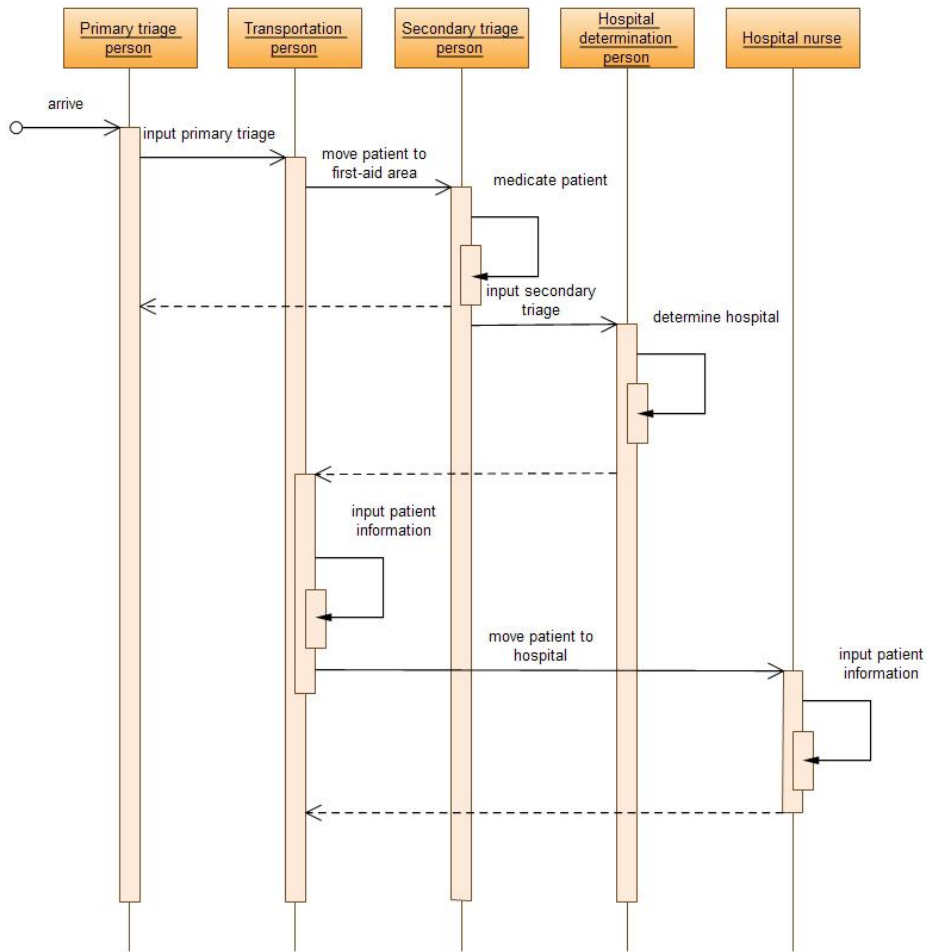


Figure 4-2: Sequence diagram visualizing emergency treatment

4.2 Use Cases

This section discusses the use cases of the electronic triage system giving an rough overview of the use cases of an emergency person in figure 4-3 shows a rough overview for an emergency person in the RFID triage system.

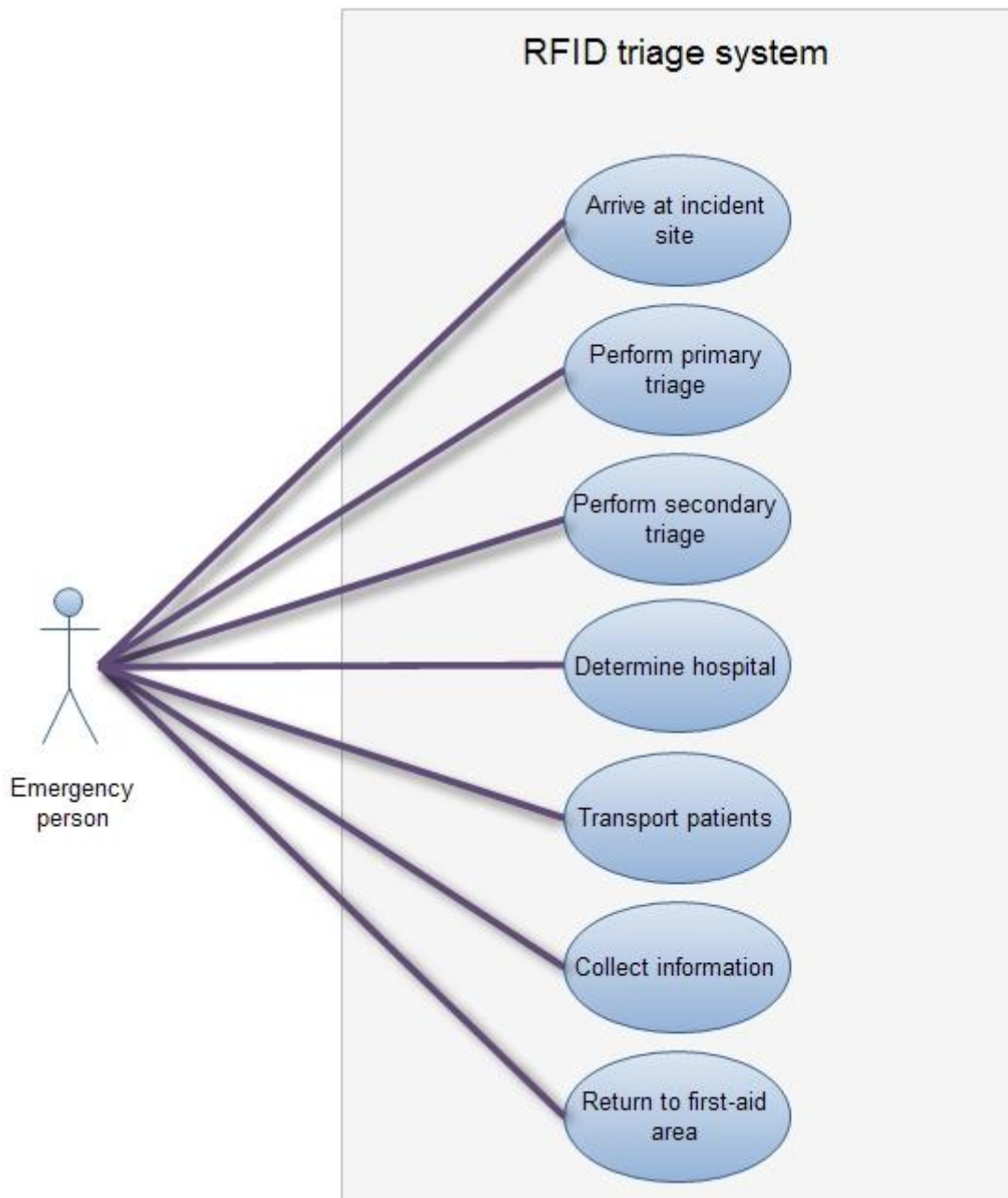


Figure 4-3: Rough overview of the use cases for an emergency person

In Table 4-1 the use cases of the RFID triage system are described and demonstrated in Figure 4-4:

ID	Use Case Name	Primary Actor	Brief Description
1	Arrive at incident site	Primary triage person (the actors are derived from the superior actor "Emergency person")	Emergency personnel responsible for the primary triage arrive at the incident site. They start scanning the incident site for injured people.
2	Establish first-aid area	First-aid nurse	Close to the incident site, but on a safe place, the first-aid area is established. Patients are moved from the incident site to the first aid area after the primary triage is performed. After the hospital determination transportation personnel move the patients from the first-aid area to the hospitals.
3	Establish control center	Director of operations	Close to the incident site, but on a safe place, the control center is established. The director of operation can browse the patient information stored on the server. The director of operation can inform different facilities like the emergency control center in the municipality or the search and rescue teams. The responsibility of the director of operations is to establish wireless network at the incident site, the first-aid area and the control center.
4	Attach triage tag	Primary triage person	Primary triage person attaches the triage tag (including the RFID tag) to the injured person and identify the injury level in about 30 seconds.
5	Input primary triage information	Primary triage person	The primary triage person inputs the primary triage information (age, sex, injury category) with the mobile triage device and writes the information to the triage tag and tears of the appropriate color of the injury level. In the background the mobile triage device sends the information of the injured person, written to the RFID tag, to the server as soon as the wireless network is available.
6	Move patients to first-aid area	Transportation person	Triaged patients with the attached triage tag are brought to the first-aid area by

			transportation personnel. Emergency personnel can perform first-aid in the ambulance.
7	Medicate patients	First-aid nurse	Patients arriving at the first-aid by the transportation personnel get a medical treatment. The nurse performs first-aid to the injured person in the first-aid area.
8	Input secondary triage	Secondary triage person	The secondary triage person reads the information of each patient from the RFID tag through the mobile triage device and adds or changes information by interviewing the injured person. Afterwards the emergency person writes the information to the RFID tag with the mobile triage device and saves the information. If wireless network is available the mobile triage device sends the information to the server.
9	Determine hospital	Hospital determination person	Before the patient leaves the first-aid area the target hospital must be determined. The hospital determination person decides which patient is brought to which hospital.
10	Input hospital	Hospital determination person	After determining the target hospital the hospital determination person inputs the address (postal code) of the hospital into the mobile triage device and saves the information to the RFID tag. If wireless network is available the mobile triage device sends the information to the server.
11	Move patients to hospital	Transportation person	After the hospital has been determined the transportation person moves the injured person to the hospital by the ambulance. Emergency personnel can record the time needed to carry the injured person to the ambulance. Changed or added information is stored on the RFID tag and sent to the server as soon as mobile network is available.

12	Input patient information	Transportation person & hospital nurse	Emergency personnel in ambulance and hospital input or change information of the injured person with the ambulance terminal and hospital terminal and save the information to the RFID tag and send the information as soon as mobile network is available. The transportation person and the hospital nurse use notebook PC combined with an RFID reader for the input of patient information.
13	Return to first-aid area	Transportation person	After moving the injured person to the hospital the transport vehicles return from the hospital to the first-aid area again and repeat the transportation of the injured people to the hospital.
14	Read information of injured people	Director of operations	The information of the injured people is collected on the server in the database of injured people. The director of operation can read this information by using for instance browser software.
15	Coordinate triage	Director of operations	After reading the information of the injured people the director of operations can make decisions how to proceed with the triage activities. This information is stored on the server and can be visualized by using web browser software for instance. Then the emergency person can inform different facilities like the emergency control center in the municipality or the search and rescue teams.
16	Public information	Director of operations	The collected information about injured people can be published or forwarded to particular facilities.

Table 4-1: Use cases of the RFID triage system

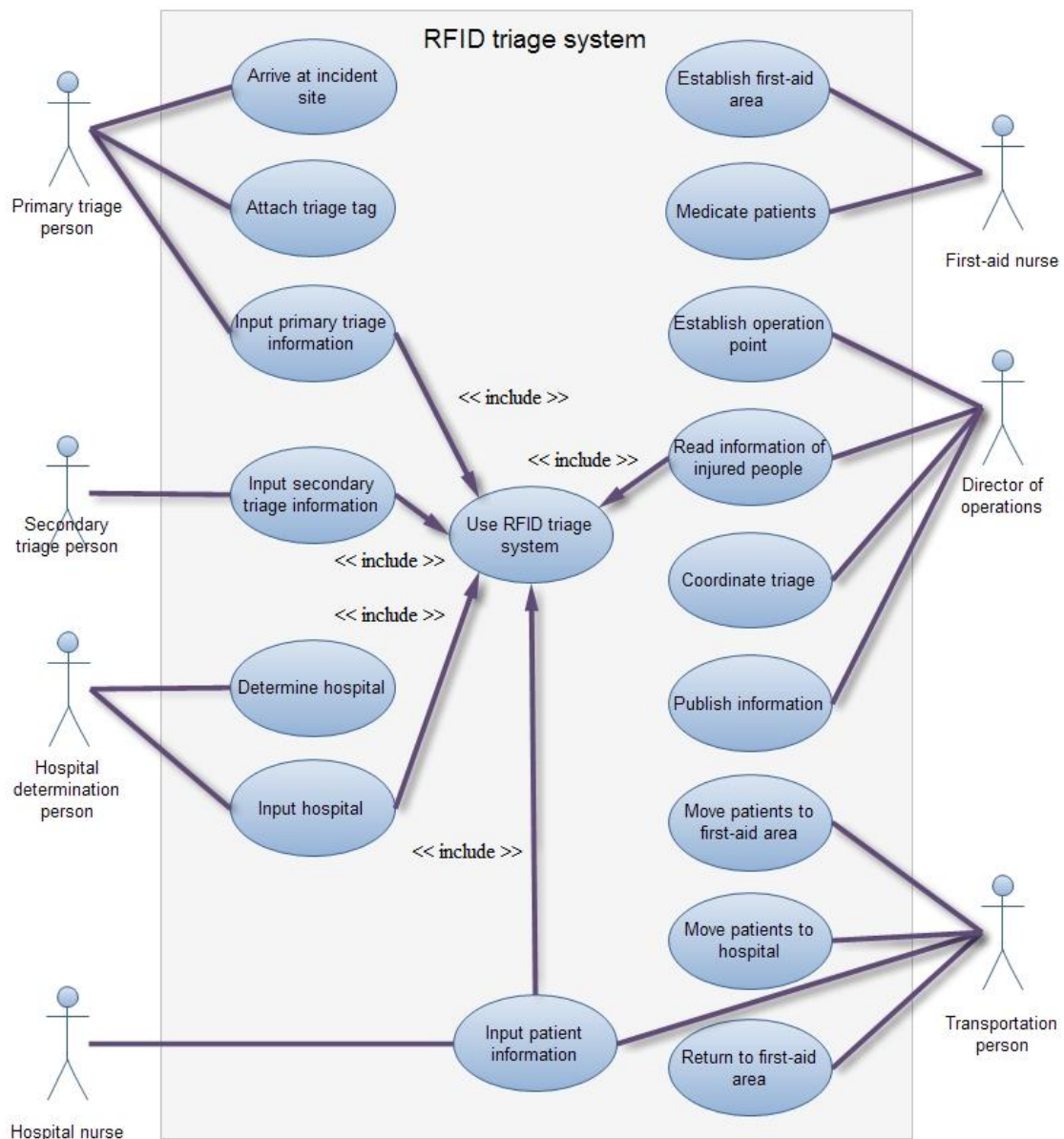


Figure 4-4: Use case diagram of the RFID triage system

The actors using the electronic triage system add or change patient information by the mobile triage device or the terminals. Only the director of operation in the command center obtains the information by read access to coordinate the triage.

The coordination of the field management consists of predefined processes operated by certain actors (Figure 4-4):

- **Primary triage person:**
After arriving at the incident site the primary triage person starts scanning the incident site for injured people, inputs patient information (age, sex, injury category) by the mobile triage device and writes it on the RFID tag and finally attaches the triage tag with the RFID tag to the injured person.

- Secondary triage person:
In the first-aid area the secondary triage person reads the information of each patient from the RFID tag through the mobile triage device and changes or adds the information (name, phone, address) to the RFID tag by interviewing the injured person.

- Hospital determination person:
The hospital determination person is responsible for the selection of the hospital to which the patient must be transported. This information is written to the RFID tag by the mobile triage device.

- First-aid nurse:
The first-aid nurse is responsible for the medication of the patients arriving in the first-aid area.

- Transportation person:
The transportation personnel move the patient from the incident site to the first-aid area and afterwards from the first-aid area to the hospital and return to the incident site or the first-aid area again. Emergency personnel in the ambulance can change or add patient information and write it to the RFID tag. Except that they record the time needed to transport the injured person to the hospital.

- Hospital nurse:
The hospital nurse can add or change patient information using the electronic triage system.

- Director of operations
The director of operations can browse the patient information stored on the server and can be visualized by using web browser software for instance. He/she can inform different facilities like the emergency control center and coordinate the search and rescue teams.

The following sequence diagram shows the information flow and the connection between the emergency personnel and the server with the information database (Figure 4-5).

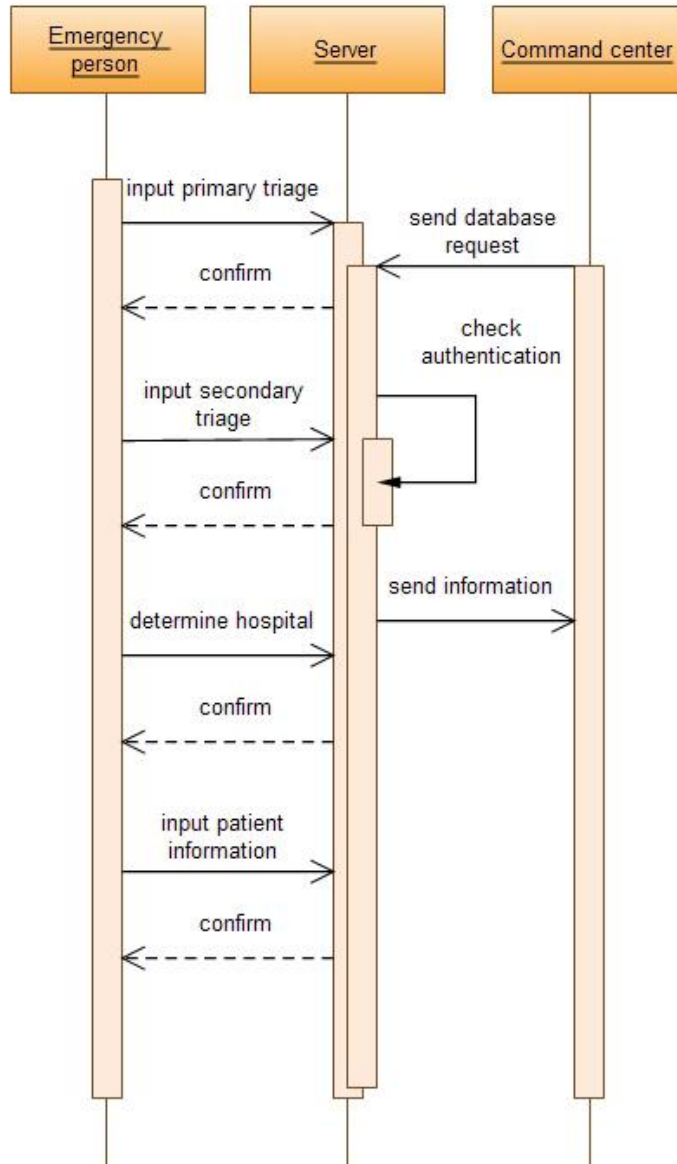


Figure 4-5: Information flow between emergency personnel and server

4.3 Technical Requirements for the RFID Middleware

The RFID middleware software is the bridge between the RFID architecture and the data repositories (the central database). The RFID middleware is the central part of the RFID system managing and coordinating it. It is responsible that patient information is consistent, updated constantly and provided for the control center. The main challenge for the RFID middleware is to provide data consistency.

4.3.1 Information Consistency

To ensure availability of patient information to the emergency personnel the mobile triage devices send patient information after writing it to the RFID tag. In certain circumstances there is no wireless network available. The mobile triage device queues the patient information and sends it to the server as soon as wireless connection is established.

In the meantime other emergency personnel read the information from the RFID tag whereby changing and adding information and storing it to the RFID tag again. We assume that wireless network is available and the information is sent to the server.

If the mobile triage device having no wireless network now establishes a wireless connection it sends the queued information to the server. Storing this information to the database by a so-called blind write leads to lost updates of patient information. To prevent this data inconsistency the RFID middleware verifies the version of the sent data. This is implemented by storing and increasing the versionID with every write operation of the RFID tag.

To simplify this data consistency conflict we will illustrate the lost update problem.

4.3.2 Lost Update Problem

Depending on the availability of the wireless network the mobile triage device can send the patient information to the server. Thus it is possible that the server gets old information at a later date. This write-write conflict is outlined in Figure 4-1.

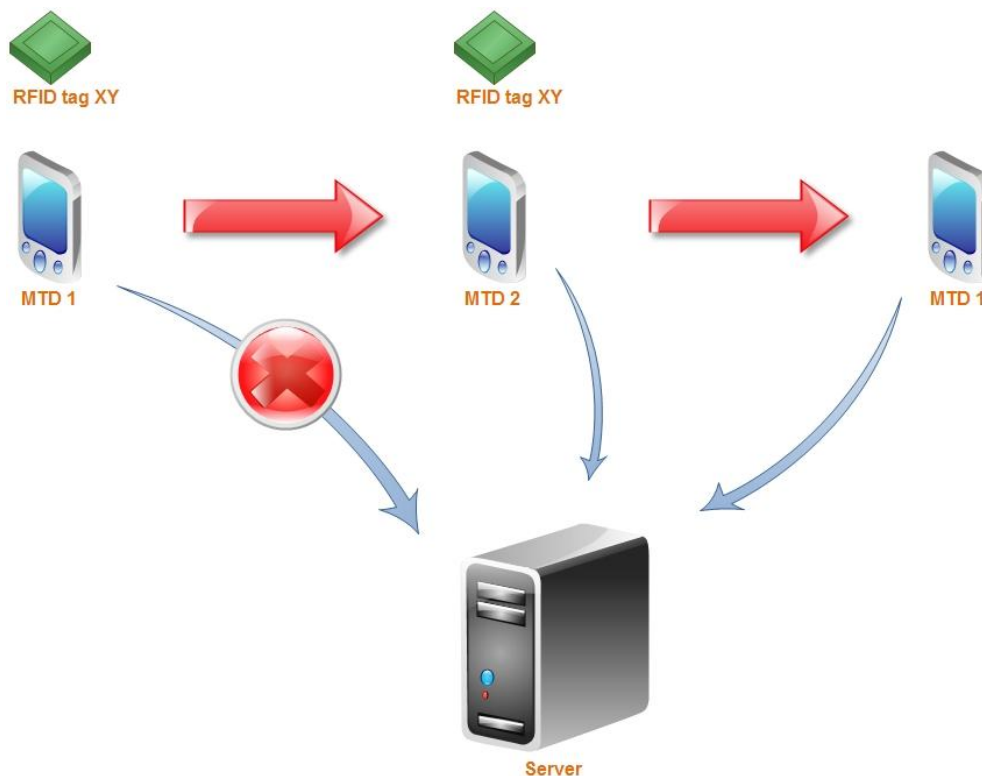


Figure 4-6: Lost update problem

After storing patient information to the RFID tag the mobile triage device 1 (MTD 1) tries to establish a connection to the wireless network. At that time the wireless network is not available in the area of the MTD 1, thus the information is queued in MTD 1 until a wireless connection is established. The patient is moved to another location (e.g., first-aid area) treated by an emergency person using the mobile triage 2. MTD 2 reads the information from the RFID tag and adds or changes information. Finally it stores the information to the RFID tag and sends to the server via the available wireless connection.

In the meantime the emergency person carrying MTD 1 moved to a location where wireless network is available. Now MTD 1 sends the queued information to the server. Writing this information to the database leads to a lost update made by MTD 2.

Hence, the RFID middleware is responsible to prevent this information lost by applying a mechanism which prevents overwriting the latest patient information through old information. The problem is simply solved by storing a version of the patient information on the RFID tag. The RFID middleware checks the versionID before storing patient information to the database. If the versionID is lower than the current versionID the information will be discarded, otherwise it will be stored in the database.

The described setting is chronologically structured in Table 4-2 including the network status of the mobile triage devices and the versionID of the written data.

Time	Mobile Device	Triage	Wireless Network	Action	versionID
T1	MTD 1		Not available	Write (RFID tag)	1
T2	MTD 1		Not available	Queue (Information)	1
T3	MTD 2		Available	Write (RFID tag)	2
T4	MTD 2		Available	Send (Server)	2
T5	MTD 1		Available	Send (Server)	1 (→ discard!)

Table 4-2: Lost update

This mechanism assures consistency of patient information stored on the server. Nevertheless there are further general concerns which must be considered in the electronic triage system.

4.4 System Requirements

Several technical requirements of the electronic triage system can be identified as important challenges for pervasive computing arise regarding the paths through which the information of injured people is collected:

a) Confidentiality:

Patient information is stored on the RFID tag and on the central unit. This information must be accessible only to authorized emergency personnel. Thereby the electronic triage system ensures information security. Accuracy of the stored data must be provided by the system through security measures applied to the different layers of the electronic triage system.

b) Input Rate:

The time is a critical factor in the early stage of triage. Hence, the input time of the patient information must be optimized to a minimum. Input rate is improved by the mobile devices using less error prone input read/write methods and automating information storage like the emergency personnel information.

The network status must not influence the input rate, this is assured by storing the patient information primary on the RFID tag and in the case of an available wireless connection the information is sent asynchronously to the central unit.

c) Availability

Emergency personnel must be able to use the system properly. Especially, input operations of the information of a patient must be available anytime in the triage, even when the network is not reachable. This is assured by the storing the patient information on the RFID tag and using it as local buffer. Emergency personnel can read or write data by referring the RFID data already which has already been written so far. The input device pushes the new data to the queue that is sent to the destination independent of the user's operation, as well as writing to the RFID tag.

d) Low Latency:

Input information of the early stages of triage must be collected quickly and viewed from the control center. Latency is lowered by defining minimum wireless communication areas in the paths of the triage workflow.

4.5 Technical Requirements of the RFID Tag and RFID Reader

This section discusses the technical requirements of the RFID tag and the RFID reader of the electronic triage system.

4.5.1 Requirements of the RFID Tag

- a) Non-powered (passive) RFID chip: Passive RFID tags don't need a battery because they receive their energy from the read/write device that powers the tag to allow transmitting the data.

The advantages of a passive RFID tag are:

- It works without battery and has a durability of over twenty years
- It is less expensive to manufacture
- It is smaller (one passive tag has the size of a grain of rice)

The disadvantages of a passive RFID tag are:

- It can be read only at short distances
- It requires a higher-powered reader than active RFID tags
- It has difficulty sending data through liquids or metal

Active RFID tags are equipped with a battery that can be used as a partial or complete source of power for the tag's circuitry and antenna. They can be read at distances of one hundred feet or more. But they cannot function without battery

power, which limits the lifetime of the tag. The fact that active tags are typically more expensive and physically larger combined with the battery limiting their lifetime make active RFID tags unsuitable for the electronic triage system.

The requirements for the electronic triage system are achieved by the characteristics of the passive RFID and the disadvantages of the not affecting the electronic triage system in a negative way. Thus we recommend the usage of passive RFID tags for the technical implementation of the electronic triage infrastructure.

- b) Rewritable memory of 1 kilobyte: Passive tags usually have 64 byte to 1 kilobyte memory. For the RFID triage system 1 kilobyte of rewritable memory are required on the silicon based tag because of the evaluated data model in chapter 5.4.

When the reader supplies the tag with power the radio waves from the reader are encountered by the passive RFID tag, the wound antenna within the tag generates a magnetic field. The tag draws power from it which energizes the circuits in the tag. After this the tag sends the encoded information in its memory. [EpSp09]

- c) High frequency of 13.56 MHz: High frequency tags are less failure sensitive than low frequency tags. They usually have a read range lower than 1 meter but the size of the RFID tag has a significant impact on the read range too.
- d) Read range limited to 5cm: The main factors the read range of an RFID tag depends on are:
- size of the antenna of the tag
 - size of the antenna of the reader
 - output power of the reader

In the RFID triage system the read range should be limited to 5cm. This restriction avoids reading collisions between two different tags.

- e) Size of tag limited to 2.5cm by 2.5cm: The smallest tags available today have the size of a 25mm square. There are specialized tags scaled down to 2mm by 2mm but this size is not necessary because there is enough space on the conventional paper triage tag.

f) **Durability:** The RFID tag should be resistant and unsusceptible against effects of the environment like temperature, pressure, radiation, chemical and water.

- **Temperature:**

The most RFID tags have the typical read/write temperature between -25°C and $+70^{\circ}\text{C}$ and a storage temperature between -40°C and 80°C . These values may vary a little bit from manufacturer to manufacturer. Specialized tags can withstand temperatures up to 250° which is not necessary for the RFID triage system.

- **Pressure:**

The resistance against pressure depends on the construction of the tag. The usual tags can withstand high pressure.

- **Radiation:**

Depending on the intensity of the radiation the tag is resistant against almost all kinds of radiation except gamma radiation which erases or destroys most silicon based circuits.

- **Chemical:**

The tag should satisfy the requirements in terms of chemical resistance which is very important in incidents with chemicals. Common RFID tags fulfill these requirements.

- **Water:**

The tag must be waterproof which means that the data stored on the RFID tag will not be lost when the tag gets wet through rain, flood or anything else. Common tags are waterproof. [IIAh08]

4.5.2 Requirements of the RFID Reader

a) **Integrated in the mobile triage device:**

The RFID reader must be integrated into the mobile triage device being an easy portable device for the emergency personnel while the primary triage, secondary triage and hospital determination.

b) **Ability to interrogate the tag:**

The RFID reader must be able to read from and to write to the specified RFID tag in the previous chapter.

Many factors affect the read range of the reader to read the tag:

- Frequency used for identification
- Antenna gain
- Orientation and polarization of the antenna
- Placement of the tag on the object to be identified

4.6 Security Aspects

The security concerns about the RFID technology in the electronic triage system are grouped in four main categories:

- a) Data ownership: Address, religion and other personal information of the injured person is stored on the RFID tag. In order to prevent abuse of the individual privacy there is urgency to this discussion.
- b) Data theft: Having the according RFID reader data theft is possible. Chip manufacturers work against this by adding security features such as secure encryption schemes to the chips and data. Some examples of secure encryption schemes will be described in this chapter.
- c) Data corruption: Most RFID tags are rewritable like the RFID used in the RFID triage system. This feature normally can be locked but it does not make sense in the RFID triage system because the tag should be rewritable from start of the triage process till the end. Therefore the tags have to be unlocked so emergency personnel are able to add or change information about the injured person. Therefore the potential exists for malicious users to rewrite the tags with wrong information or fraudulent data. [AhII08]
- d) Disposal: After a certain time period the RFID tags and the electronic patient data can be disposed depending on the different law regularizations in each country.

4.6.1 Aspects of RFID Security

Under the various security interests in RFID technology, authenticity of identification and data, privacy and availability are the most critical.

- a) Authentication and Integrity

The performance of secure identity verification is improved by RFID facilitated identification which makes the RFID technology suitable for the electronic triage system. As an example, RFIDs have been added to the new international passport standard (ICAO) to enhance the security and efficiency of database-driven checks at ports of entry. It is helpful to consider this example in some detail to appreciate the real-world consequences of the adoption of RFID as a security mechanism in the electronic triage. While RFIDs are not supposed to replace manual verification by the agent/officer, documents guiding its adoption indicate an intention to reduce the time taken to process passports, including eliminating

the need to use optical scanning to verify them. Focus on processing time may lead to RFID-based identification becoming the primary mechanism providing passport authenticity guarantees, such as protection from forgery. [AhII08]

It is claimed that the additional difficulty of forging an RFID tag will make the passport and ID systems more secure. Secure facilities have adopted RFID for controlled access to restricted areas and RFID is being deployed to increase the efficiency of container shipping tracking, including supporting international initiatives on combating drug and weapons smuggling. [AhII08]

In each of these examples, the RFID system substitutes for other security systems providing more convenience and potentially more security by increasing the ability to consistently apply security checks which can be adapted to the electronic triage system.

The use of strong authentication mechanisms in triage tags is one element of making such systems more resilient against coning attacks. At the physical layer, protection against extraction of authentication keys through observation of the reflected electromagnetic field must be addressed.

Authentication and integrity are also important in connection with privacy concerns to be considered next.

b) Privacy

RFID triage tags have low intrinsic value and even any data they carry may itself be of low relevance. However, such tags are attached for monitoring the patients. As standard RFID technology dictates that tags must satisfy interrogation requests by arbitrary readers, it is possible for covert and unauthorized readers to be deployed.

Anonymity of the identifier must provide for unlinkability, i.e., must prevent an observer from correlating two instances of interaction/communication by the same tag. In this section, whenever we refer to location privacy, or to anonymity, we refer to unlinkable anonymity.

Triage tags contain patient information as needed by the infrastructure of the electronic triage. This transport of related data provides a secondary channel that can be exploited by information gathering efforts. If the patient information is stored in plaintext in the tag, the target of an attack may be simply reading it to use for any purposes. This threat to privacy through exploitation of hidden channels may also utilize unauthorized readings, for instance, of counters or other da-

ta structures that change in predictable ways between instances of the communication protocol involving a particular tag.

In addition to considering the threat of privacy compromises by outsiders, one must also evaluate the potential for abuse by system operators using the mobile triage devices and ambulance and hospital terminals. Such privacy concerns are referred to as Big Brother privacy concerns. They involve considerations of a different nature, including legal aspects, individual privacy expectations and other public policy matters.

c) Availability

Availability refers to the security guarantee that system resources will be accessible when needed. Clearly, availability implies some preexisting level of expectation for performance parameters and it is both a security as well as a reliability and performance concern. Concentrating on security aspects, it is possible to enumerate a number of different attacks against availability and/or available counter-measures:

- Killing attacks: RFID tags support kill functionality or kill key. If a particular value is broadcast to a tag, it will be de-activated, either temporarily (until an enabling value is received) or permanently. For instance, the kill-key feature is available in RFID tags used to prevent shoplifting; these are disabled at the point-of-sale to allow for handling and reuse without raising false alarms. This feature can be relevant if the local facility wants to prevent larceny of the archived triage tags including the RFID tags with the patient information.
- Disabling attacks: This generic class of attacks exploits state synchronization requirements of authentication mechanisms for tags. Some existing and proposed protocols for secure RFID authentication [ZhKi09] require tags to maintain state information that should match with other information available to the readers or (more commonly) to the back-end server. Disabling attacks interfere with the communication between tag and authorized reader to cause divergence between the state information among the parties, preventing further use of the RFID triage tag. To prevent against such attacks, either mechanisms must be provided for recovery of a convergent state, or mutual authentication must be used to ensure integrity of exchanged messages before a state update is performed.
- Jamming attacks: The communication frequencies can be filled with noise by a reader (or other broadcasting device) that does not comply with accepted standards. If the level of introduced noise is high, it may difficult or impossible to

prevent against such attacks. Available techniques to tolerate (some level of) jamming attacks involve mechanisms at the communication layer.

4.6.2 Anonymity and Availability Requirements Conflict

Anonymity and availability appear often to conflict in RFID technologies. For instance a privacy preserving technique can be created from an availability threat (jamming). In the following, we discuss how privacy techniques lead to availability risks.

Of the earlier-mentioned classes of attacks against availability, disabling attacks represent a particularly difficult challenge to address, particular in conjunction with location privacy requirements. Privacy implies that tags must change the values they use to authenticate or identify themselves to the system, to prevent from recognition and tracking by unauthorized parties. This implies that some form of changeable shared state must be maintained between tags and server.

Consider the case of single-side authentication, i.e., the tag authenticates itself to the reader but not conversely. In some protocols, this is achieved through the use of a shared-state such as the seed for generating an unpredictable sequence. Disabling attacks against such protocols involves impersonating a reader to lead the tag in stepping the sequence, reaching the next state. Typically, as tag authentication protocols are designed to take a few hundred milliseconds, the fake reader has ample opportunity to cause the tag to become significantly desynchronized from the back-end server, by repeated application of this attack. Since there is no obvious bound on the number of state updates that an adversary could force on a tag, there is accordingly no guarantee that the back-end server will recognize the tag after speculatively stepping the state for every tag in its database a fixed number of times.

In general, protecting the exchanges between tags and the other system components to prevent faulty state changes is difficult. Passive tags do not maintain a clock and cannot use (even loosely synchronized) timing information as a security mechanism; they allow for implementation of only a limited set of cryptographic operations and have limited transient and permanent storage, therefore being less capable of detecting attacks. The following are some strategies that are available to prevent against such resynchronization attacks:

- Tag Identification and Server Authentication
- Resynchronization
- Exhaustive Key Search

Having discussed the remaining challenges attending the simultaneous provision of anonymity and availability in RFID authentication protocols, we now describe the set of

tools that are available to their solution and can be applied to the electronic triage system.

4.6.3 RFID Security Mechanisms

This section describes capabilities available to RFID tags for security measures, considering the requirements of passive tags.

The minimal circuit area used by each feature, in terms of gate-equivalents (GE) is a crucial measure of their feasibility for RFID implementations, with the lowest gate count being preferred because current technology can only provide a few thousand GEs for security in the tags.

a) Asymmetric Cryptographic Primitives

The use of special architectural constructions (digit-serial multipliers) may make it possible to achieve elliptic curve cryptography (ECC) implementations in a few as 6300 GEs, though the numbers get worse if such constructions are not available. These numbers indicate at least the possibility that ECC may eventually be available in high-end, passive tags. Still, taking into consideration pricing pressures and the current state of the art in passive tag technology, it appears unlikely that RFID deployments based on public-key cryptography will be common in the next few years. [IIAh08]

b) Symmetric Cryptographic Primitives

Among the symmetric key primitives, not all are equally amenable to implementation.

- Block ciphers:

Block ciphers suitable for RFID implementations are those that have been designed to achieve highly efficient hardware optimizations under constrained memory conditions. In particular, substantial work has been done that validates suitability of AES for RFID tags, with full implementations requiring as few as 3300-3400 GE.

- Pseudo-random number generators (PRNG):

PRNGs are a flexible primitive and can be built from block ciphers in counter mode, from stream ciphers (the key stream is pseudo-random) and independently using other technologies, such as LFSR based generators, providing flexible trade-off opportunities between security and efficiency needs.

- Stream ciphers:
Stream ciphers are encryption algorithms in which the sequence of plaintext characters is encrypted sequentially using a different function for every step realized with the so-called one-time pad.
- Pseudo-random functions (PRF):
One advantage in designing PRF-based security for RFID is the amount of choice available in the construction of PRFs. They can be composed using the strategy of cascading a PRG, which while being a relatively slow method, results in little gate-count and per-cycle power overhead over the underlying PRG. Block ciphers also provide ready implementations of the PRF primitive.
- Hash functions:
Counter to intuition, hash functions seem at the moment to be less suitable for RFID implementation than the most efficient block ciphers. The reason is that the design of many collision-resistant hash functions uses an underlying block cipher with a large block length – which optimizes the software performance of the hash function by allowing it to process large chunks of data at a time, but makes it inefficient to implement under constrained-memory settings. Their use is discouraged in favor of other primitives whenever collision-resistance is not a requirement.
- Message authentication codes:
Implementations based on block ciphers, e.g., CBC-MAC, or on universal hashing, are preferred to those based on hashes, such as HMAC, due to the earlier-mentioned disadvantages of implementing hashes in RFID tags. [IIAh08]

4.6.4 Data Integrity Solutions

When transmitting data using contactless technology it is very likely that interference will be encountered, causing undesired changes to the transmitted data and thus leading to transmission errors (Figure 4-7).

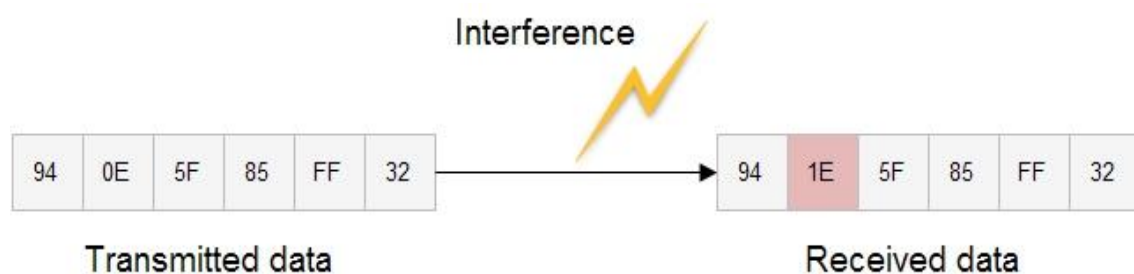


Figure 4-7: Interference during transmission

A checksum can be used to recognize transmission errors and initiate corrective measures for example the retransmission of the erroneous data blocks. The most common checksum procedures are parity checks, XOR sum and CRC. [IIAh08]

a) Parity checking

The parity check is a very simple and therefore a very popular checksum procedure. In this procedure a parity bit is incorporated into each byte and transmitted with it with the result that 9 bits are sent for every byte. Before data transfer takes place a decision needs to be made as to whether to check for odd or even parity, to ensure that the sender and receiver both check according to the same method.

The value of the parity bit is set such that if odd parity is used an odd number of the nine bits have the value 1 and if even parity is used an even number of bits have the value 1. The even parity bit can also be interpreted as the horizontal checksum (modulo 2) of the data bit. This horizontal checksum also permits the calculation of the exclusive OR logic gating (XOR logic gating) of the data bits.

However, the simplicity of this method is balanced by its poor error recognition. An odd number of inverted bits (1, 3, 5...) will always be detected, but if there is an even number of inverted bits (2, 4, 6...) the errors cancel each other out and the parity bit will appear to be correct.

Using odd parity for instance the number E5h has the binary representation 1110 0101 $p = 0$. A parity generator for even parity can be realized by the XOR logic gating of all the data bits in a byte. The order in which the XOR operations take place is irrelevant. In the case of odd parity, the parity generator output is inverted (Figure 4-8).

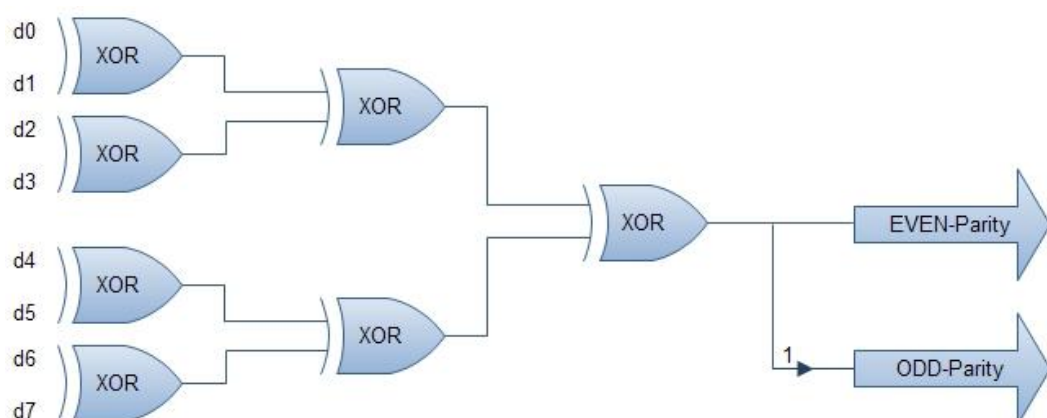


Figure 4-8: Parity determination of a byte by multiple XOR operations

b) LRC procedure

The XOR checksum and so called longitudinal redundancy check (LRC) can be calculated very simply and quickly. If the LRC is appended to the transmitted data, then a new LRC calculation incorporating all received data yields the checksum 00h. This permits a rapid verification of data integrity without the necessity of knowing the actual LRC sum (Figure 4-9).

The XOR checksum is generated by the recursive XOR gating of all the data bytes in a data block. Byte 1 is XOR gated with byte 2, the outcome of this gating is XOR gated with byte 3, and so on. If the LRC value is appended to a data block and transmitted with it, then a simple check for transmission errors can be performed in the receiver by generating an LRC from the data block + LRC byte. The result of this operation must always be zero; any other result indicates that transmission errors have occurred.

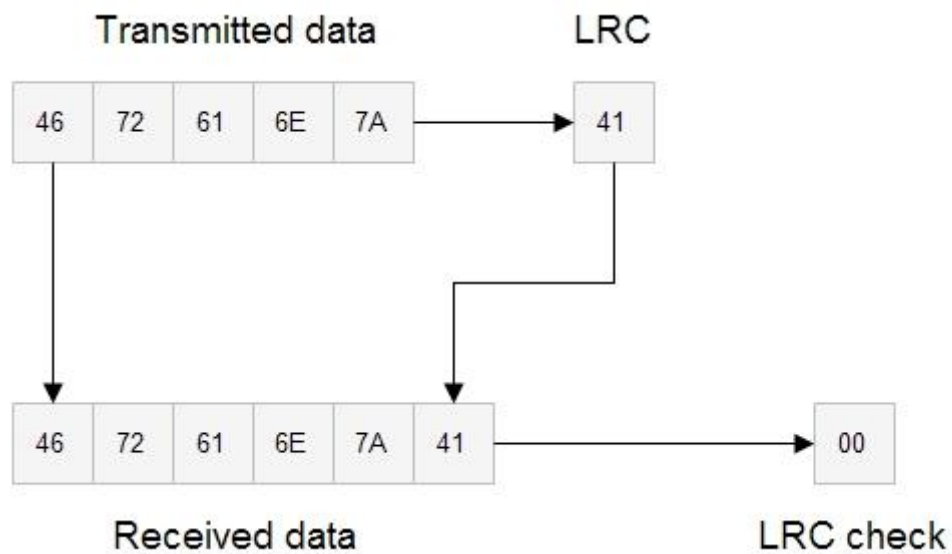


Figure 4-9: LRC checksum

Due to the simplicity of the algorithm, LRCs can be calculated very simply and quickly. However, LRCs are not very reliable because it is possible for multiple errors to cancel each other out and the check cannot detect whether bytes have been transposed within a data block. LRCs are primarily used for the rapid checking of very small data blocks.

c) CRC procedure

The CRC (cyclic redundancy check) procedure was originally used in disk drives and can generate a checksum that is reliable enough even for large data quantities. However, it is also excellently suited for error recognition in data transfer via wire-bound (telephone) or wireless interfaces (radio, RFID). The CRC procedure represents a highly reliable method of recognizing transmission errors, although it cannot correct errors.

As the name suggests, the calculation of the CRC is a cyclic procedure. Thus the calculation of a CRC value incorporates the CRC value of the data byte to be calculated plus the CRC values of all previous data bytes. Each individual byte in a data block is checked to obtain the CRC value for the data block as a whole.

If the CRC value that has just been calculated is appended to the end of the data block and a new CRC calculation performed, then the new CRC value obtained is zero. This particular feature of the CRC algorithm is exploited to detect errors in serial data transmission.

When a data block is transmitted, the CRC value of the data is calculated within the transmitter and this value is appended to the end of the data block and transmitted with it. The CRC value of the received data, including the appended CRC byte is calculated in the receiver. The result is always zero, unless there are transmissions errors in the received block. Checking for zero is a very easy method of analyzing the CRC checksum and avoids the costly process of comparing checksums. However, it is necessary to ensure that both CRC calculations start from the same initial value (Figure 4-10). If the CRC is appended to the transmitted data a repeated CRC calculation of all received data yields the checksum 0000h. This facilitates the rapid checking of data integrity without knowing the CRC total.

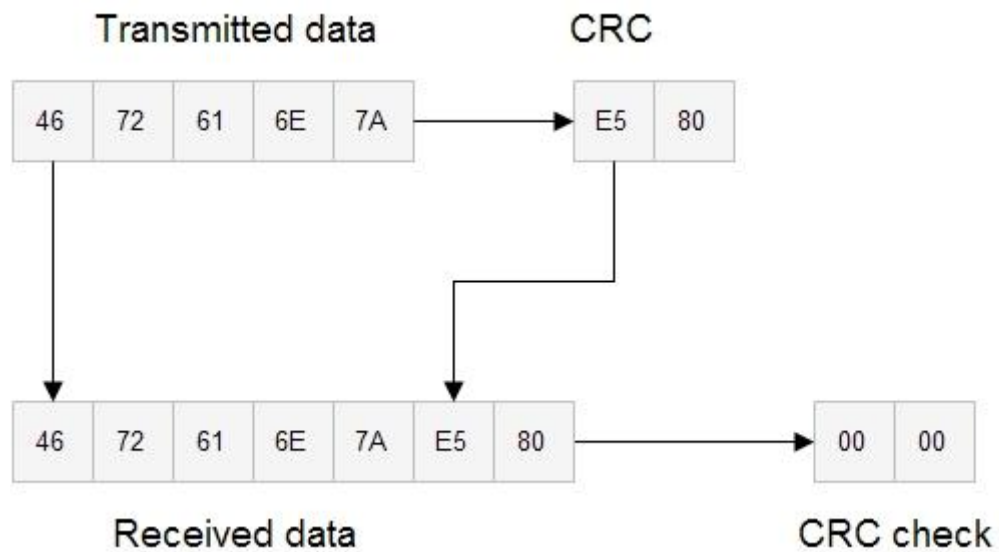


Figure 4-10: CRC checksum

The great advantage of CRCs is the reliability of error recognition that is achieved in a small number of operations even where multiple errors are present. A 16-bit CRC is suitable for checking the data integrity of data blocks up to 4 kilobytes in length – above this size performance falls dramatically. The data blocks transmitted in the electronic triage system are considerably shorter than 4 kilobytes, which means that 12- and 8-bit CRCs can also be used in addition to 16-bit CRCs.

4.6.5 Data Security Solutions

High security RFID systems such as the RFID triage system must have a defense against the following individual attacks:

- Unauthorized reading/writing of data in order to duplicate and/or modify data.
- The placing of a foreign data carrier within the interrogation zone of a reader with the intention of gaining unauthorized access to patient information
- Eavesdropping into radio communications and replaying the data, in order to imitate a genuine data (“replay and fraud”).

When selecting a suitable RFID system, consideration should be given to cryptological functions. The electronic triage system requires the incorporation of cryptological procedures to prevent unauthorized access to patient information.

a) Mutual Symmetrical Authentication

Mutual authentication between RFID reader and RFID tag is based upon the principle of three-pass mutual, in which both participants in the communication check the other party's knowledge of a secret (secret cryptological key).

In this procedure, all the transponders and receivers that form part of an application are in possession of the same secret cryptological key K (\rightarrow symmetrical procedure). When a transponder first enters the interrogation zone of a reader it cannot be assumed that the two participants in the communication belong to the same application. From the point of view of the reader, there is a need to protect the application from manipulation using falsified data. Likewise, on the part of the transponder there is a need to protect the stored data from authorized reading of overwriting.

The mutual authentication procedure begins with the reader sending a GET_CHALLENGE command to the transponder. A random number R_A is then generated in the transponder and sent back to the reader (response \rightarrow challenge-response procedure). The reader now generates a random number R_B . Using the common secret key K and a common key algorithm e_K , the reader calculates an encrypted data block (Token 1), which contains both random numbers and additional control data and sends this data block to the transponder.

$$\text{Token 1} = e_K (R_B \parallel R_A \parallel \text{ID}_A \parallel \text{Text1})$$

The received Token 1 is decrypted in the transponder and the random number R'_A contained in the plain text is compared to the previously transmitted R_A . If the two figures correspond, the transponder has confirmed that the two common keys correspond. Another random number R_{A2} is generated in the transponder and this is used to calculate an encrypted data block (Token 2), which also contains R_B and control data. Token 2 is sent from the transponder to the reader.

$$\text{Token 2} = e_K (R_{A2} \parallel R_B \parallel \text{Text2})$$

The reader decrypts Token 2 and checks whether R_B , which was sent previously, corresponds with R'_B , which has just been received. If the two figures correspond, then the reader is satisfied that the common key has been proven. Transponder and reader have thus ascertained that they belong to the same system and further communication between the two parties is thus legitimized (Figure 4-11).

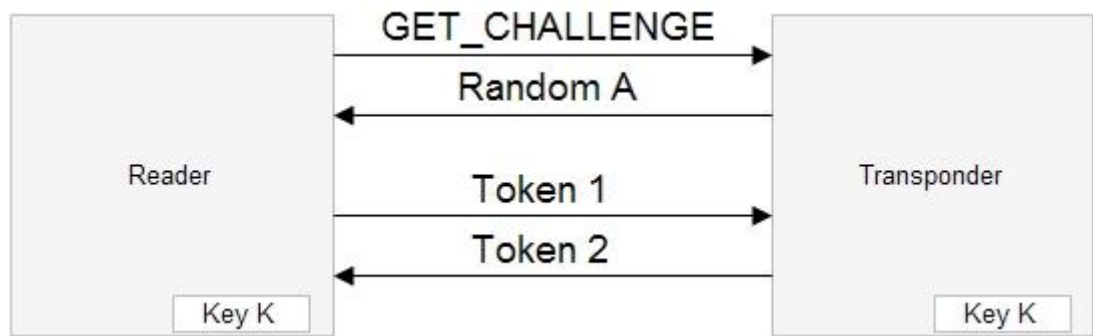


Figure 4-11: Mutual authentication procedure between transponder and reader

To sum up, the mutual authentication procedure has the following advantages:

- The secret keys are never transmitted over the airwaves, only encrypted random numbers are transmitted.
- Two random numbers are always encrypted simultaneously. That rules out the possibility of performing an inverse transformation using R_A to obtain token with the aim of calculating the secret key.
- The token can be encrypted using any algorithm.
- The strict use of random numbers from two independent sources (transponder, reader) means that recording an authentication sequence for playback at a later date (replay attack) would fail.
- A random key (session key) can be calculated from the random numbers generated, in order to cryptologically secure the subsequent data transmission.

b) Authentication Using Derived Keys

One disadvantage of the authentication procedure described in the previous section is that all transponders belonging to an application are secured using an identical cryptological key K . For applications that involve vast quantities of transponders this represents a potential source of danger. Because such transponders are accessible to everyone in uncontrolled numbers, the small probability that the key for a transponder will be discovered must be taken into account. If this occurred, the procedure described above would be totally open to manipulation.

A significant improvement on the authentication procedure described can be achieved by securing each transponder with a different cryptological key. To achieve this, the serial number of each transponder is read out during its production. A key K_X is calculated (\rightarrow derived) using a cryptological algorithm and a master key K_M , and the transponder is thus initialized. Each transponder thus receives a key linked to its own ID number and the master key K_M .

The mutual authentication begins by the reader requesting the ID number of the transponder (Figure 4-12). In a special security module in the reader, the SAM (security authentication module), the transponder's specific key is calculated using the master key K_M , so that this can be used to initiate the authentication procedure. The SAM normally takes the form of a smart card with contacts incorporating a cryptoprocessor, which means that the stored master key can never be read.

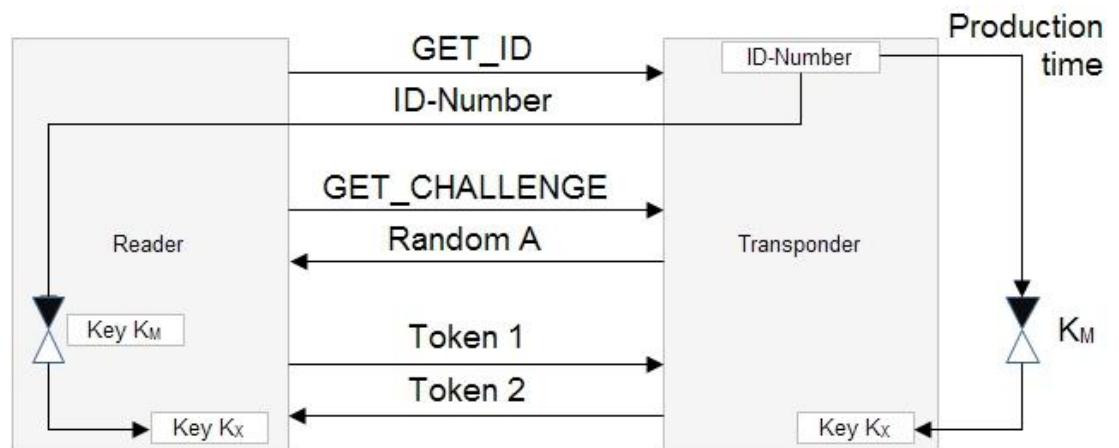


Figure 4-12: Authentication procedure based upon derived keys

c) Encrypted Data Transfer

One of the previous sections (data integrity) described methods of dealing with interference caused by physical effects during data transmission. Let us now extend this model to a potential attacker. We can differentiate between two basic types of attack. Attacker 1 behaves passively and tries to eavesdrop on the transmission to discover confidential information for wrongful purposes. Attacker 2, on the other hand, behaves actively to manipulate the transmitted data and manipulate it to his benefit (Figure 4-13).

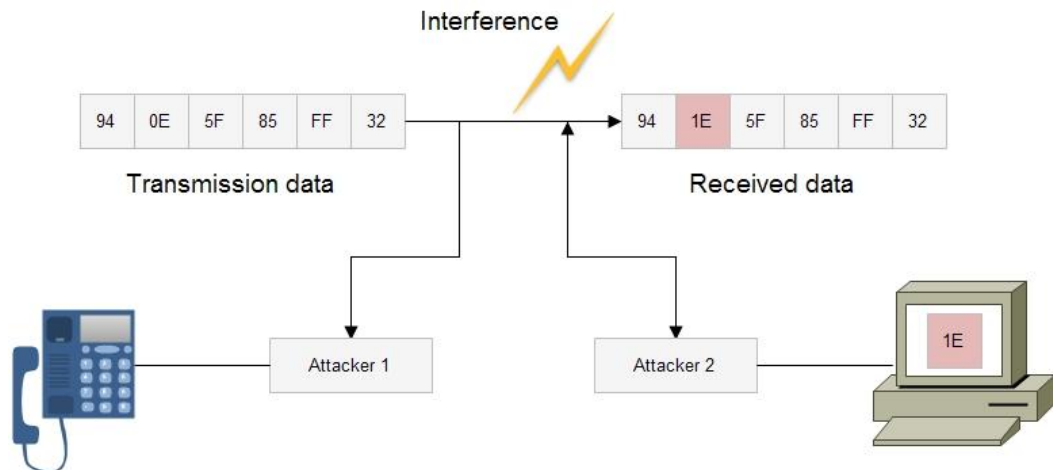


Figure 4-13: Attempted attacks on a data transmission

Cryptological procedures are used to protect against both passive and active attacks. To achieve this, the transmitted data (plain text) can be altered (encrypted) prior to transmission so that a potential attacker can no longer draw conclusions about the actual content of the message (plain text).

Encrypted data transmission always takes place according to the same pattern. The transmission data (plain text) is transformed into cipher data (cipher text) (\rightarrow encryption, ciphering) using a secret key K and a secret algorithm. Without knowing the encryption algorithm and the secret key K a potential attacker is unable to interpret the recorded data. It is not possible to recreate the transmission data from the cipher data.

The cipher data is transformed back to its original form in the receiver using the secret key K' and the secret algorithm (\rightarrow decryption, deciphering) (Figure 4-14).

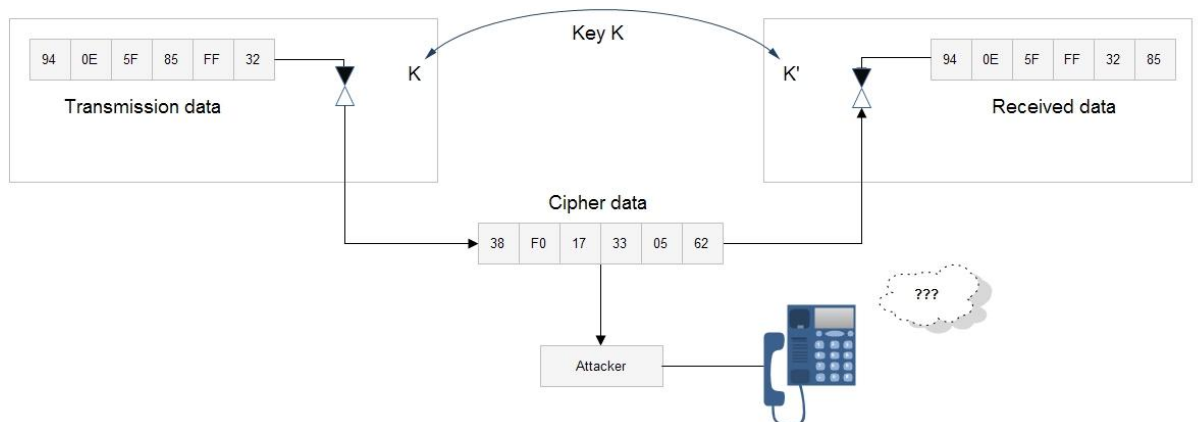


Figure 4-14: Encrypting the transmitted

If the keys K for ciphering and K' for deciphering are identical ($K = K'$) or in a direct relationship to each other, the procedure is a symmetrical key procedure. If knowledge of the key K is irrelevant to the deciphering process, the procedure is an asymmetrical key procedure. RFID systems have for a long time used only symmetrical procedures, therefore we will not describe other procedures in further detail here.

If each character is individually encrypted prior to transmission, the procedure is known as sequential ciphering (or stream ciphering). If, on the other hand several characters are incorporated into a block then we talk of a block cipher. Because block ciphers are generally very calculation intensive, they play a less important role in RFID systems. Therefore the emphasis is placed on sequential ciphers in what follows.

A fundamental problem of all cryptological procedures is the secure distribution of the secret key K , which must be known by the authorized communication participants prior to the start of the data transfer procedure.

d) Stream Cipher

Sequential ciphers or stream ciphers are encryption algorithms in which the sequence of plaintext characters is encrypted sequentially using a different function for every step. The ideal realization of a stream cipher is the so-called one-time pad.

In this procedure a random key K is generated, prior to the transmission of encrypted data and this key is made available to both parties (Figure 4-15). The key sequence is linked with the plaintext sequence by the addition of characters or using XOR gating. The random sequence used as a key must be at least as long as the message to be encrypted, because periodic repetition of a typically short key in relation to the plaintext would permit cryptanalysis and thus an attack on the transmission. Furthermore, the key may only be used once, which means that an extremely high level of security is required for the secure distribution of keys. Stream ciphering in this form is completely impractical for RFID systems.

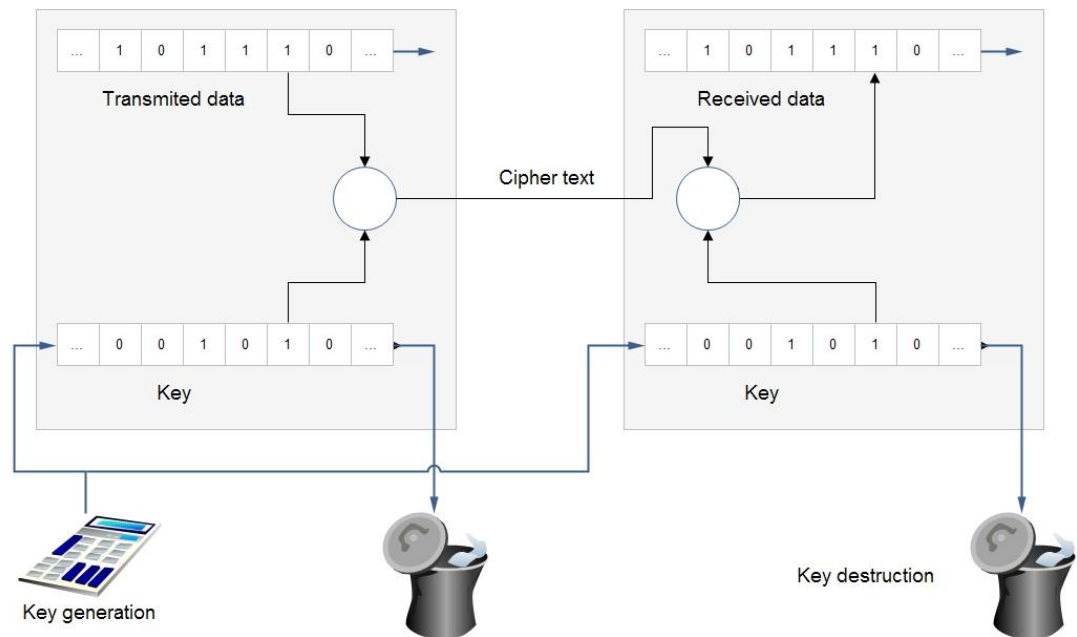


Figure 4-15: Stream cipher realized by one-time-pad

4.6.6 Disposal of RFID Tags

Depending on the different law regularizations in each country the disposal of the RFID tags and the patient information in electronic media cannot be generalized. All patient information records must be retained for a certain time, irrespective of the patient's age or health status at that time. Records must be retained for the full retention period required by state laws or local hospital policy. After this time period the RFID tags and the electronic patient data can be disposed.

Patient information in electronic media may be used for patient care or research until the retention requirements have been met. Emergency departments determine the criteria for inactive record status in their areas, based on need for the records and available storage space. Storage facilities for these records must meet certain security requirements providing a secure safekeeping of patient information.

4.7 System Architecture of RFID Triage

The electronic triage system consists of the following components (Figure 4-2):

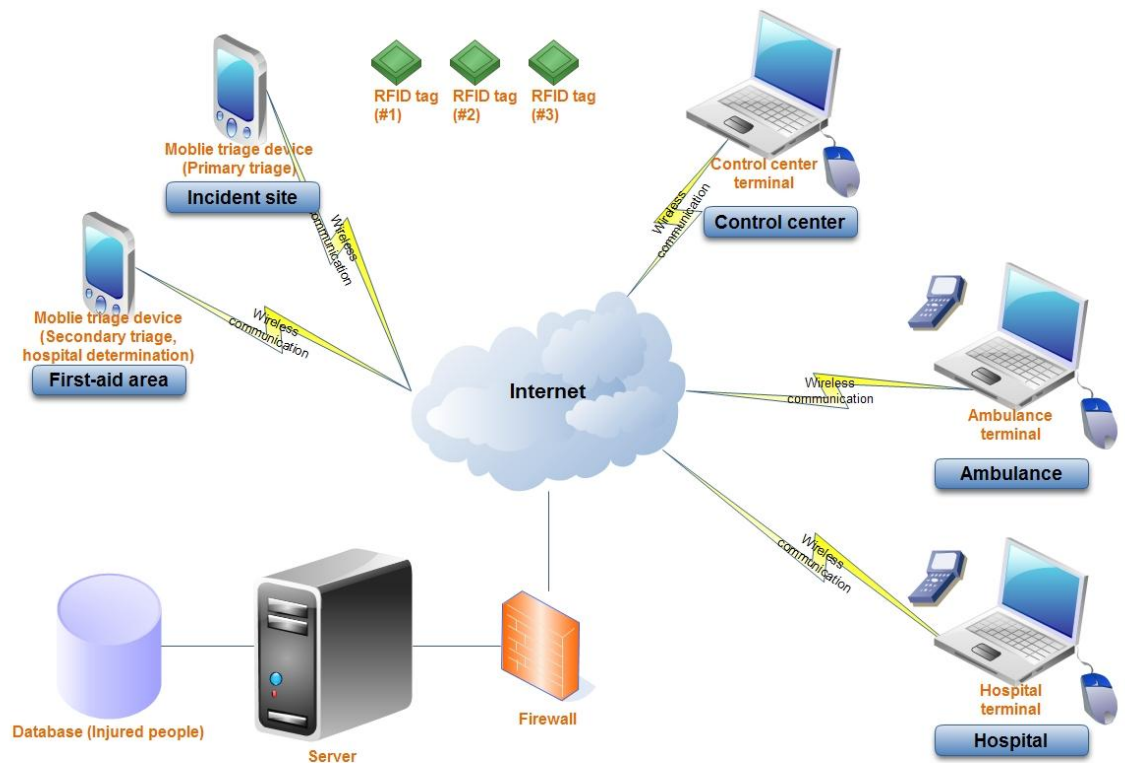


Figure 0-1: System and network architecture [InSo08]

- a) **Triage Tag:** Each RFID tag has a unique ID in the system. The RFID tag has re-writable memory of 1 kb and uses wireless communication in the frequency of 13.56 MHz. Besides that there is the conventional triage tag with input forms for the information of the injured person. [EpSp09]
- b) **Mobile Triage Device:** The mobile triage device is a handheld scanner carried by emergency personnel and used for information collection. Emergency personnel use the mobile triage device designed for the usage in the first three phases. [InSo08]
 - primary triage
 - secondary triage
 - hospital determination
- c) **Control Center Terminal:** A notebook PC equipped with a wireless communication interface should be placed in the control center. From this unit the whole triage is monitored and controlled. Emergency personnel can browse the information collected by the mobile triage devices and stored on the server. [InSo08]

- d) Ambulance Terminal: A notebook PC equipped with an RFID reader and a wireless communication interface is placed in each ambulance or transport vehicle. It is possible for the emergency personnel to edit or add the patient information using keyboard and mouse. [InSo08]
- e) Hospital Terminal: A notebook PC equipped with an RFID reader and wireless communication interface like the Ambulance Terminal. The electronic triage software can be integrated into existing IT infrastructure of the hospital. [InSo08]
- f) Server: The information collected by the mobile triage devices, the ambulance terminal and the hospital terminal is stored on one central server. This server is placed away from the incident site being protected by a firewall and having a database for the storage of injured people information. The server responds to the incoming request from the control center terminal. The server must keep the information from an injured person up-to-date, because the mobile devices and terminals can change this information anytime. [InSo08]

4.8 Near Field Communication (NFC) - Triage

In order to improve the efficiency of the Electronic Triage System, considering the defined requirements, we decided to extend the RFID Triage with an additional technology – Near Field Communication (NFC).

NFC is a wireless data interface between devices. Comparable technologies to NFC are Bluetooth and Infrared. NFC has characteristics being interesting in relation to RFID systems. Data transmission between two NFC interfaces uses high-frequency magnetic alternating fields in the frequency range of 13.56 MHz. The name near-field communication derives from the fact, that the maximum communication range typical for NFC data transmission is 10 centimeters which means that the dedicated communication counterpart is located in the near-field of the transmitter antenna.

The physical principle of data transmission between two NFC interfaces is shown in Figure 4-17. The NFC interface has a 13.56 MHz transmitter and a 13.56 MHz receiver that are alternately connected to the antenna which is designed as a large-surface coil or conductor loop. The NFC interfaces alternately emit magnetic fields for data transmission. [FiK110]

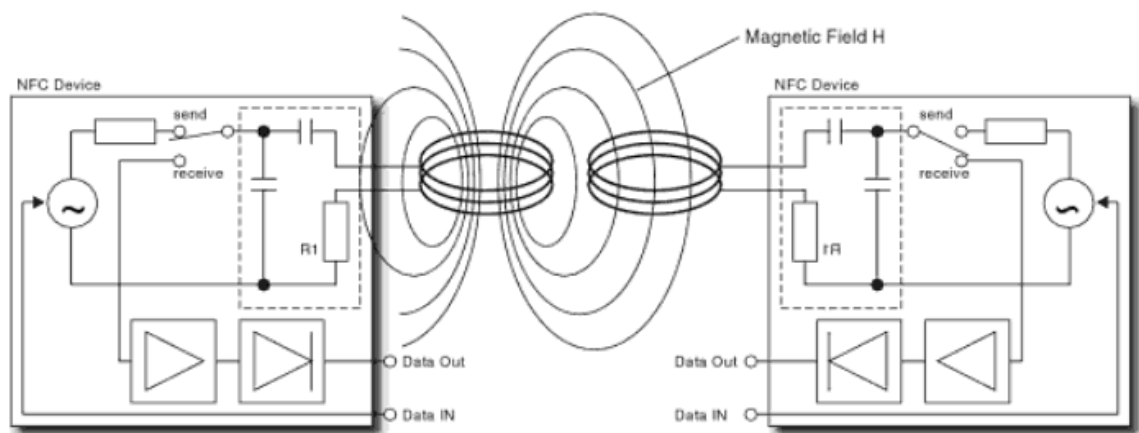


Figure 0-2: NFC Data transmission [FiK110]

The individual NFC interface acts as NFC initiator (master device) or an NFC target (slave device) during the communication between two NFC interfaces. The NFC initiator always starts the communication. There are two different operational modes in NFC communication; the active mode and the passive mode.

4.8.1 Differences between NFC and RFID

The main differences between NFC (Near-Field Communication) and RFID (Radio Frequency Identification) are:

- NFC is an extension to RFID technology
- RFID is capable of accepting and transmitting beyond a few meters while NFC is restricted to within 10 centimeters
- RFID has a wide range of uses while NFC is usually used in cases where security is needed
- Some mobile phones are equipped with NFC

NFC is a subset of RFID that limits the range of communication to within 10 centimeters. RFID is a tagging technology gaining widespread attention due to the offered advantages compared to current tagging technologies like barcodes. RFID uses radio frequency waves that are either active, passive, or a combination of both. Active RFID tags have a power source that helping extend their range while passive devices rely on the energy receiving it from the interrogating device to send its own information. One of the advantages of RFID is the small size of the tag making it possible to be used with small products or to be hidden away. Another advantage is that it doesn't need a direct line of sight for the information to be read. These advantages are desirable in an electronic triage system where speed is very essential.

RF waves (and RFID) are used to transmit information across very long distances especially when powered. This kind of range is requested in certain applications like animal tracking where the animal being tracked might move a couple of kilometers but it is not requested in an application like the electronic triage system. Besides that it is possible to receive the information and clone it into another tag. This is where the advantages of NFC become useful for the electronic triage system.

Objects that are tagged with NFC are usually passive because they don't require that much range. Some have even employed shielding to further reduce the possibility for others to read the information. The shielding is necessary because even non-powered tags can still be read over 10 meters away with specialized equipment. Some mobile phones are equipped with NFC being used as a kind of cash card.

4.8.2 NFC Applications

NFC is able to provide contactless communication over short ranges (typically up to about 10 cm) providing connection by placing the two devices requiring connection close together. As no physical connectors are used with NFC near field communication, the connection does not suffer problems of contact wear, corrosion and dirt.

NFC technology has evolved from a combination of contactless identification and inter-connection technologies including RFID. Two electronic devices are able to communicate by bringing them close together and this greatly simplifies the issues of identification and security, making it far easier to exchange information. It is expected that NFC technology will allow the complex set-up procedures required for some longer range technologies to be avoided.

There is a variety of applications where NFC technology is used:

- PDA and mobile phone
- PC
- Point-of-sale equipment
- Vending machine
- Parking meter
- ATM (asynchronous transfer mode)
- Applications in the house or office (e.g. garage doors)

NFC near field communication is ideally placed to provide a link with the contactless smart card technology being already used for ticketing and payment applications. It is compatible with the existing standards that have been set in place so it is quite possible that NFC enabled devices could be used for these applications as well.

There are many other applications for near field communications which could include general downloading data from digital cameras or mobile phones, as well as any other data communication required between two devices.

NFC technology has many of its roots in the RFID business. Some of the basic ideas came directly from RFID work that had been previously undertaken. Sony and Phillips have taken the lead and jointly developed the technology. This technology follows on from their proprietary smart card protocols and can be seen as an initiative to move forward the contact-less ticketing and payment applications that are seen as the next stage in this market.

4.8.3 Modes of Operation

a) Active Mode

In order to transmit data between two NFC interfaces in active mode, at first one of the NFC interfaces activates its transmitter and thus works as the NFC initiator. The high-frequency current that flows in the antenna induces an alternating magnetic field H which spreads around the antenna loop. Part of the induced magnetic field moves through the antenna loop of the other NFC interface which is located close by. Then a voltage U is induced in the antenna loop and can be detected by the receiver of the other NFC interface. If the NFC interface receives signals and the corresponding commands of an NFC initiator, this NFC interface automatically adopts the roll of an NFC target. [FiK110]

For data transmission between the NFC interfaces, the amplitude of the emitted magnetic alternating field is modulated (ASK modulation), similar to the data transmission between RFID reader and transponder. However, the difference between an NFC target in active mode and an RFID transponder consist in that the magnetic alternating field has to supply the transponder with power in order to operate the microchip. As opposed to this, the electronic device containing the NFC interface supplies the interface with power. [FiK110]

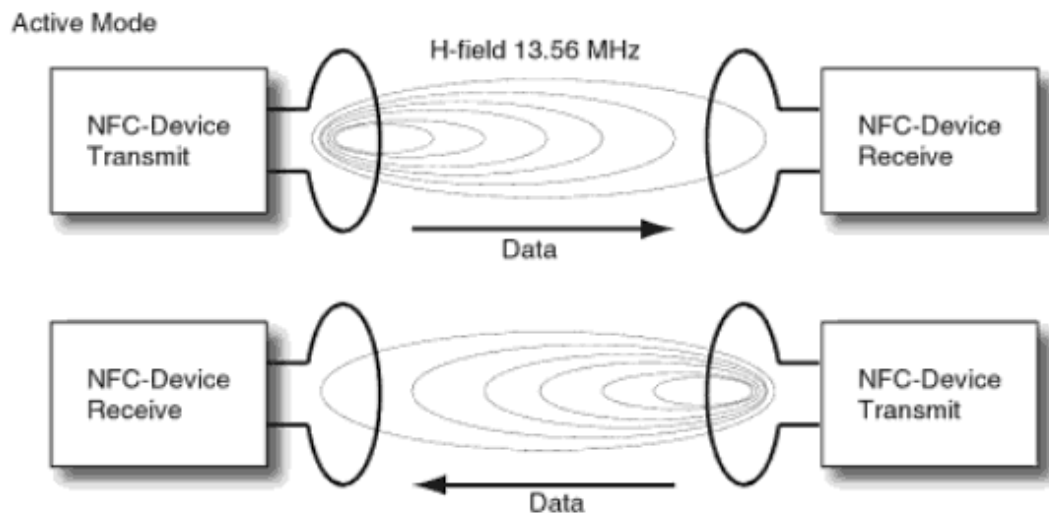


Figure 0-3: NFC – Active Mode [FiK110]

In order to send data from the NFC target to the NFC initiator the transmission direction is reversed. This means that the NFC initiator switches to receiving mode and the NFC target activates the transmitter. Both NFC interfaces alternately induce magnetic fields where data is transmitted from transmitter to receiver only. (Figure 4-18)

b) Passive Mode

In the passive mode, too, the NFC initiator induces a magnetic alternating field for transmitting data to the NFC target. The field's amplitude is modulated in line with the pulse of the data to be transmitted (ASK modulation). However, after having transmitted a data block, the field is not interrupted, but continues to be emitted in an unmodulated way. The NFC target now is able to transmit data to the NFC initiator by generating a load modulation. The load modulation method is also known from RFID systems. [FiK110]

Using this method for NFC interfaces provides a number of advantages and interesting options for practical operation. Thus the different roles of the two NFC interfaces within the NFC communication can be negotiated and changed, at any time. An NFC interface with weak power supply, e.g. with a low-capacity battery, can negotiate and adopt the role of the NFC target in order to save power by transmitting data via load modulation. [FiK110]

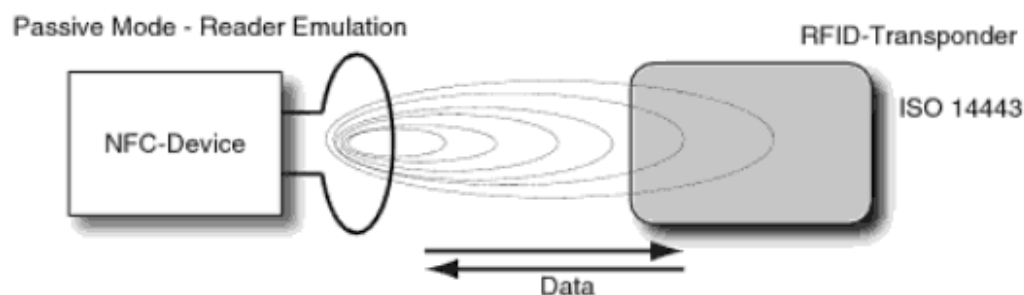


Figure 0-4: NFC – Passive Mode – Reader Emulation [FiK110]

The NFC (target) interface is also able to establish, in addition to other NFC interfaces, the communication to compatible passive transponders that the NFC target supplies with power. This can be e.g. an RFID transponder that transmits data to the NFC interface via load modulation. This option enables electronic devices equipped with NFC interfaces, such as NFC mobile phones, to read and write on different transponders such as smart labels or e-tickets. As the NFC interface in this case behaves similar to an RFID reader, this option is also called “reader mode” or “reader-emulation mode”. (Figure 4-19)

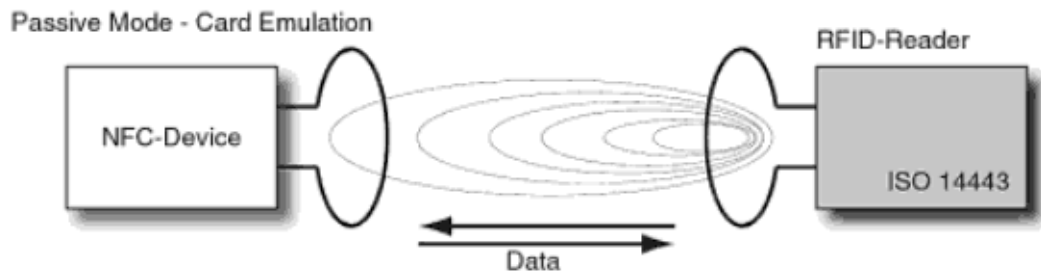


Figure 0-5: NFC – Passive Mode – Card Emulation [FiKI10]

An NFC interface is also able to communicate with a close located and compatible RFID reader. The NFC interface adopts the roll of an NFC target and can transmit data to the reader using load modulation. This option enables RFID readers to exchange data with an electronic device with NFC interface, such as NFC mobile phones. From the reader's perspective, the electronic device behaves like a contactless smart card; this option is also called "card mode" or "card-emulation mode". (Figure 4-20)

The card-emulation mode is the relevant option for the electronic triage system providing more security during the triage read/write communication shown in the following chapters.

4.8.4 Communication Modes

The NFC forum defines the following three communication modes:

a) Peer to peer

This mode supports device to device link-level communication. This mode of NFC communication is not supported by the Contactless Communication API.

b) Read / Write

This mode allows applications to transfer data in an NFC Forum-defined message format. It should be noted that this mode is not secure. It is also necessary to note that this mode is supported the Contactless Communication API.

c) NFC card emulation

This mode enables the NFC device to behave as a standard Smartcard. In this mode, data transfer is secure and the mode is also supported by the Contactless Communication API.

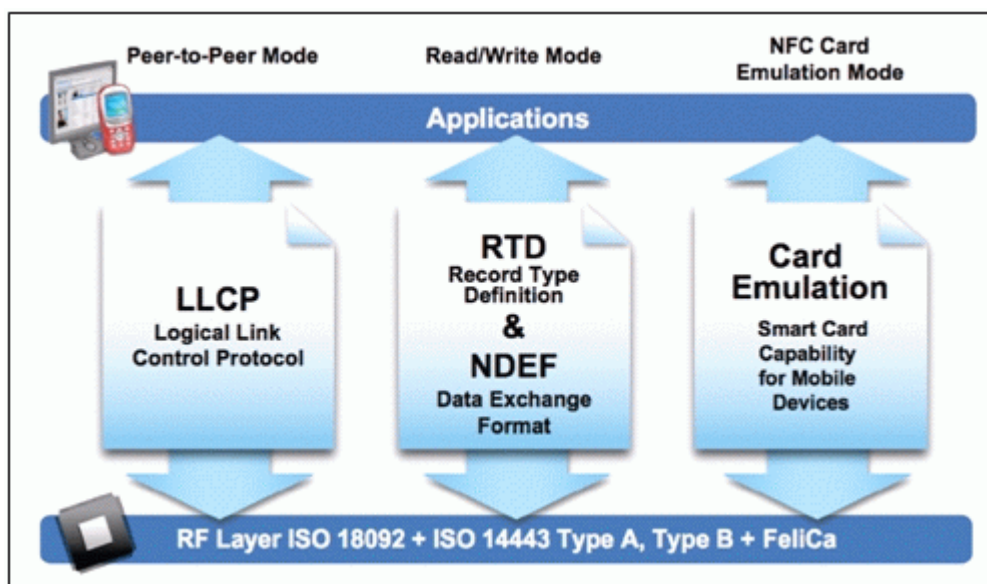


Figure 0-6: NFC Communication Modes (by courtesy of [NeFe10])

NFC is a standard, and is ISO standards-based. The ISO 14443 Type A and Type B standards + FeliCa is a four-part international standard for contact-less smart cards operating at 13.56 MHz in close proximity with a reader antenna. The ISO 18092 standard defines communication modes for NFC Interface and Protocol. [SuDe10]

4.8.5 The Contactless Communication API

The Contactless Communication API Java specification, led by Nokia and defined under the Java Community Process as JSR-257, defines a set of APIs for proximity, contactless-based communication. [SuDe10] The API consists of five packages for the communication with RFID tags, NDEF (NFC Data Exchange Format) formatted data tags, external smartcards and for reading and generating visual tags. It is possible to discover and exchange data with contactless targets such as NDEF tags, RFID tags, and external smartcards.

Figure 4-22 shows the elements of a typical mobile Java application (MIDlet) that uses the Contactless Communication API:

- The Java Runtime with JSR-257 implementation
- The MIDlet application running on a handset
- RFID/NFC transponder, controllers, and baseband
- SIM card, secure and external elements

External readers include contactless payment readers in Point of Sale stations, ticketing systems on transportation systems, external radio, visual tags such as NFC, RFID and barcodes or Smartcards.

Secure elements (SE) can be internal or external elements; example of a secure element is a Java Card-based smartcard. MIDlets can access secure elements by using the Security and Trust Services API (SATSA), and/or the Contactless Communication API (JSR 257). External readers access internal secure elements directly via the RFID circuitry (using the Card Emulation mode). [SuDe10]

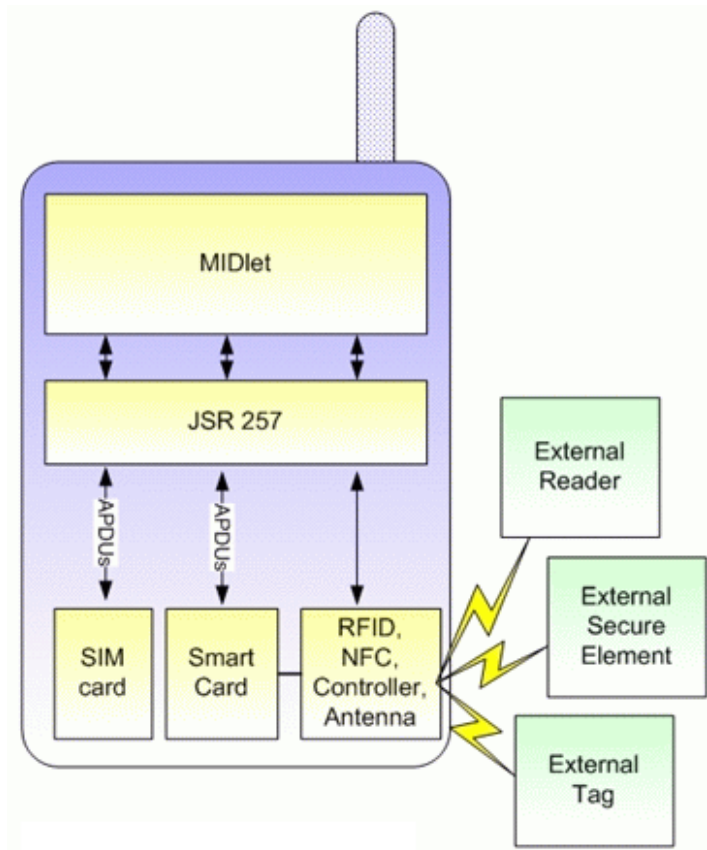


Figure 0-7: Anatomy of Contactless Communication API (by courtesy of [EnOr10])

4.8.6 Secure Element (SE)

In card emulation mode, a secure element (SE) on the device communicates and transacts with an external reader over RFID hardware. (Figure 4-23)

- 1) The internal security element interacts with an external reader
- 2) The application (MIDlet) is notified when the external reader has been detected
- 3) If needed, the application communicates with the secure element, using the Contactless Communication API ISO14443 connection interface, or SATSA if available

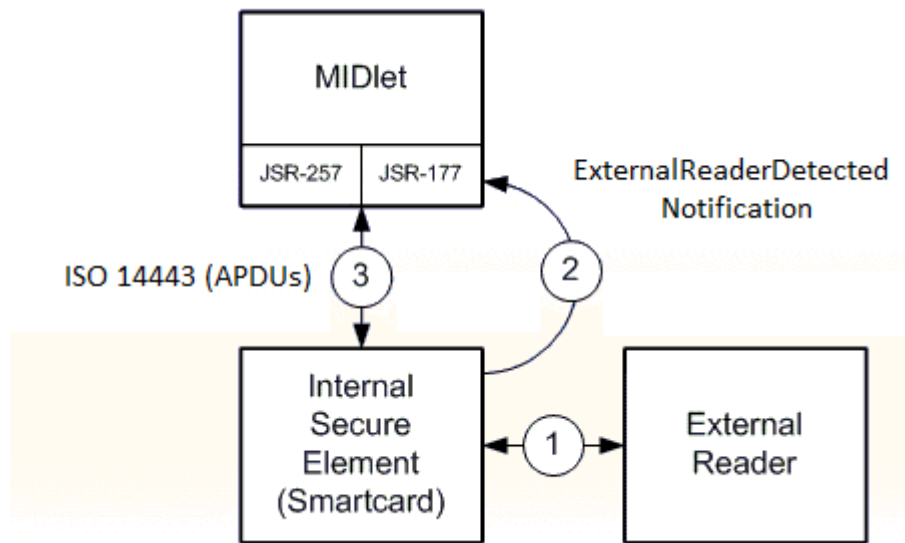


Figure 0-8: Card Emulation Activity Notifications (by courtesy of [EnOr10])

The communication between secure element and the external readers is transparent to the application itself using APDU commands similarly to how Java Cards communicate with external readers. The communication between the application and the secure element requires internal knowledge of the secure applet within the secure element. [SuDe10]

Figure 4-24 illustrates the typical relationships of a Java Card application (in this case from the perspective of MIDlet playing the role of the "reader"), and the Secure Elements (playing the role of the "card-side") showing a contactless communication application scenario.

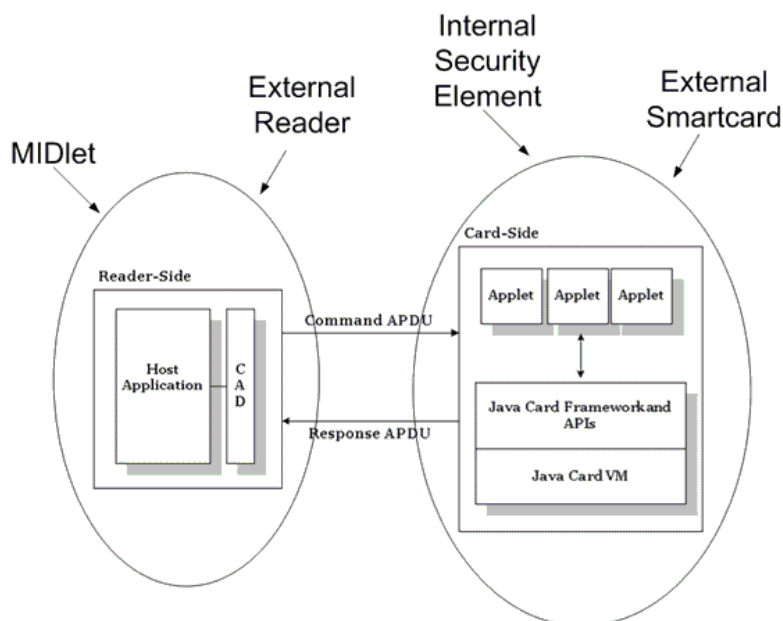


Figure 0-9: Typical Elements of a Java Card Application (by courtesy of [EnOr10])

On a Contactless (NFC) handset, the left side could be an internal reader, the MIDlet itself, or an external reader (via NFC Card Emulation Mode). The right-side, the "card", could be an internal or an external secure element, which is accessible via SATSA or JSR-257, or over RFID hardware. [SuDe10] This scenario is relevant for the electronic triage system with the Mobile Triage Device on the left side and the Triage Tags on the right side.

As mentioned above the Contactless Communication API consists of five packages. Some packages are mandatory and some optional which all are included in the API implementation of Nokia called Software Development Kit for Nokia 6131 NFC (Nokia 6131 NFC SDK).

4.8.7 Impact on the Requirements of the Electronic Triage System

Confidentiality was mentioned as one of the system requirements of the Electronic Triage. Hence there is a need for durable security and confidentiality of sensitive applications and data downloaded to and stored on an NFC enabled device for performing contactless transactions. The component in the Electronic Triage System providing the security and confidentiality is referred to as a Secure Element (SE).

Besides adding power and functionality, there is a third method of enhancing RFID: combining the tag and reader into one device. This offers two-way communication between both devices; each device can act as either a tag or a reader.

Especially for mobile equipment, this can be a useful feature. Sometimes the PDA acts like a tag, communicating with existing readers. On other moments the PDA can read RFID tags itself. [LiGr07]

In the following section we will elaborate the different impacts of NFC on the Electronic Triage System:

a) Impact of the short range of NFC

NFC is designed, as the name already indicates, for very short range (10 cm) wireless communication. Its purpose is to securely transport small amounts of data mainly for configuration purposes or initiating actions and/or communication. Long-range RFID tag technology, according to the Alliance and other industry watchers, should be used for tracking products, not people. [LiGr07]

Applying NFC to the Electronic Triage System would practically mean that emergency personnel could not read the patient information from the RFID Triage Tag by the Mo-

mobile Triage Device from a distance more than 10 centimeters. That would mean that they would have to put the Mobile Triage Device close to the Triage Tag and start the read/write operations.

This process decreases the probability that the Mobile Triage Device comes to a reading conflict by entering more than one Triage Tags the antenna field of NFC.

b) Impact of the Secure Element (SE)

The implementation of NFC technology and consequently the application of a Secure Element (SE) affect the design of the devices used in the Electronic Triage System.

The Mobile Triage Device additionally has to be equipped with an NFC interface. This interface communicates with the RFID Triage Tag using the Passive Mode – Reader Emulation. Besides that the interface communicates with the RFID Reader using Passive Mode – Card Emulation.

For the communication with the RFID Triage Tag the SE is interposed. This means that the SE is playing the role of the Triage Tag which implicates that there must be an application playing the role of the reader.

The application (analogous to mobile Java Application - MIDlet) is implemented on the Mobile Triage Device working as intermediary between the screen application running of the Mobile Triage Device and the SE.

c) Impact on the Security

In former sections we analyzed various security aspects of the Electronic Triage System. In the following there are different threats mentioned and the solutions of the NFC technology.

- Data Corruption and Data Modification:

NFC devices can counter this attack because they can check the RF field, while they are transmitting data. The power which is needed to corrupt the data is significantly bigger, than the power which can be detected by the NFC device. Therefore every data corruption attack is detectable.

- Data Insertion:

One possible countermeasure is that the answering device answers with no delay. In this case the attacker cannot be faster than the correct device. The attacker can be as fast as the correct device, but if two devices answer at the same time no correct data is received. Another possible countermeasure is listening by the answering device to the channel during the time it is open and the starting point of the transmission. The device could then detect an attacker, who wants to insert data.

- Eavesdropping:

Establishing a secure channel between two NFC devices is the best approach to protect against eavesdropping. A standard key agreement protocol (e.g. Diffie-Hellmann) based on RSA could be applied to establish a shared secret between two devices.

The shared secret can then be used to derive a symmetric key like 3DES or AES, which is then used for the secure channel providing confidentiality, integrity, and authenticity of the transmitted data. [HaBr10]

- d) Impact on the robustness

NFC offers the advantage to be robust in harsh environments. This means that e.g. metal or moisture within the antenna field does not interrupt safe data transmission remaining unaffected by electronic interference.

This is an important characteristic in consideration of the fact that the Electronic Triage System is thought to come into operation in barely predictable disaster situations.

5 Implementation

This chapter describes the implementation of the Triage Interface software running on the mobile triage devices, the ambulance terminal and the hospital terminal. The Fosstrak framework simulating RFID hardware (tag, reader) will be used for this implementation. Besides that this chapter describes the components of this framework and their collaboration between each other and with the implemented Triage Interface.

5.1 Fosstrak Framework

The Fosstrak project is free and open source software based on Java simulating the RFID technology. The Fosstrak framework provides an infrastructure which manages readers, filters and aggregates raw RFID data and also facilitates data exchange among the components. The Fosstrak HAL project allows simulating RFID readers with more antennas and creating RFID tags. By dragging the tags over the reader antenna the user can simulate the reading of an RFID tag. The central component of the Fosstrak project used by the HAL simulator is the Fosstrak RFID Reader which can identify RFID tags.

5.2 Fosstrak Reader

The Fosstrak RFID Reader consists of 3 main components:

- a) Client (reader-rp-client)
The Reader RP Client allows communication with a Reader Protocol compliant reader via a graphical user interface.
- b) Proxy (reader-rp-proxy)
The Reader RP Proxy allows communication with a Reader Protocol compliant reader within a Java application.
- c) Core (reader-rprm-core)
The Reader RP/RM Core allows simulation of a Reader Protocol compliant reader.

The goal of Fosstrak Reader is to provide an example implementation of the EPCglobal Reader Protocol specifications. Besides, the Fosstrak Reader supports the EPCglobal Reader Management.

The backend of the Fosstrak Reader is the Fosstrak HAL (Hardware Abstraction Layer) project controlling and managing simulators or readers over the Reader Protocol. These readers and simulators must implement the HardwareAbstraction interface.

The Reader Core (reader-rprm-core) module contains the reader implementation, but the Fosstrak Reader project contains two other modules with interfaces to control a Reader Protocol compliant reader.

The Reader Proxy (reader-rp-proxy) module contains a library to control a reader with a Java application. This application uses the Reader Protocol for receiving reader notifications.

The Reader Client (reader-rp-client) module contains a graphical client to configure a reader. This client uses the Reader Protocol and has two versions of an event sink that display information about events reported by the reader through a notification channel.

Figure 5-1 gives an overview of the architecture of the Fosstrak Reader.

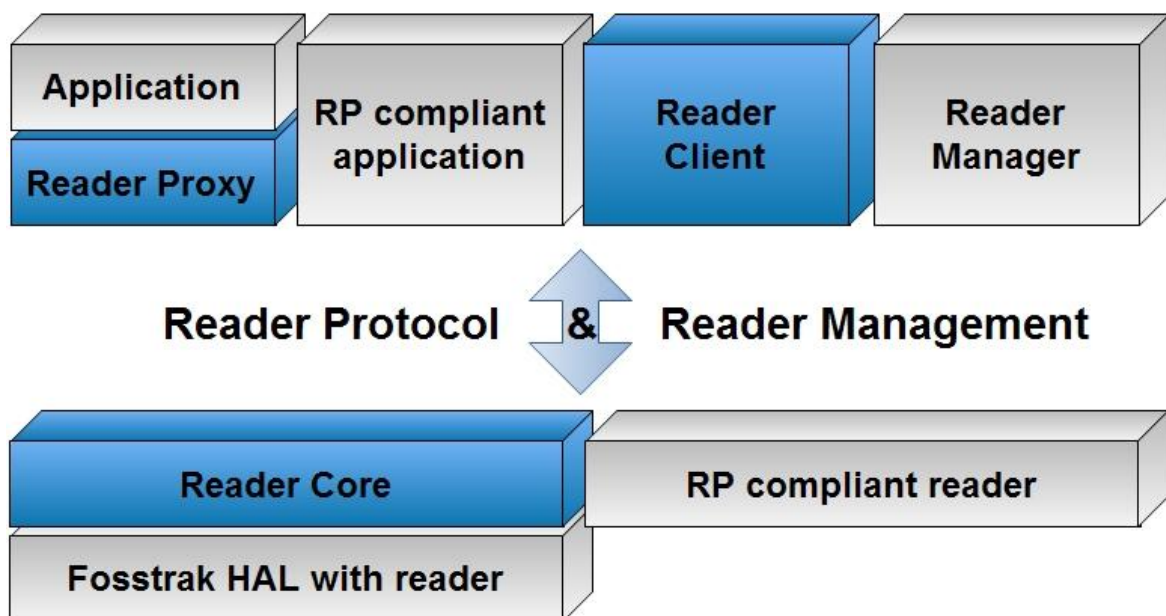


Figure 5-1: Fosstrak Reader architecture

Fosstrak HAL is the backend of the Reader Core and can be used and controlled like any other Reader Protocol compliant reader, e.g., by the Reader Proxy, Reader Client or an application supporting the Reader Protocol.

The Reader Proxy does not support Reader Management over SNMP, but it can be used by a Java application as a library which can easily control a reader over the EPCglobal Reader Protocol. The Reader Proxy shares code of the Reader Core module.

The Reader Client does not support Reader Management over SNMP too, but is a stand-alone application to control any Reader Protocol compliant reader using a graphical user interface. This GUI allows sending commands to the reader and receiving the response.

5.2.1 Reader RP/RM Core

The Reader RP/RM Core implements the EPCglobal Reader Protocol Version 1.1 and Reader Management Version 1.0 in Java. The elements of the implemented protocol include:

- Transport Binding (TCP and HTTP)
- Message Binding (XML and Text)
- Synchronous and Asynchronous Messaging (Notification Channels)
- Triggers
- Data Selectors
- SNMP Binding of Reader Management 1.0

Field of application

- Simulation of a single reader through a graphical user interface using the Fosstrak HAL Simulator module.
- Simulation of a network of hundred of readers using the simulation framework of the Fosstrak HAL project.
- Embedding of the Fosstrak Reader implementation into a reader.
- Turning a reader which does not implement the EPCglobal Reader Protocol itself into a compliant reader through deployment of the appropriate Fosstrak HAL module and this Reader Core module as a Reader Protocol compliant proxy together with the reader.

Fosstrak HAL Simulator

The Fosstrak HAL project defines a hardware abstraction interface that is used to access RFID readers and implements it for various reader devices and reader simulators. The goal is to provide a common interface and wrappers to uniformly access various RFID readers. Fosstrak HAL is used by the Fosstrak Reader.

The main objectives of the Fosstrak HAL project are:

- Different readers can be accessed over a uniform graphical user interface

- RFID tags can be created and the reading of an RFID tag by an RFID reader can be simulated

The Fosstrak HAL project consists of modules shown on the Figure 5-2:

- Hardware abstraction interface
- A module for hardware abstraction interface implemented with simulators
- A module for each implementation of the hardware abstraction interface

Fosstrak HAL solves the problem of accessing each reader through its own proprietary protocol by providing one single interface to access all the implemented readers. Thus the application does not need to change code to a specific reader but simply uses the HardwareAbstraction interface to communicate with the RFID reader.

RFID readers which are not implemented in the Fosstrak HAL project can be added as a new module by implementing the HardwareAbstraction interface and communicating with the reader over the corresponding protocol.

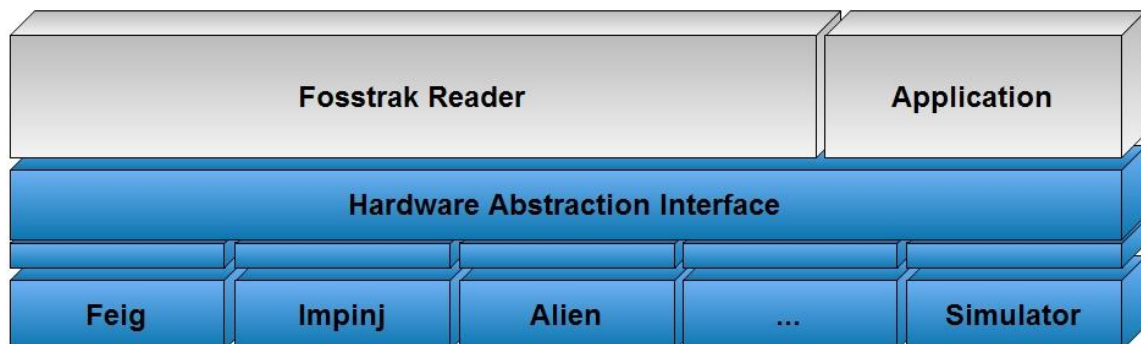


Figure 5-2: The Fosstrak HAL implementation

5.2.2 Reader RP Proxy

The Reader RP Proxy is a Java class library supporting the communication with a reader that implements the EPCglobal Reader Protocol Version 1.1. The elements of the implemented protocol include:

- Transport Binding (TCP and HTTP)
- Message Binding (XML and Text)
- Synchronous and Asynchronous Messaging (Notification Channels)
- Triggers
- Data Selectors

The reader can be configured by a configuration file which contains the settings or through a method call for each command (Figure 5-3).

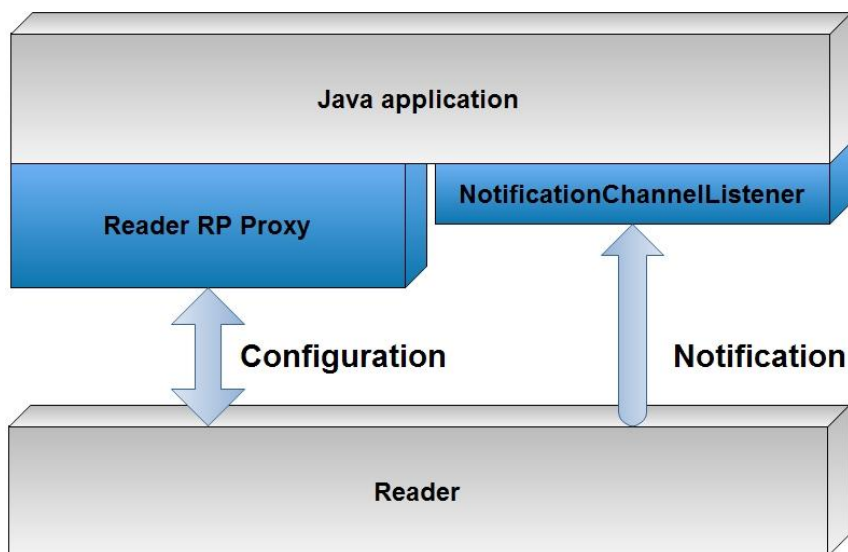


Figure 5-3: Reader RP Proxy

Field of application

- Communication with a reader through a Java application over the EPCglobal Reader Protocol Version 1.1
- Receiving notifications from the reader in the java application by implementing the NotificationChannelListener

5.2.3 Reader RP Client

The Reader RP Client is a Java Swing GUI which allows executing commands and communicating with an RFID reader that implements the EPCglobal Reader Project Version 1.1. The elements of the implemented protocol include:

- Transport Binding (TCP and HTTP)
- Message Binding (XML and Text)
- Synchronous and Asynchronous Messaging (Notification Channels)
- Triggers
- Data Selectors

Reader RP Client module contains beside the Test Client (GUI) two versions of an event sink. The EventSinkUI using a graphical user interface and the EventSink using the console are started separately. The notifications from the reader are received and displayed either in a text area or in the console (Figure 5-4).

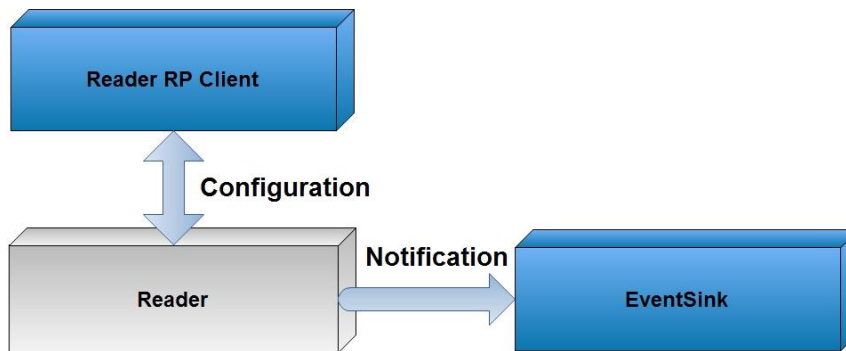


Figure 5-4: Reader RP Client and EventSink module

Field of application

- Communication with a reader using a graphical user interface to create and send commands over the EPCglobal Reader Protocol Version 1.1
- Receiving and displaying reader notifications with the EventSink

5.3 Implementation of the Triage Interface

The goal of the practical part of my diploma thesis is to create a Triage Interface application based on a software framework simulating the RFID technology. Besides that the Triage Interface must collect all the information which is usually written on the conventional paper triage tag.

The design of the Triage Interface is mapped from the combination of the DMS All Risk Triage Tag and the New Jersey Disaster Triage Tag (Chapter 1.4.1). Hence the graphical user interface of the Triage Interface looks similar to the front side of these conventional triage tags.

Conventional triage tags store patient information on the front and the back side; the Triage Interface uses tabs for detailed information, vital signs and the S.T.A.R.T. scheme to store the same information like the conventional triage tags.

By clicking on the body picture injuries can be added. The Triage Interface limits the number of injuries to 25 and allows one type of injury to occur more times unlike the conventional triage tags. Furthermore the space for comments and other patient data is less restricted by the Triage Interface.

Conventional tags identify the injury level by tearing of the colored category of the injury. Once a patient is marked for immediate treatment it is impossible to change this information to delayed treatment with the same triage tag (see also chapter 1.4.1). The

Triage Interface uses 4 buttons to determine the injury category allowing quick modifications of the patient status.

The Triage Interface is thought to be running on the mobile triage devices and the ambulance and hospital terminals. The implementation of the Triage Interface into the Fosstrak project is shown in Figure 5-5.

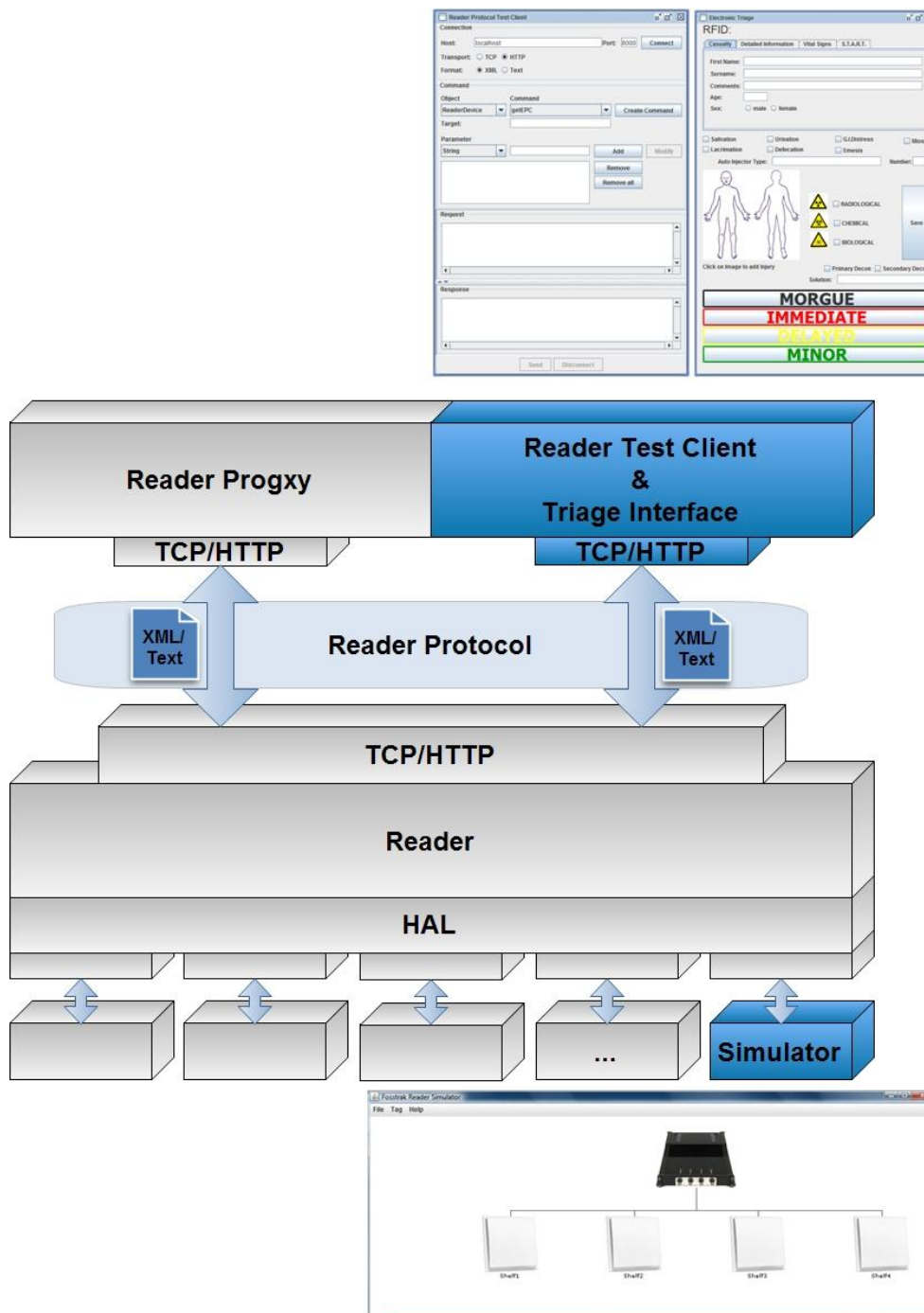


Figure 5-5: Triage Interface and the Fosstrak modules

5.3.1 Configuration

This section gives instructions which modules of the Fosstrak project must be started and how to configure the reader.

First of all these necessary modules must be started before configuring the reader:

- The Fosstrak reader using the graphical HAL Simulator with a source “Shelf2” (Figure 5-6)

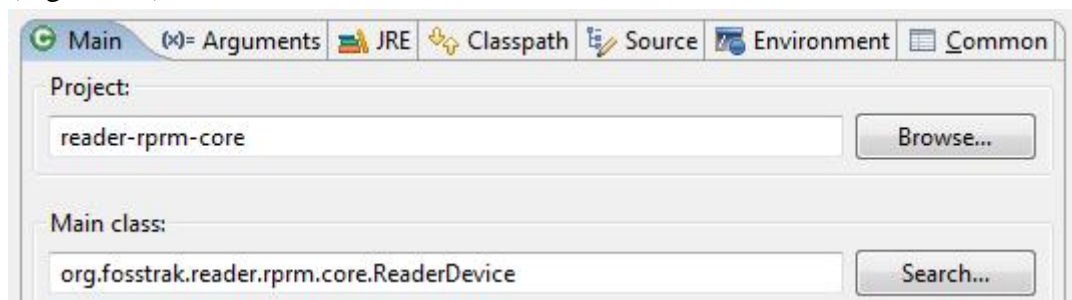


Figure 5-6: Start the Fosstrak Reader

- The Reader RP Client (TestClient) for the reader configuration (Figure 5-7)

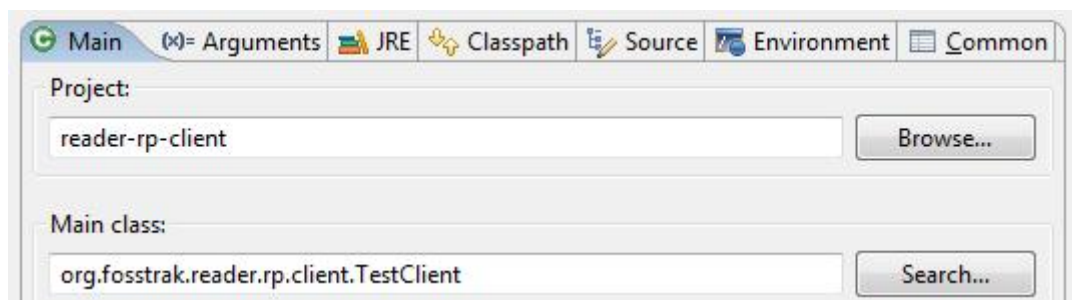


Figure 5-7: Start the Reader RP Client

- The Triage Interface listening on port 9999 if no port is specified (Figure 5-8)

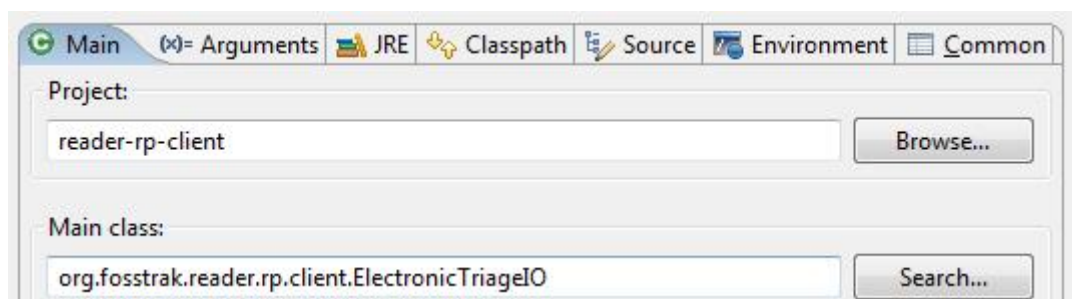


Figure 5-8: Start the Triage Interface

After starting these 3 modules the reader has to be configured:

- 1) Connect to the reader on localhost port 8000 with transport binding HTTP and format XML. (Figure 5-9)



Figure 5-9: Connect to the reader

- 2) Create a read trigger

Parameter: 'rt' (name), 'TIMER' (type), 'ms=2000' (timer value)

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:command xmlns:ns2="urn:epcglobal:rp:xsd:1">
  <id>2</id>
  <targetName></targetName>
  <trigger>
    <create>
      <name>rt</name>
      <triggerType>TIMER</triggerType>
      <triggerValue>ms=2000</triggerValue>
    </create>
  </trigger>
</ns2:command>
```

- 3) Create a notification trigger

Parameter: 'nt' (name), 'TIMER' (type), 'ms=2000' (timer value)

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:command xmlns:ns2="urn:epcglobal:rp:xsd:1">
  <id>4</id>
  <targetName></targetName>
  <trigger>
    <create>
      <name>nt</name>
      <triggerType>TIMER</triggerType>
      <triggerValue>ms=2000</triggerValue>
    </create>
  </trigger>
</ns2:command>
```

- 4) Create a notification channel

Parameter: 'nc' (name), 'tcp://localhost:9999?mode=connect' (address)

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:command xmlns:ns2="urn:epcglobal:rp:xsd:1">
  <id>6</id>
  <targetName></targetName>
  <notificationChannel>
    <create>
```

```

        <name>nc</name>
        <address>tcp://localhost:9999?mode=connect</address>
    </create>
</notificationChannel>
</ns2:command>

```

5) Add the notification trigger to the notification channel

Parameter: 'nt' (trigger name)

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:command xmlns:ns2="urn:epcglobal:rp:xsd:1">
    <id>8</id>
    <targetName>nc</targetName>
    <notificationChannel>
        <addNotificationTriggers>
            <triggers>
                <list>
                    <value>nt</value>
                </list>
            </triggers>
        </addNotificationTriggers>
    </notificationChannel>
</ns2:command>

```

6) Add the source to the notification channel

Parameter: 'Shelf2' (source name)

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:command xmlns:ns2="urn:epcglobal:rp:xsd:1">
    <id>10</id>
    <targetName>nc</targetName>
    <notificationChannel>
        <addSources>
            <sources>
                <list>
                    <value>Shelf2</value>
                </list>
            </sources>
        </addSources>
    </notificationChannel>
</ns2:command>

```

7) Add the read trigger to the source

Parameter: 'rt' (read trigger name)

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:command xmlns:ns2="urn:epcglobal:rp:xsd:1">
    <id>12</id>
    <targetName>Shelf2</targetName>
    <source>
        <addReadTriggers>
            <triggers>
                <list>
                    <value>rt</value>
                </list>
            </triggers>
        </addReadTriggers>
    </source>
</ns2:command>

```


After performing these commands the reader is configured properly. To test the Triage Interface do the following:

- Add a new tag to the Fosstrak Reader Simulator
- Drag the tag over the defined Antenna
- The Triage Interface gets a notification text formatted in XML filtering out the needed information; The RFID number appears in the Triage Interface indicating that it is an input for a “new patient”.

An example for the notification text for the Triage Interface looks like this; [FoCI09]

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:notification xmlns:ns2="urn:epcglobal:rp:xsd:1">
  <id>1</id>
  <reader>
    <readerEPC>ReaderEPC</readerEPC>
    <readerName>MyReader</readerName>
    <readerHandle>0</readerHandle>
    <readerRole>ReaderRole</readerRole>
  </reader>
  <notifyTriggerName>NotificationTrigger</notifyTriggerName>
  <notifyChannelName>NotificationChannel</notifyChannelName>
  <readReport>
    <sourceReport>
      <sourceInfo>
        <sourceName>Shelf2</sourceName>
        <sourceFrequency>0</sourceFrequency>
        <sourceProtocol>not supported</sourceProtocol>
      </sourceInfo>
      <tag>
        <tagID>9204F0004B000000</tagID>
        <tagIDAsPureURI>urn:epc:raw:64.x9204F0004B000000</tagIDAsPureURI>
        <tagIDAsTagURI>urn:epc:raw:64.x9204F0004B000000</tagIDAsTagURI>
        <tagType>not supported</tagType>
        <tagEvent>
          <eventType>evGlimpsed</eventType>
          <eventTriggers>
            <trigger>ReadTrigger</trigger>
          </eventTriggers>
          <time>
            <eventTimeTick>1199287632796</eventTimeTick>
            <eventTimeUTC>2008-01-02T16:27:12.796+01:00</eventTimeUTC>
          </time>
        </tagEvent>
        <tagEvent>
          <eventType>evNew</eventType>
          <eventTriggers>
            <trigger>NoTrigger</trigger>
          </eventTriggers>
          <time>
            <eventTimeTick>1199287632796</eventTimeTick>
            <eventTimeUTC>2008-01-02T16:27:12.796+01:00</eventTimeUTC>
          </time>
        </tagEvent>
      </tag>
    </sourceReport>
  </readReport>
</ns2:notification>
```

5.3.2 Implementation

The Triage Interface is implemented in Java consisting out of the following 4 classes:

- ElectronicTriageIO
- ElectronicTriageNotification
- ElectronicTriageParser
- ElectronicTriageData

a) ElectronicTriageIO

This Java class is the main class for the Triage Interface containing the main-method. The graphical user interface and the editor for the injuries are initialized. Methods for displaying and saving the information of a patient and clearing the Triage Interface are implemented. The run-method creates a ServerSocket on a certain port and waits for incoming notifications of the reader.

In the following section the most important methods and classes of ElectronicTriageIO.java are described shortly:

- public static void main(String[] args)

The main method creates an instance of the ElectronicTriageIO class and starts the run method. If there is no parameter specified the default port number in ElectronicTriageIO () is 9999.

```
ElectronicTriageIO client;
int port;

if (args.length == 1){
    port = Integer.parseInt(args[0]);
    client = new ElectronicTriageIO(port);
} else
    client = new ElectronicTriageIO();
...
client.run();
```

- run ()

The run method creates a ServerSocket on the specified port and waits for incoming notifications. The reader notification text is formatted in XML. The incoming notification is parsed to an ElectronicTriageNotification class by the ElectronicTriageParser. The runParser () method gets the XML notification as text and converts this to the ElectronicTriageNotification object. If there is no

patient saved with the special RFID number a clear display will be shown otherwise the information of the patient will be displayed.

The following code is a code section from the method run () in the class ElectronicTriageIO:

```

ServerSocket ss = null;
try {
    ss = new ServerSocket(port);
    while(true) {
        try {
            Socket s = ss.accept();
            BufferedReader in = new BufferedReader(new
            InputStreamReader(s.getInputStream()));
            String data = in.readLine();
            String xmlNotificationString = "";
            while(data != null) {
                ...
                xmlNotificationString = xmlNotificationString+data;
                data = in.readLine();
            }
            ...
            ElectronicTriageParser etp = new ElectronicTriageParser();
            ElectronicTriageNotification n =
            etp.runParser(xmlNotificationString);
            ...
            if (n.getEventType().equals("evGlimpsed"))
                displayPatient(n.getTagID());
        } catch (Exception e) {
            System.out.println("\nERROR: "+e.getMessage());
        }
    }
} catch (IOException e1) {
    System.out.println("\nERROR: creating ServerSocket on Port " + port + "
    failed.");
}

```

- initComponents ()

In this method all the needed visual Java Swing components are created, initialized and positioned properly. This method is started in the constructor.

- savePatient ()

This method saves all the information with the actual RFID number of the patient. The information input on the Triage Interface can be changed and saved any times.

- displayPatient ()

By dragging the tag over the antenna in the HAL simulator the run method gets the notification and filters out the RFID number and displays with this method the information of a patient.

- clearDisplay ()

This method clears the display of the Triage Interface.

- class InjuryEditor

This class is creates a graphical user interface for the input of the injuries. It allows adding one injury and deleting or editing the old injuries already input.

b) ElectronicTriageNotification

The ElectronicTriageNotification class provides get- and set-methods to save notification information. The notification text sent from the reader simulator has XML format. After The ElectronicTriageParser class gets the XML code as a String and converts it to an ElectronicTriageNotification object. Now the needed notification information can be easily accessed through the get methods of the ElectronicTriageNotification object (e.g., getReaderName (), getTagID (), getEventType ()).

c) ElectronicTriageParser

The ElectronicTriageParser class parses a Java String with XML code into a Document and then saves the information into an ElectronicTriageNotification object.

The runParser () method gets the notification as a String parameter and parses the String with the XML tags into a DOM-object. The parsed text becomes a DOM representation of the XML code by using the DocumentBuilder. After that the information can be accessed easily through the NotificationElement and stored into the ElectronicTriageNotification object.

```
Element notificationElement = dom.getDocumentElement();
...
String readerName = getTextValue(notifEl,"readerName");
String tagID = getTextValue(notifEl,"tagID");
...
ElectronicTriageNotification n = new ElectronicTriageNotification(..., reader-
Name, ..., tagID, ...);
```

The notification element (XML) and the tag name are needed in the `getTextValue ()` method to look for the tag and get the text content of it. For instance we have the XML snippet `<notification><tagID>12</tagID></notification>` and the `Element` points to the notification node and the `tagName` is `tagID` then 12 will be returned.

```
private String getTextValue(Element ele, String tagName) {
    String textVal = null;
    NodeList nl = ele.getElementsByTagName(tagName);
    if(nl != null && nl.getLength() > 0) {
        Element el = (Element)nl.item(0);
        textVal = el.getFirstChild().getNodeValue();
    }
    return textVal;
}
```

d) ElectronicTriageData

The `ElectronicTriageData` class is for the storage of the patient information. All the information from a conventional paper triage tag can be input and saved with the Triage Interface. The information of one patient is stored in a `ElectronicTriageData` object and can be identified by the RFID number.

5.3.3 Data Storage

Patient information is stored by the mobile triage interface to the RFID tag. If wireless network is available the mobile triage device sends the patient information to the server.

The storage of patient information is outlined in the data model in Appendix A. The following tables are necessary for the storage of this information:

- Triage Tag:
The triage tag table stores information about the patient status (e.g., injury level) and general triage information (e.g., transportation agency, hospital determination). The version ID attribute defines the current version of the patient information providing data consistency in the electronic triage system. The emergency person who stored the patient information is identified by the emergency person ID attribute.
- Patient:
Personal patient information (e.g., name, address, religion) are stored in this table. The catastrophe ID is necessary for the correlation of the patient to a certain mass casualty. Each triage tag table is related to exactly one patient identified by the triage tag ID.
- Catastrophe:
This table stores the date, type and place of the catastrophe.

- **EmergencyPerson:**
Emergency personnel are identified by unique IDs. The forename, surname, degree and the facility being employed of the emergency person is stored in this table.
- **Symptom:**
The symptoms are a part of the triage tag information being stored in the symptom table. This information is assigned to the particular triage tag by the triage tag ID.
- **Start:**
The S.T.A.R.T. scheme information is stored in this table being assigned to the particular triage tag by the triage tag ID.
- **Injury:**
The injury table stores the type of the patient injury and x- and y-coordinates of the injury to define its location.
- **VitalSign:**
This table stores vital signs of the patient being measured during the triage process.
- **Medication:**
This table stores performed medications to the patient during the triage process.

The storage space on the RFID tag is limited to 1 kb. Hence a storage mechanism requiring little memory is essential. Except that the mechanism must be able to store variable number of patient attributes. The TLV (type-length-value) format, e.g., ASN.1 [InTe09] outlined in Figure 5-10 meets these requirements.



Figure 5-10: Type-length-value format

- **Type:**
The first byte of the TLV record ascertains the identifier and data type of the patient information to store. Each number defines the name of 1 record of patient information being stored by the Triage Interface (e.g., First Name = 2, Surname = 3, Injury Category = 12).

Table 5-1 lists all data records of patient information which might be stored on the RFID tag. Each type number defines the name and the data type of the patient record. 23 different types of patient records can be stored requiring maximum 573 bytes for storage. Hence we can limit the type size to 1 byte (max. 127 types possible) and the RFID tag memory of 1 kilobyte is sufficient.

- Length:
The second byte defines the length of the value.

- Value:
The last part of the TLV record is the value of patient information acquired by emergency personnel.

#	Name	Data Type	(Max) Size	Description
1	versionID	Number[]	4 bytes	2 bytes respectively for the versionID and emergency person ID
2	First Name	String	30 bytes	
3	Surname	String	30 bytes	
4	Comments	String	200 bytes	
5	Age	Number	1 byte	Max. age = 127 years
6	Sex	Char	1 byte	'm'=male, 'f' = female
7	Symptoms	Boolean[]	1 byte	bit 1 = Salivation, bit 2 = Urination, bit 3 = GI Distress, bit 4 = Miosis, bit 5 = Lacrimation, bit 6 = Defecation, bit 7 = Emesis
8	Auto injector type	Number	1 byte	Each auto injector type has a predefined number
9	Auto injector number	Number	1 byte	
10	Agent	Boolean[]	1 byte	1 bit respectively for: radiological, chemical, biological
11	Decontamination	Boolean[]	1 byte	1 bit respectively for: primary decontamination, secondary decontamination
12	Injury category	Number	1 byte	1=morgue, 2= immediate, 3= delayed, 4=minor
13	Injury	Number[]	4 bytes (max. 25 records)	1 byte respectively for: id, injury type, x- and y-coordinate for the body picture (see Figure 5-13). The number of injuries is limited to 25 (max. 100 bytes for injury storage). Injury id definition

				1 = Blunt Trauma, 2 = Burn, 3 = C-Spine, 4 = Cardiac, 5 = Crushing, 6 = Fracture, 7 = Laceration, 8 = Penetrating Injury, 9 = Other
14	Address	String	30 bytes	
15	Town/ZIP	Number	2 bytes	
16	Phone	String	15 bytes	
17	Religion	Number	1 byte	Each religion is defined by a certain number
18	Destination	String	30 bytes	Destination hospital
19	Via	String	30 bytes	Transportation agency
20	Vital sign	Number[]	11 bytes (max. 3 records)	3 bytes for time (hh:mm:ss), 4 bytes for blood pressure, 2 bytes respectively for pulse and respiration. The number of vital sign entries is limited to 3 (max. 33 bytes for vital sign storage)
21	Medication	String	15 bytes (max. 3 records)	3 bytes for time (hh:mm:ss converted from number to string), 2 bytes for drug solution (converted from number to string), 10 bytes for dose. The number of drug solutions is restricted to 3 (max. 45 bytes for medication storage)
22	Start	Boolean[]	1 byte	1 bit respectively for: respirations-yes, respirations-no, perfusion -2 seconds, perfusion +2 seconds, mental status-can do, mental status can't do

23	Date time	String[]	14 bytes	YYYY-MM-DD hh:mm:ss
maximum required capacity			573 bytes	

Table 5-1: Type definition for data storage on the RFID tag

Example:

The emergency personnel performed primary triage to a patient called John Doe, 22 years old and having minor injuries. There are 4 TLV records necessary to store this information to the RFID tag:

Type	Length	Value
2	4	John
3	3	Doe
5	1	22
12	1	4

Table 5-2: Type-length-value

Table 5-2 outlines the 4 TLV records stored on the RFID tag. Type 2 stands for the first name and type 3 for the surname, type 5 for the age and type 12 for the injury category. The mobile triage device and the RFID middleware can determine the data type of the value through the type number (type 2 = String, type 5 = Number).

In some cases the value must be interpreted by the mobile triage device or the middleware. Type 12 stands for the injury category and the value 4 stands for minor injuries.

5.3.4 Documentation

In the following section I will document a short test of the already started Fosstrak Reader, Test Client and Triage Interface. Of course the reader must be configured like described two sections before.

The following steps could be done to test the Triage Interface application.

- 1) Add a new tag to the Fosstrak Reader simulator via menu or the context menu

There are two possibilities to add a tag to the reader (Figure 5-11). Either via menu (“Tag”) or via context menu (“Add new Tag”). Before adding the tag you can change the RFID number.

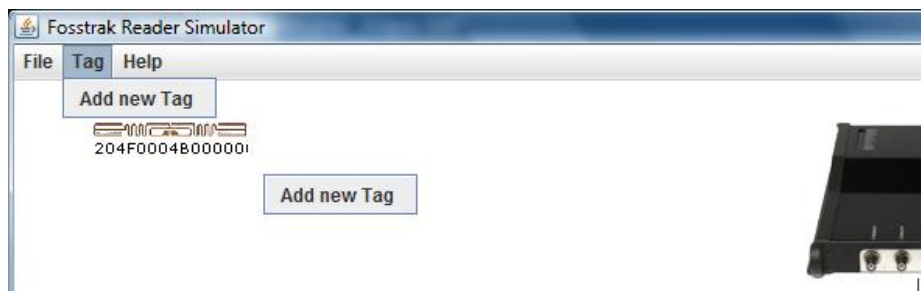


Figure 5-11: Add a new tag to the reader

- 2) Move the tag over the reader antenna (Figure 5-12)

Click on the RFID tag and drag and drop it over the antenna with the name “Shelf2”. Then wait a moment until the reader sends the notification to the Triage Interface. This simulates the reading of an RFID with an RFID reader by emergency personnel.

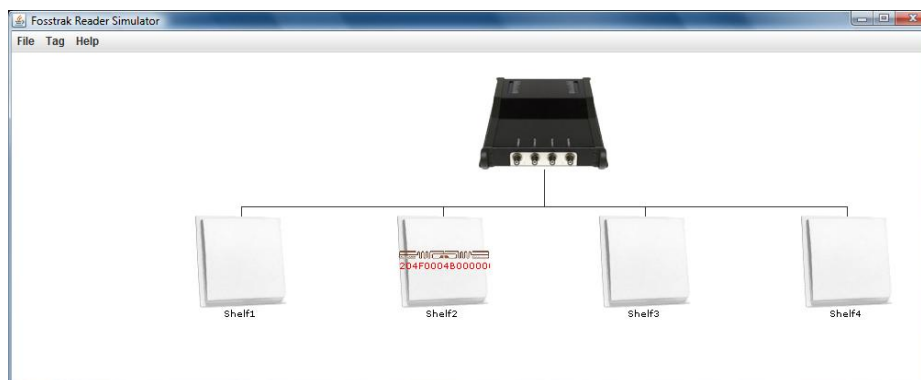


Figure 5-12: Move the tag over the antenna

3) RFID number appears in the Triage Interface

The RFID number of the tag appears on the top of the Triage Interface (Figure 5-13). There is no information stored yet with this RFID number therefore there is beside the RFID number the label: “(new patient)”

The screenshot shows a web-based interface titled "Electronic Triage". At the top, it displays the RFID number "9204F0004B000000" followed by "(new patient)". Below this are four tabs: "Casualty" (selected), "Detailed Information", "Vital Signs", and "S.T.A.R.T.". The "Casualty" tab contains several input fields: "First Name:", "Surname:", "Comments:", "Age:", and "Sex:" with radio buttons for "male" and "female". Below these are checkboxes for various symptoms: "Salivation", "Urination", "G.I. Distress", "Miosis", "Lacrimation", "Defecation", and "Emesis". There is also an "Auto Injector Type:" field and a "Number:" field. Two human figures are shown for injury selection, with a "Click on Image to add Injury" instruction. To the right are three hazard icons (Radiological, Chemical, Biological) with corresponding checkboxes. Below these are checkboxes for "Primary Decon" and "Secondary Decon", and a "Solution:" field. A large "Save" button is on the right. At the bottom, four horizontal bars indicate triage status: "MORGUE" (black), "IMMEDIATE" (red), "DELAYED" (yellow), and "MINOR" (green).

Figure 5-13: Triage Interface

4) Input patient information

The emergency personnel can decide which information to input. Usually for primary triage information only the injury category, age and sex is needed. For secondary triage there is more information about the patient needed and for hospital destination the address of the hospital.

A nice feature of the Triage Interface is the possibility to add new injuries by clicking on the picture with two bodies. A new popup window will appear where the emergency personnel can add one new injury (Figure 5-14). Besides that there is the possibility to delete or edit already input injuries.

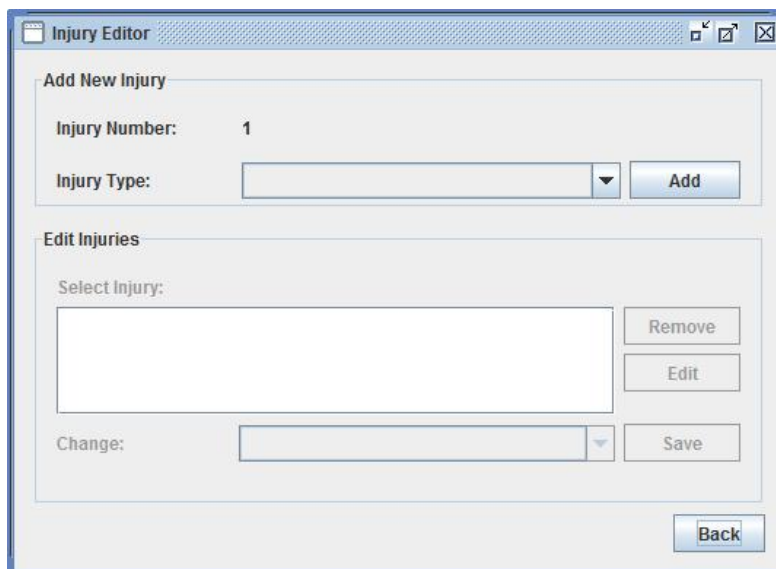


Figure 5-14: Injury editor of the Triage Interface

5) Press “Save” button

After the input of the test information press the “Save” button. Now the patient information is saved.

Now add more tags in the Fosstrak Reader simulator. Move one new tag over the reader antenna and add new information. Then save the information of the second patient. Move the second tag away from the antenna and the first over the antenna again. Now the information of the first patient should appear in the Triage Interface.

6 Discussion and Future Work

Probably the main advantage of an electronic triage system is the collection of the needed information about injured people to a central unit in real-time and without any media breaks. This information is collected by mobile triage devices and terminals in the ambulance and in hospitals. Before the information is sent to the server it is stored on the RFID chip. In the case that there is no wireless network connection the information about the injured person is still available for the emergency personnel. Nevertheless the emergency personnel can change or add information to the RFID tag. As soon as wireless network is available the mobile triage device sends the queued patient information to the server.

The RFID tag is attached to the conventional paper triage tag. The mobile triage device or the reader device must be moved less than 5 cm to the RFID tag when saving information. This prevents collisions of reading from more tags at the same time.

Patient information is stored to the RFID tag first; afterwards the mobile triage device sends the information to the server if wireless connection is available. This assures that the most current version of patient information is always available for the emergency personnel by reading the information from the RFID tag.

The mobile triage devices and the ambulance and hospital terminals with the Triage Interface designed and programmed in the practical part of the diploma thesis improve the input throughput by automating information of the emergency personnel and hospitals (emergency personnel name and degree, address of the hospital by inputting the postal code, current date and time). Handwritten triage tags sometimes are not easy to read and can be corrupted. This disagreeableness can be prevented through the electronic triage tag. The durability requirements for the RFID tag assure that the RFID tag should be resistant and unsusceptible against effects of the environment like temperature, pressure, radiation, chemical and water.

Most limitations of the conventional triage tag are abolished through the electronic triage system. But the place for comments about the injured person is still limited by the capacity of the passive RFID tag with 1 kb of memory.

The Fosstrak project is an open source RFID software which provides core software components for track and trace applications. It consists amongst others out of the Fosstrak Reader. The Fosstrak Readers allows to simulate many RFID readers with antennas and then to configure them. Afterwards it is possible to add RFID tags and simulate the reading of an RFID tag with the Fosstrak HAL project.

The Triage Interface is the practical part of the diploma thesis written in Java. It uses the Fosstrak project to emulate the RFID technology simulating RFID readers interrogating RFID tags.

The Fosstrak project does not allow saving information on the RFID tag. The only information saved on the RFID tag is the RFID identification number. This restriction of the Fosstrak project leads to saving the necessary information only in the Triage Interface.

The main concern about the electronic triage system is the strong dependence on the IT infrastructure. Wireless network is not everywhere available or can crash anytime hence the collection of patient information is delayed. Mobile triage devices with the integrated RFID reader are at risk to become defective by hardware errors during the triage process. The RFID middleware and the database on the server are the central unit of the electronic triage infrastructure. In case of a server crash the whole triage management guided through the command center would be destabilized and disrupted. This is not a disadvantage of the electronic triage system but a concern which must be addressed in the planning stage of the infrastructure.

The mobile triage devices are used in the early and stressful stages of triage by emergency personnel. The acceptance of the electronic information gathering through emergency personnel cannot be assured. It is even possible that the input of patient information by the mobile triage device is slower and less intuitive than the writing of patient information to the conventional tag. These doubts and uncertainties about the acceptance and prosperity of the electronic triage system can be reduced or eliminated through the results of studies or field trials.

6.1 Open Issues

- The practical part of the diploma thesis is the software which would run on the mobile triage devices and the ambulance and hospital terminals. But there must be a software interface which would run on a notebook PC in the command center obtaining the whole information about injured people. The director of operations using this software coordinates the field management and publishes information of the mass casualty incident efficiently.
- The software running on the server and managing the information of the injured people in a database was not a part of this diploma thesis. It is necessary to collect all the information sent by the mobile triage devices and ambulance and hospital terminals and to store this information into the database. On a request

from the command center software the server software must send back the information about the injured people after the authentication is verified.

- The Triage Interface software can be expanded with special features. On condition that the mobile triage devices and the ambulance and hospital terminals are equipped with a GPS module, it would be possible to save the GPS coordinates in the system. These coordinates could help to improve many activities in a case of a disaster situation especially in case of a big incident site. For instance the command center could have a better geographic overview or the save and rescue teams could locate a triaged patient through the GPS coordinates.
- The Triage Interface uses the open source Fosstrak project to simulate the RFID reader and RFID tags. Because of the results in the Requirements Analysis we decided to store the information about the injured person on the RFID tag. Unfortunately the Fosstrak project does not allow writing data on the RFID tag which is possible to do with the real (passive) RFID tags. It is only possible to read the RFID number to identify the unique tag in the simulator of the Fosstrak Reader. Therefore it was not possible to simulate the storage of the patient information on the RFID tag.
- The Triage Interface software is usually thought for the primary and secondary triage and for hospital determination as well as for the information collection. In the Requirements Analysis we decided to reduce the information for the primary triage to the injury level, sex and age. A particular interface for primary triage allowing the emergency personnel to input only these 3 records about the patient improves the efficiency of the stressful primary triage.

7 Summary

7.1 Introduction

Medical areas such as diagnose, treatment and patient care benefited from the application of IT-infrastructure. The goal of this thesis is to bring these benefits to the field of emergency care.

Overview

Triage is a process during emergency care which aims at maximizing the provided care in a situation where the available resources are insufficient for medical treatment of all patients. One of the goals of triage is to diagnose critical injuries requiring lifesaving treatment in the shortest possible time. To this end patients are categorized into groups to determine their priority for treatment and transport to definitive care facilities. Thereby emergency personnel attach Triage Tags to the injured people. Triage tags are used to

- Classify the degree of the injury and determine the transport order of injured people to the hospitals
- Obtain information about the casualty incident to publish to special facilities or to use for decision making like medical resource procurements.

To aid the emergency personnel in the triage process and to avoid some of the drawbacks of conventional triage tags in this diploma thesis we propose a triage system using RFID tags (silicon chips with IDs, radio frequency functions and some additional logic and memory) which are attached to the conventional paper triage tags. RFID readers supply power to the RFID tags (passive) through radio frequency communication and read/write information from/on the tag. The RFID tags recommended in our diploma thesis are passive and have 1 kb of rewritable memory.

Emergency personnel use mobile devices equipped with an RFID reader. Mobile devices are used for the collection of patient information and identification of the injured person by the unique ID of each RFID tag. The RFID tag is embedded to the convention triage tag.

Motivation for the Electronic Triage Tag

Real-time information about patients and their status is critical to the overall management of field medical care by the command center. Because of the known and limited availability of resources (such as on-scene providers, ambulance locations, and area hospital capacities) medical command must coordinate timely information on the num-

ber of casualties and their needs. Moreover real-time information is critical to determine the appropriate patient destination, depending on the type of injuries and the capabilities of the receiving facilities.

The main advantages of an electronic triage system compared to a conventional triage system are:

- Mobile devices combined with wireless communication allow collecting the needed information of injured people via the network by sending the information to a central server.
- Input method using mobile devices allow less error prone read/write features compared to handwriting
- Input rate is improved by automating the information of the emergency personnel and hospital addresses
- Real-time access to the patient information which is critical to the overall management of field medical care is provided by the wireless data transmission and the storage of the information on a central unit

7.2 Requirements of Medical Equipment

The electronic triage system architecture consists of different components necessary for the collection of patient information. The mobile triage device with an integrated RFID reader is used by the emergency personnel in the early stages of triage. It has a significant role in the information collection process of the electronic triage and as such has to be regarded as a medical device. Thus we must define general requirements as basic principles for a medical device.

7.3 Requirements Analysis

The requirements for the electronic triage system must ensure that critical information collected in the field is communicated to receiving personnel quickly and accurately. All patients and emergency personnel must be registered and identifiable. The electronic triage system must ensure that patients and emergency personnel are accounted for at all times without over reliance on manual, error prone, processes. The collected information relevant to situational management and decision support must be integrated into a central unit and available over a single application for the command center. In case of system or network failure the electronic triage system must have contingency capabilities.

Technical Requirements for the Middleware

The RFID middleware software is the bridge between the RFID architecture and the data repositories (the central database). The RFID middleware is the central part of the RFID system managing and coordinating it. It is responsible that patient information is consistent, updated constantly and provided for the control center. The main challenge for the RFID middleware is to provide data consistency.

System Requirements

In this diploma thesis we outline a solution for the challenges of the electronic triage system by analyzing the workflow and optimizing the network usage by following approaches:

- Availability is assured by the storage of the information of the injured people on the RFID tag and using it as local buffer.
- Confidentiality is assured by the security measures applied to the electronic triage system on different layers.
- Latency is lowered by defining minimum wireless communication areas in the paths of the triage workflow.
- Input rate is improved by the mobile devices using input easier input methods and automating information storage.
- Integrity is assured by mechanisms in the middleware being responsible that patient information is consistent, updated constantly and provided for the control center.

System Architecture

The electronic triage system consists of the following components:

- Triage Tag: Each RFID tag has a unique ID
- Mobile Triage Device: The mobile triage device is a handheld scanner carried by emergency personnel and used for information collection
- Control Center Terminal: A notebook PC equipped with a wireless communication
- Ambulance Terminal: A notebook PC equipped with an RFID reader and a wireless communication
- Hospital Terminal: A notebook PC equipped with an RFID reader and wireless communication
- Server: The information collected by the mobile triage devices, the ambulance terminal and the hospital terminal is stored on one central server

Workflow in RFID Triage

By applying the RFID technology into the triage workflow the triage system implicates the change that instead of writing and collecting the conventional paper tags, emergency personnel read the information of each injured person from the RFID tag, input the information of each injured person to the mobile triage device and then write it on the RFID tag.

7.4 Implementation

The Triage Interface software running on the mobile triage devices, the ambulance terminal and the hospital terminal is based on the Fosstrak Framework simulating RFID hardware (tag, reader). The Fosstrak project is free and open source software based on Java simulating the RFID technology.

The goal of the practical part of my diploma thesis is to create a Triage Interface application based on a software framework simulating the RFID technology. Besides that the Triage Interface must collect all the information which is usually written on the conventional paper triage tag.

The design of the Triage Interface is mapped from the combination of the DMS All Risk Triage Tag and the New Jersey Disaster Triage Tag (Chapter 1.4.1). Hence the graphical user interface of the Triage Interface looks similar to the front side of these conventional triage tags.

Conventional triage tags store patient information on the front and the back side; the Triage Interface uses tabs for detailed information, vital signs and the S.T.A.R.T. scheme to store the same information like the conventional triage tags.

Data Storage

Patient information is stored by the mobile triage interface to the RFID tag. If wireless network is available the mobile triage device sends the patient information to the server.

The mechanism for data storage must be able to store variable number of patient attributes. The rewritable memory on the RFID tag is limited to 1 kb. Hence a storage mechanism requiring little memory is essential. These requirements are fulfilled by the TLV format (type-length-value).

7.5 Discussion and Future Work

Probably the main advantage of an electronic triage system is the collection of the needed information about injured people to a central unit in real-time and without any media breaks. This information is collected by mobile triage devices and terminals in the ambulance and in hospitals. Before the information is sent to the server it is stored on the RFID chip. In the case that there is no wireless network connection the information about the injured person is still available for the emergency personnel.

The mobile triage devices and the ambulance and hospital terminals with the Triage Interface designed and programmed in the practical part of the diploma thesis improve the input rate by automating information of the emergency personnel and hospitals (emergency personnel name and degree, address of the hospital by inputting the postal code, current date and time...).

The mobile triage devices are used in the early and stressful stages of triage by emergency personnel. The acceptance of the electronic information gathering through emergency personnel cannot be assured. It is even possible that the input of patient information by the mobile triage device is slower and less intuitive than the writing of patient information to the conventional tag. These doubts and uncertainties about the acceptance and prosperity of the electronic triage system can be reduced or eliminated through the results of studies or field trials.

Open Issues

- Software interface which would run on a notebook PC in the command center obtaining the whole information about injured people.
- The software running on the server and managing the information of the injured people in a database. This software must be implemented and tested.
- On condition that the mobile triage devices and the ambulance and hospital terminals are equipped with a GPS module, it would be possible to save the GPS coordinates in the system.
- The Triage Interface uses the open source Fosstrak project to simulate the RFID reader and RFID tags. The Fosstrak project does not allow writing data on the RFID tag which is possible to do with the real (passive) RFID tags. The simulation of reading/writing patient information on the RFID tag should be implemented.
- A particular interface for primary triage allowing the emergency personnel to input only these 3 records about the patient improves the efficiency of the stressful primary triage.

References

- [BlBu05] S. Blitz, M.J. Bullard, I. Colman, S.L. Dong, B.R. Holroyd, D.P. Meurer, B.H. Rowe BH, "Emergency triage: comparing a novel computer triage program with standard triage" in *Acad. Emerg. Med.*, 2005, Volume 12 (6), pp. 533-535
- [BuLy07] C.J. Buonoa, J. Lyona, R. Huanga, F. Liua, S. Browna, J.P. Killeena, D. Kirsha, T.C. Chana and L. Lenerta, "Comparison of Mass Casualty Incident Triage Acuity Status Accuracy by Traditional Paper Method, Electronic Tag, and Provider PDA Algorithm" in *Annals of Emergency Medicine*, 2007, Volume 50, pp. 12-13
- [CoLe04] J. Considine, S. A. LeVasseur, E. Villanueva, "The Australasian Triage Scale: Examining Emergency Department Nurses' Performance Using Computer and Paper Scenarios" in *Annals of Emergency Medicine*, 2004, pp. 517
- [CrIl08] Critical Illness and Trauma Foundation, Inc., "START (Simple Triage and Rapid Treatment) – Background", December 2008, <http://www.citmt.org/start/background.htm>.
- [DeDr02] J. S. Delaney, R. Drummond, "Mass casualties and triage at a sporting event" in *British Journal of Sports Medicine*, 2002, pp. 36:85-88
- [DiMa09] Disaster Management Systems – Saving Lives Through Aggressive Field Management, "All Risk Triage Tag - Standard", February 2009, <http://www.triagetags.com/p-77-all-riskreg-triage-tags-standard.aspx>.
- [DoBu07] S. L. Dong, M. J. Bullard, D. P. Meurer, S. Blitz, B. R. Holroyd, B. H. Rowe, "The effect of training on nurse agreement using an electronic triage system" in *Canadian Journal of Emergency Medicine*, 2007, Volume 9 (4), pp. 260-266
- [ElMe07] J. Elshove-Bolk, F. Mencl, B. T. F. van Rijswijck, M. P. Simons, A. B. van Vugt, "Validation of the Emergency Severity Index (ESI) in self-referred patients in a European emergency department" in *Emerg Med J*, 2007, pp. 170
- [EnOr10] About Mobility - CEO on Mobile & Wireless, "NFC/Touch", December 2010, <http://weblog.cenriqueortiz.com/touch-nfc/>
- [EpIn09] EPCglobal Inc., "Overview - What is EPCglobal?", March 2009, <http://www.epcglobalinc.org/home/>
- [EpSp09] EPCglobal Specifications, "13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag Interface Specification", April 2009,

-
- http://www.epcglobalinc.org/standards/specs/13.56_MHz_ISM_Band_Class_1_RFID_Tag_Interface_Specification.pdf
- [EuUn09] European Union Law, “Council Directive 93/42/EEC of 14 June 1993 concerning medical devices”, April 2009, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31993L0042:EN:NOT>
- [FiKl10] K. Finkenzeller: RFID Handbook – Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication
- [FrLe05] E. A. Fry, L. A. Lenert, “MASCAL: RFID Tracking of Patients, Staff and Equipment to Enhance Hospital Response to Mass Casualty Events” in AMIA Annu Symp Proc., 2005, pp. 261-265
- [FoCl09] Free Software Foundation, Inc., “Fosstrak - User Guide Reader RP Client”, April 2009, <http://www.fosstrak.org/reader/docs/user-client.html>.
- [FoNo10] Forum.Nokia, “Nokia 6131 NFC SDK 1.1” , December 2010, http://www.forum.nokia.com/info/sw.nokia.com/id/ef4e1bc9-d220-400c-a41d-b3d56349e984/Nokia_6131_NFC_SDK.html
- [FoOw09] Free Software Foundation, Inc., “Fosstrak - Overview”, February 2009, <http://www.fosstrak.org/overview.html>.
- [HaBr10] E. Haselsteiner, K. Breitfuß, “Security in Near Field Communication (NFC)”, Philips Semiconductors, 2010
- [HoBu07] D. E. Hogan, J. L. Burstein: Disaster Medicine. Lippincott Williams & Wilkins; 2nd edition, 2007
- [HuJe03] W. W. Hurd, J. G. Jernigan, P. K. Carlton : Aeromedical Evacuation - Management of Acute and Stabilized Patients. Springer; 1st edition, 2003
- [IIAh08] M. Ilyas , S. Ahson: RFID Handbook – Applications, Technology, Security, and Privacy. CRC Press; 1st edition, 2008
- [InOr09] International Organization for Standardization, “Medical devices -- Application of risk management to medical devices”, April 2009, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31550
- [InSo08] S. Inou, A. Sonoda, H. Yasuura, “Triage with RFID Tags for Massive Incidents” in Syed Ahson and Mohammad Ilyas, RFID Handbook: Applications, Technology, Security and Privacy, 2008, pp.329-349

-
- [IsMo07] K. V. Iserson, J. C. Moskop, "Triage in Medicine, Part I: Concept, History, and Types" in *Annals of Emergency Medicine*, 2007, Volume 49, Issue 3, 2007, pp. 275-282
- [KeAg96] K. Kennedy, R. V. Aghababian, L. Gans, C. P. Lewis, "Triage: Techniques and Applications in Decisionmaking" in *Annals of Emergency Medicine*, 2005, pp. 136-147
- [LeFr06] S. Levin, D. France, S. Mayberry, S. Stonemetz, I. Jones, D. Aronsky, "The Effects of Computerized Triage on Nurse Work Behavior" in *AMIA Annual Symposium Proceedings*, 2006, pp. 1005
- [LePa05] L. A. Lenert, D. A. Palmer, T. C. Chan, R. Rao, "An Intelligent 802.11 Triage Tag For Medical Response to Disasters" in *AMIA Annu Symp Proc.*, 2005, pp. 440-444
- [LiGr07] M. v. Lieshout, L. Grossi, G. Spinelli, S. Helmus, L. Kool, L. Pennings, R. Stap, T. Veugen, B. v. d. Waaij, C. Borean, "RFID Technologies: Emerging Issues, Challenges and Policy Options" in *JFC Scientific and Technical Reports*, 2007
- [MaGa06] T. Massey, T. Gao, M. Welsh, J. H. Sharp, M. Sarrafzadeh, "The Design of a Decentralized Electronic Triage System" in *AMIA Annu Symp Proc.*, 2006, pp. 544-548
- [MeMa09] Mettag – Maximize Survivors, "Mettag MT-137 – The Original Medical Emergency Triage Tag", February 2009, <http://www.metttag.com/mt137.html>.
- [MiCh03] M. Cheng: *Medical device regulations - global overview and guiding principles*; 1st edition, 2003
- [MiWi95] M. E. Wiklund: *Medical Device and Equipment Design: Usability Engineering and Ergonomics*. CRC Press; 1st edition 1995
- [NeFe10] NFC Forum, "The Near Field Communication (NFC) Forum", December 2010, <http://www.nfc-forum.org/home/>
- [OeOe04] Normensammlung 2004-1; *Medical electrical equipment, Part1: General requirements for safety and essential performance*. ÖVE/ÖNORM, EN 60601-1, edition 2004-05-01, pp. 42
- [RiFr06] R. C. Fries: *Reliable Design of Medical Devices*. CRC Press; 2nd edition 2006
- [RaFo09] The RadioActive Foundation, "The standards based open source RFID project", April 2009, <http://www.radioactivehq.org/index.html>
- [RiSo09] Rifidi, "Rifidi – Software defined RFID", 2009, <http://www.rifidi.org/>

-
- [RoBo06] B. H. Rowe, K. Bond, M. B. Ospina, S. Blitz, M. Schull, D. Sinclair, M. Bullard, "Data collection on patients in emergency departments in Canada" in *Canadian Journal of Emergency Medicine*, 2006, pp. 417-424
- [ScKo96] C. H. Schultz, K. L. Koenig, E. K. Noji, "A Medical Disaster Response to Reduce Immediate Mortality after an Earthquake" in *The New England Journal of Medicine*, 1996, Volume 334, pp. 438-444
- [StOf09] State of New Jersey – Department of Health and Senior Services, "New Jersey Triage Tag Presentation", February 2009, <http://www.state.nj.us/health/ems/documents/njdisastertag.pdf>.
- [SuDe10] Sun Developer Network (SDN) – Java ME Technology, "An Introduction to Near-Field Communication and the Contactless Communication API", December 2010, <http://java.sun.com/developer/technicalArticles/javame/nfc/>
- [ThDo00] J. M. Thompson, G. Dodd, "Ruralizing the Canadian Triage and Acuity Scale" in *Canadian Journal of Emergency Medicine*, 2000, pp. 267-269
- [TsAs09] TSG Associates Ltd., "Smart Tag – For Triage that Works", February 2009, http://www.tsgassociates.co.uk/English/Civilian/products/smart_tag.html
- [VaGr03] V. G. A. Grossman: *Quick Reference to Triage*. Lippincott Williams & Wilkins; 2nd edition, 2003
- [VeSt08] M. van Veen, E. W. Steyerberg, M. Ruige, A. H. J. van Meurs, J. Roukema, J. van der Lei, H. A. Moll, "Manchester triage system in paediatric emergency care: prospective observational study" in *BMJ*, 2008, pp. 337:a1501
- [WiGr07] W. C. Wilson, C. M. Grande, D. B. Hoyt: *Trauma: Emergency resuscitation, preoperative anesthesia, surgical management*. Springer New York; 1st edition, 2007
- [ZhKi09] Y. Zhang, P. Kitsos: *Security in RFID and Sensor Networks*. CRC Press; 1st edition, 2009

Appendix A

Data model for the storage of patient information.

