Master Thesis

Design and Implementation of a Mobile Patient Terminal for Ambulances

Robert Maier, BSc

Institute for Technical Informatics
Graz University of Technology

Assessor: Univ.-Ass. Dipl.-Ing. Dr. techn. Christian Steger

Advisors: Univ.-Ass. Dipl.-Ing. Dr. techn. Christian Steger
Dipl.-Ing. Rene Pachernegg (APUS Software GmbH)

Graz, January 2014

Abstract

Paramedics are legally bound to protocolling all actions they have taken during their ambulance missions [38]. These protocols must not only be kept safe for the next ten years, but also serve as basis for the accounting with the health insurance. To avoid the administration and the storage of each service protocol and to automate the accounting with the health insurance a concept of an integrated system within the transport area of ambulance cars has been elaborated in this thesis. This concept does not only address the data security of medical data and the connection to the central operating mission system of a rescue centre, but also includes a GUI-prototype for the processing of mission data as well as medical patient data. Furthermore, the thesis addresses the possibility to communicate with nearby hospitals as well as video- and audio conferences with doctors during ambulance operations. The central component of the system is a rugged Windows tablet, equipped with several communication technologies. On this tablet a mobile application enables the input of medical- as well as service data, and automatically forwards all entered data to the central mission guidance system. To sum up, the system outlined in this thesis provides the basis for a medical emergency system including several interfaces for the connection and the data transfer to the central operating mission system of a rescue centre.

Kurzfassung

Sanitäter sind dazu verpflichtet alle Tätigkeiten während eines Einsatzes in Form eines Protokolls zu dokumentieren [38]. Diese Protokolle müssen nicht nur für die nächsten 10 Jahre aufbewahrt werden, sondern dienen auch als Grundlage für die Verrechnung mit der jeweiligen Versicherungsanstalt. Um die Verwaltung dieser Protokolle zu erleichtern wird im Zuge dieser Arbeit ein Konzept für ein System ausgearbeitet, welches die Verrechnung automatisiert. Dieses Konzept beinhaltet nicht nur die Datensicherheit im Umgang mit medizinischen Daten und die Verbindung zu einem Einsatzleitsystem einer Rettungsstelle, sondern auch einen GUI-Prototypen für die Erfassung und Verarbeitung der zu dokumentierenden Daten. Des Weiteren wird im Zuge dieser Arbeit die Möglichkeit der Kommunikation mit nahegelegenen Krankenhäusern und deren Ärzten im Rettungsdienst diskutiert. Die zentrale Komponente des ausgearbeiteten Systems ist ein robustes Windows Tablet, welches über einige Kommunikationsmöglichkeiten verfügt. Auf diesem Tablet wird eine mobile Applikation ausgeführt, welche die Dokumentation von Einsatz-, Patienten- und Einsatzverrechnungsdaten ermöglicht. Zusammenfassend kann gesagt werden, dass diese Arbeit die Grundlage für ein medizinisches Rettungssystem ist, welches die Verbindung und die Datenübertragung an ein Einsatzleitsystem einer Rettungsstelle ermöglicht.

Statutory Declaration

I declare that I have authored this thesis independently, that I have not used other than the declared sources / resources, and that I have explicitly marked all material which has been quoted either literally or by content from the used sources.

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst, andere als die angegebenen Quellen/Hilfsmittel nicht benutzt und die den benutzten Quellen wörtlich und inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

Ort	Datum	Unterschrift

Acknowledgement

At this point, I would like to express my deep gratitude to the people without whose guidance and support my studies as well as this master thesis would not have been possible.

First and foremost I would like to thank my parents, whose support has never ceased me through my studies.

I also want to thank my girlfriend Ingrid and her parents for their patience and motivating words over the last years.

Furthermore, I would like to thank my advisor Ass.-Prof. Dipl.-Ing. Dr.techn. Christian Steger for his academic and professional assistance which shaped my thesis.

Without the company *APUS Software GmbH*, and especially Dipl.-Ing. Rene Pachernegg I would have never gotten the opportunity to pursue this challenging and interesting work. Therefore, I would like to express my gratitude to the employees, who have supported me with their technical knowledge and guidance through this thesis.

I also express my gratitude to the members of the Styrian Red Cross, with whose help I have gained an insight in the field of ambulance operations.

Graz, January 2014 Robert Maier

Contents

List of Figures

List of Tables

1 Introduction

The emergency medical services (EMS) are an integral part of the today's health care system. These services cover functions from providing trained emergency personnel and health services for medical emergencies to the timely transportation to the hospital and the health care of patients on location [3].

Paramedics are legally bound to protocolling all actions taken during ambulance operations [38]. As in emergency cases the transportation of patients to the hospitals by ambulance organizations has to be performed as fast as possible, there is not much time left for the documentation. Thus, most of the time mission protocols are filled in at the end of a mission. In order to technically support the ambulance operations, several systems are in use. In Austria, the mission operating systems of rescue services are usually connected to data terminals in the ambulance cars. These data terminals show related mission data and support the operation of the ambulance crew by the help of a navigation system.

1.1 Motivation

In Austria the documentation of ambulance operations is usually performed by the filling in of predefined mission protocols on papers. These mission protocols have to be stored for the next ten years, which leads to a certain level of administrative effort. In order to reduce the administrative burden, a system that automatically manages mission protocols has to be provided. Additionally, this system should not only enable the protocolling of ambulance operations in the transport area of the ambulance cars, but also outside the cars. Due to the fact that existing solutions for the documentation of ambulance operations are not only unsuitable for the high requirements regarding the robustness and operability, but are also complicated to integrate into ambulance cars, a better solution has to be elaborated and implemented.

The mission protocol data serves as basis for the direct billing with the health insurance organizations. This billing is manually performed by the Styrian Red Cross. In order to enable an automatic accounting, a communication between the Rescue Centre and the related insurance organization has to be established. Thus, related mission protocol parts have to be transferred between these two organizations. However, the transferred data must also be protected against unauthorised access.

1.2 Thesis Outline

The aim of this thesis is the development of a patient terminal for the documentation of ambulance operations. Additionally, a mobile application that enables the filling in of mission protocol data on a patient terminal in the transport area of ambulance cars has to be implemented. This does not only include a GUI-prototype but also the data transfer to the related Rescue Centre and the connection to medical devices in the ambulance cars. Therefore, discussions regarding the design and the requirements of such a system with the Styrian Red Cross have been taken place.

In chapter 2 basic information about emergency medical services (EMS), existing documentation systems for ambulance operations in Austria as well as some proposed systems by other countries will be presented. Moreover, general information about the usage of medical data in Austria will be provided. Then, the developed system for a patient terminal and the system architecture for the integration into a Rescue Centre will be presented in chapter 3. In addition, two Services for the retrieving of medical data via the Internet will be compared. Furthermore, in chapter 4 the implementation of the mobile application for the filling in of mission protocol data will be presented. Additionally, the GUI-prototype as well as the entity relationship diagram for the storage of the mission protocol data will be illustrated and discussed in more detail. Finally, the thesis will be summarised in chapter 5 and some possible future work will be presented.

2 Related Work

This chapter deals with related patient documentation systems and presents several implemented and proposed Emergency Medical Service systems. In section 2.1 some related documentation systems that are implemented in Austria will be discussed. Then, the basic idea behind a Emergency Medical System as well as the two main related models will be explained in section 2.2. In addition, the proposed systems will be compared regarding their technical implementation, their availability and their performance. The storage of electronic health data on the e-card will be analysed and the Austrian health-information-system introduced in section 2.4. Additionally, electronic health cards that are based on NFC [25][page 6] will be presented. Then, some different operational areas, that are somehow related to the patient documentation system, will be discussed in section 2.5. Furthermore, related standards for electronic equipments will be elaborated on in section 2.6. These standards are especially useful for outdoor environments. Finally, limitations regarding the process and storage of medical data by the Austrian data protection law will be outlined. In order to observe this law some parts of the MAGDA-LENA guidelines [8] will be discussed.

2.1 Patient Documentation Systems

There are several systems for the documentation of medical patient data for ambulance services in Austria. These systems include EDOCTA [19] and ELEKTRA+ [2]. Three different systems which are, however, related are used: EDOCTA (used in Vienna), ELEKTRA+ (applied in Salzburg) and another system, which is implemented in Vorarlberg. However, as the technical specifications of these systems could neither be found online nor could the systems be viewed on site due to temporary bottlenecks on the part of the ambulance institutions, comparisons between these systems could not be drawn. Table 2.1 shows some details about the EDOCTA system as well as lists the disadvantages of this system.

	Advantages	**Disadvantages**
EDOCTA	• Printout of transport bills • Connection to medical devices via Bluetooth • High data security • Direct connection and interfaces to the settlement system	• All-in-One device • Small display size and resolution • Outdated hardware
ELEKTRA+	-	-

Table 2.1: Comparison between existing systems [19]

2.2 Emergency Medical Service (EMS)

The Emergency Medical Service (EMS) is an extensive system that covers functions from providing trained emergency personnel and health services for medical emergencies to the timely transportation to the hospital and the health care of patients on location. Moreover, the EMS is an integral part of the today's health care system [3]. Due to the technical improvements of medical systems patients can be monitored with multifunctional monitoring systems on location for pre-hospital health care. There are two main models of emergency health care delivery for pre-hospital environments: the Franco-German model and the Anglo-American model. This differentiation has been widely used until the late 20th century. However, nowadays most EMS systems use variations of those two models [3].

2.2.1 Franco-German Model

The basic idea behind the Franco-German model is to provide pre-hospital care by well-experienced physicians on location with less transportations to the hospital. In short, only in cases where the medical treatment on location fails or cannot be performed a transportation to the hospital will be performed. In addition, further transportation types such as helicopters are made use of. Moreover, attending emergency doctors are entitled to make complex medical decisions on location as well as they are authorized to treat patients at their home or in the field of an emergency. This kind of model is a part of the whole health care system and is widely applied in Europe including Austria, Malta, Greece, France and Germany [3].

	Franco-German model	**Anglo-American model**
No. of patients	More treated on scene Few transported to hospitals	Few treated on scene More transported to hospitals
Provider of care	Medical doctors supported by paramedics	Paramedics with medical know-how
Main motive	Brings the hospital to the patient	Brings the patient to the hospital
Destination for transported patients	Direct transport to hospital wards ie: bypassing EDs	Direct transport to EDs
Overarching organization	EMS is part of public health organization	EMS is a part of public safety organization

Table 2.2: Comparison between the two EMS models [3]

2.2.2 Anglo-American Model

The Anglo-American model focuses mainly on the rapid transportation of patients to the hospital and provides less medical treatment on location. Moreover, the type of transportation is usually performed by land ambulances and less by helicopters. The allies within this EMS are generally not the public health services or hospitals, but the public safety services such as the police and the fire brigade [3]. In addition, patients are rather transported to specialised emergency treatment departments than to hospital wards. In these treatment departments emergency medical technicians (EMT) and well-trained paramedics perform the medical care. Apart from the USA, this model is applied in Canada, New Zealand, Sultanate of Oman and Australia.

2.3 Proposed EMS Systems

A telemedicine system, which enables a secure communication between the ambulance and the hospital via Wireless Wide Area Networks (WWANs) has been proposed [56]. In addition, the data gained by the medical system inside the ambulance provides the data for the communication. This medical system consists of a video camera and a scanner, as well as a computer. The system operates as follows: The paramedics activate the connection with their computer inside the ambulance and securely send diagnostic data gained by the medical system, which is connected to the computer. At the hospital the medical data is analysed with the help of the datasets within a database. This database contains all necessary information to retrieve the right prescription. The prescription is securely sent back to the paramedics within the ambulance to support an early treatment of the patient.

Quality vs. scenarios	HSPA	3G	Congested HSPA	Fallback to GPRS
	%	%	%	%
Video quality	82	74	34	0
Sound quality	96	94	56	0
Image quality	94	90	82	44

Table 2.3: Summary of feedback from doctors [6]

Although the idea behind this medical communication system seems very simple and easy to maintain, the system has some drawbacks. The resolution of the camera must be high enough to guarantee real time medical analysis. Therefore, the data amounts are very high and cannot be managed very easily with the current technologies. Moreover, several delays during the communication may complicate the medical treatment.

2.3.1 Greek System

The Greek system establishes a real-time telemedical application based on video conferencing sessions between the hospital and the ambulance using the mobile communication standard High Speed Packet Access (HSPA) [6]. Although HSPA has a high download and upload speed, the area in which this technology can be used is limited. Therefore, the communication might fall back to 3G or even GPRS with much lower download and upload speeds. In this paper several tests have been made to evaluate the efficiency and the acceptance of such a system in the daily routine. Not only the HSPA network coverage within big cities, but also within small villages have been investigated into. Doctors have evaluated the application based on the image-, video- and sound quality inside the ambulance in their daily routine. The results of the most common practical approach, congested HSPA, shows that the image quality is high, but the video quality is very low. In case of no-congestion the video-, sound-, and image quality are high, even with a fall back to 3G.

2.3.2 US Approach

Although the HSPA communication approach appears very promising, fall backs to 3G/2G communication methods provide too small data rates to reliably send data given by the emergency equipment (e.g. defibrillator) between the ambulance and the hospital. Therefore, the use of the Vehicular Ad Hoc Network (VANET) in combination with LT-Coding for the transmission of ambulance data has been suggested [27]. The basic idea of VANET is to establish a mobile wireless network consisting of (moving) vehicles, which interact by the help of the Ad-hoc On-demand Distance Vector (AODV) protocol. (In the US the WAVE 802.11p standard supports VANET over a 5.850-5.925Ghz band [18]). Figure 2.1 shows how the routing algorithm, for the communication between the ambulance and the hospital, works. The vehicles send routing requests (RREQ) as broadcast messages and after the reception of a route reply (RREP) the communication link will be established. In addition, HELLO messages are periodically sent to maintain the connection between the nodes. However, at the time the data is send, the wireless network link may be broken and the data would be lost (see figure 2.1). Therefore, the communication should not be established until a successful data communication can be guaranteed. A LT based communication mechanism, the AODV protocol extended by the LT-coding mechanism, to prevent data loss has been presented [18]. The nodes send the encoded medical information per broadcast and the communication link will not be established until the hospital successfully decodes the information and sends a signal back.

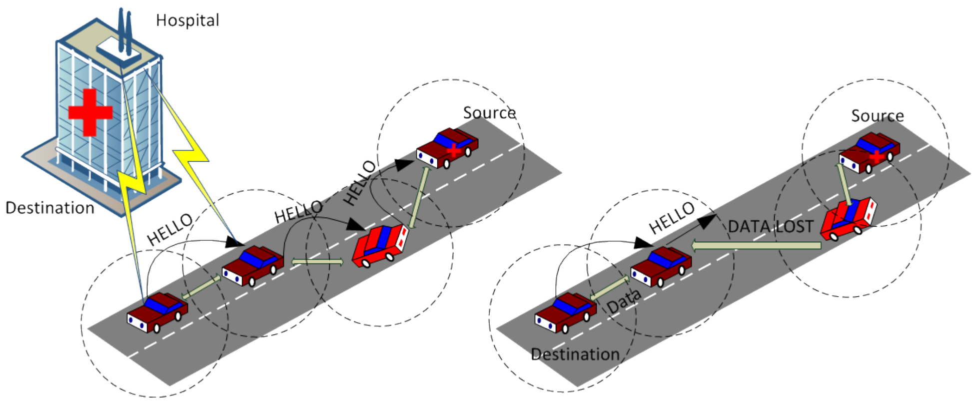


Figure 2.1: Routing mechanism and packet loss (adapted from [27])

2.3.3 China

Similar to the HSPA communication approach, the SAFER system enables the communication between the ambulance and the hospital through a cellular connection, for which a router connecting a LAN and cellular networks, is used. As shown in figure 2.2 the patient data of the medical system inside the ambulance (e.g. heart monitor) is sent, via a wireless local area connection, to the laptop of the paramedic. The router forwards the vital- and video data of the patient to the hospital so that the doctors get an idea of the patient's health and the hospital can prepare all necessary medical care in advance [55].

		CDMA 2000 Spec and China Telecom spec compliance			
Diversity reception	**Communication distance**	**Frequency bands**	**CDMA**	**WiFi**	**Max # of simultaneous subscribers**
Selective diversity	CDMA cellular zones, WiFi: 200m	CDMA: 800/1900 MHz	EDVO Rev.A	IEEE 802.11b/g	5

Table 2.4: Characteristics of the router

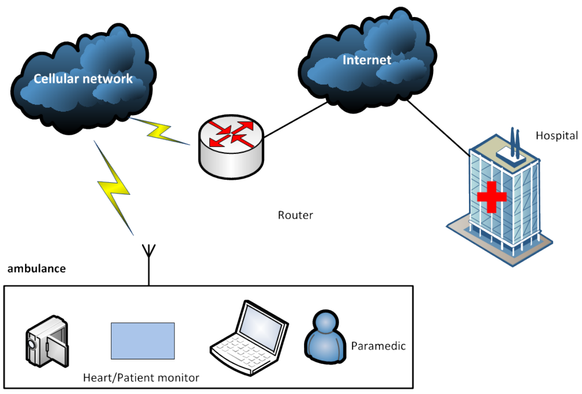


Figure 2.2: Configuration of emergency medical cares (adapted from [55])

The configuration of the router, which establishes the connection between the cellular networks and the LAN is shown in table 2.4. The code division multiple access method is used for the radio communication, the max number of subscribers is limited to five and the communication distance is extended to the cellular zones and for WiFi to 200 meters.

In addition to the system, which establishes the communication between the ambulance and the hospital, a DSRC- and GPS antenna, which is mounted on top of the ambulance, enables a fast transportation to the hospital by the help of a traffic control system. Figure 2.3 shows the configuration of this system. The ambulance informs nearby vehicles, which are equipped with a DSRC receiver, of their presence through broadcasts so that an inter-vehicle communication (IVC) is established and the way to the hospital can be cleared for the ambulance. Moreover, each traffic light contains a DSRC receiver, which directly communicates with the traffic control center so that the traffic signal can be changed to green as soon as the ambulance passes by.

	ITS Forum RC-005 settings			
communication area	**Frequency band**	**Modulation**	**Power**	**Max data rates**
GHz	**-**	**mW**	**Mbps**	**m**
5.82	$\frac{\pi}{4}$ shift QPSK	10	4.096	LOS: 400

Table 2.5: Characteristics of the communication

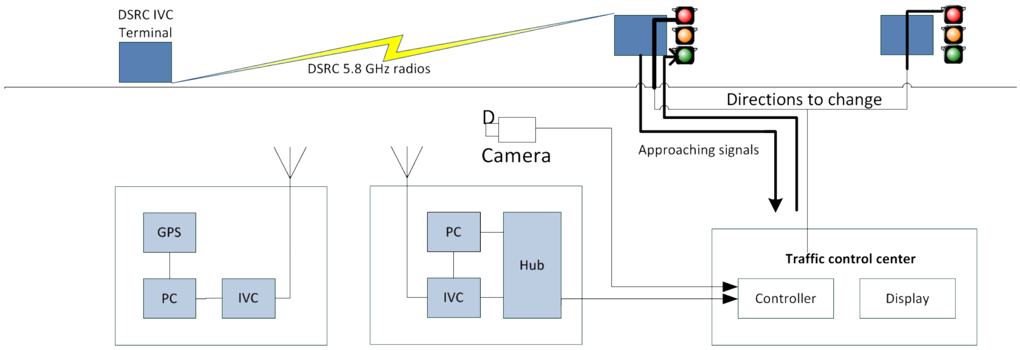


Figure 2.3: Configuration of the traffic control system (adapted from [55])

The main characteristics of the inter-vehicle communication are shown in the table 2.5. In addition, turbo codes guarantee high code rates through advanced error corrections and CSMA is used for the radio communication.

A reliable mobile communication link between the ambulance and the cellular networks, can be guaranteed by the use of cognitive routers, which are able to select the optimum link [55]. However, because of high development times for the interfaces of the Chinese communication system, the approach could not be tested. Moreover, the lack of medical equipments, which support WiFi, limited the tests for the transmission of patient data from the ambulance to the hospital. Therefore, the development of such medical equipments is essential for the proposed system.

2.3.4 Germany

The previously presented systems have elaborated on the technical equipment for the communication between the ambulance and the hospital in detail. However, no attention was paid to the communication needs of the paramedics within the ambulance. The German EMS system has been analysed with a focus on the inter-team coordination of emergency doctors and paramedics in emergency cases, and proposed the integration of a teledoctor system

[7]. The basic idea behind the teledoctor system is that a doctor, who is in communication with the paramedics inside the ambulance, has access to the medical records of patients through online databases. This approach is shown in figure 2.4. The paramedics transmit the information about the patient's health to the teledoctor and in return the teledoctor gives treatment instructions as well as the permission to execute the given instructions, which can legally only be allowed by a doctor. Therefore, a real-time communication between the paramedics and the teledoctor, via headset, is established. However, the paramedics are not only able to communicate with the teledoctor via headset but are also able to send pictures, videos, medical treatment information as well as information about the patient by a software application on a tablet. This application automatically forwards all information to the teledoctor, so that diagnosis during the ambluance mission can be made more easily [7].

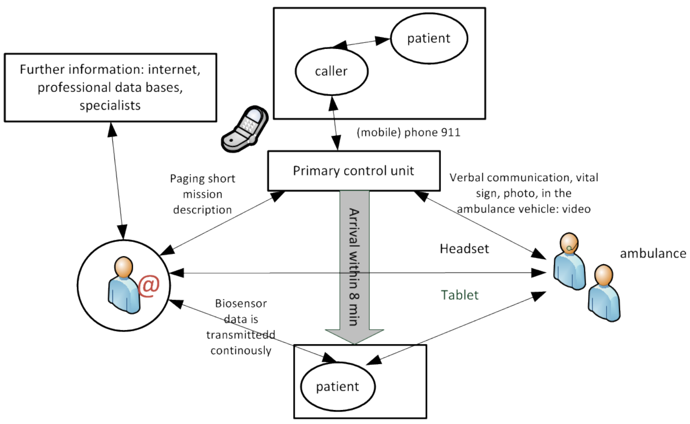


Figure 2.4: Teledoctor supports and authorizes paramedics on-site (adapted from [7])

Information Flow in the EMS

Medical teams (emergency doctors, paramedics) have been interviewed regarding the information and communication workflow during emergency cases as well as introduced the proposed teledoctor model to the medical teams to receive a feedback about the performance, the feasibility and the acceptance of the proposed system [7].

According to the interviewees the first information about the condition of the patient and the incident turns out to be incomplete or even false. Moreover, in most cases the patients are not able to provide reliable information about their medical history, because of their state of shock and the subsequent communication breakdown. In order to find the right medical treatment of a patient more easily the interviewees wish to get detailed information about the medical history of patients, especially in cases where old patients are unconscious and no information about the living will is available.

Emergency doctors have a wide range of medical expertise and are able to handle many emergency cases, but not all. Therefore, in same cases further medical knowledge is needed. The emergency doctors may rely on medical pocket books, call for expert help or transport the patient immediately to the hospital, whereby the emergency doctor has to decide, which hospital is the most suitable one for the patient. Moreover, the hospital receives relevant information about the patient's vital signs from the emergency doctor in advance and when the ambulance has arrived at the hospital the emergency doctor hands over the report with all collected data of the patient [7].

Teledoctor support in emergency cases

Participants of the teledoctor-test-study, who were not familiar with telemedical support for the communication and information workflow within an emergency case turned out to be very sceptic and averse to the teledoctor system. In addition, the significance of the use of pictures of a patient has been doubted. An emergency doctor has mentioned, that for the monitoring of the patient's health by a medical system, video material is necessary, but has cast doubt on the video material due to influences of the light. Another emergency doctor has remarked that the palpable impression a doctor gains through simply touching the skin of the patient cannot be displaced by a video.

Although the proposed teledoctor system illustrates several improvements of the current EMS, the big drawback of this system might be that the two doctors may have different treatment strategies or disturb each other during the communication via a headset. In addition, emergency doctors have mentioned that the communication via a headset irritates the elderly and in psychiatric emergency cases the communication can complicate the handling of the patient [7]. Moreover, experienced physicians on-site were only required for only 14.3 % of all medical procedures [17]. Therefore, well-trained paramedics are sufficient for most emergency cases.

The empirical findings of the proposed system in emergency cases are:

- In most cases the patients are not able to provide reliable information about their medical history. Therefore, physicians need access to medical health records such as medication lists or letters of performed surgeries.

- Emergency doctors must respect the last will of a patient. As a result, the access to such documents must be available in the field.

- The proposed communication between the ambulance and the hospital is very helpful and enables a fast medical treatment of patients. However, pictures and videos cannot replace the impression a doctor gains through simply touching the skin of a patient.
- The user acceptance of the system as well as the acceptance of the patients is crucial. In addition, the system must guarantee that patients feel safe and are not irritated by the technical system.

2.3.5 Comparison of the Systems

The proposed EMS systems that have been discussed in the previous sections will be compared in table 2.6. This comparison is based on several technical aspects such as the communication mechanism, the availability and the performance of the systems. Basically, all systems provide a communication channel between ambulance cars and the hospital. However, these system have certain differences in the establishment of such a connection.

	Greek	**U.S.**	**China**	**Germany**
Short description	Video conference between a paramedic and a doctor over HSPA	Network of vehicles that send the data with the help of a routing protocol to the hospital	Cellular antenna on the ambulance sends data to the hospital	Verbal communication via headset. Photos and vital signs are transmitted to a teledoctor.
Medical communication system	-	Not specified	✓	✓
Com. type	-	Not specified	802.11b/g	Not specified
Advantages	Faster than UMTS and GSM	No fees to pay, constant bandwidth	*	*
Disadvantages	Patchy bandwidth	Interconnecting vehicles required	*	*
Communication				
Type	Cellular network	Vehicular Ad Hoc Network (VANET)	Cellular network	Not specified
Average downlink	1 Mbps	>1 Mbps	Not specified	Not specified
Average uplink	200 Kbps	Not specified	Not specified	Not specified
Protocol	HSPA	WAVE 802.11p	802.11b/g	Not specified
Components	Laptop, HSPA-module, webcam	Vehicles	Cellular antenna, Laptop, Router, Camera	Headset, webcam
Availability	Medium-high	High	Low-high	Medium-high
Performance	Poor-high	High	High	High

* Not enough information provided to make a statement

Table 2.6: Comparision of the outlined EMS proposals

2.4 Electronic Health Records

In this section the Austrian health-information-system will be presented. This will not only include the information about the e-card, but will also illustrate the e-card infrastructure. In addition, the medical data, stored on the e-card, as well as the electronic signature service, which is provided by the e-card, will be discussed. Furthermore, the proposed extension to the German EMS system, the electronic Health Card that uses NFC, will be presented in this section.

2.4.1 E-card

In Austria the e-card is not only the key to the health system but also the key to personal medical data of a patient. With the handover of the e-card in a medical office and the following reading of the e-card by an e-card reader, the access to medical records is digitally signed as well as granted by the owner of the e-card and the medical records can be accessed by the physician. However, without the e-card, doctors, hospitals and all other partners of the social security institution are not able to view medical records of the patient [9]. Moreover, with the e-card the insurance companies are aware of all medical services, which a patient has made use of.

No medical records, but only the name, the academic title, the sex, the card serial number, the insurance number and the user group identification of a patient are stored on the e-card [9]. Moreover, the European Health Insurance Card (EHIC), located on the back side of the e-card, replaces the health insurance document for abroad, so that patients are able to use medical services in European Union member states, European Economic Area countries as well as in Switzerland. The data of the EHIC are not only printed on the e-card, but also stored on the chip of the e-card.

In order to exchange medical data, the Austrian medical information system (closed private network) is used. This system is only available for people in the health-care sector and has compared to other networks high requirements regarding the security, the availability and the quality of the data. In order to satisfy the special requirements of a hospital regarding the bandwidth a special eHI-Net-Connection is installed.

Moreover, the e-card replaces the health insurance certificate, which saves lots of paperwork and administration effort. The health-information-network (GIN would be the German abbreviation) is connected with the ADSL modem and the GIN-adapter to ensure the secure transmission of medical data (see figure 2.5). Value-added services of the eHealth network such as Internet-services or the transmission of the clinical report are processed via the same network [42]. The e-card application is installed on the GIN adapter and is necessary to communicate with the e-card server [9]. Moreover, the peering point securely forwards the data packages to the right locations. In order to guarantee a high performance and availability of the system two data centres with different locations are available.

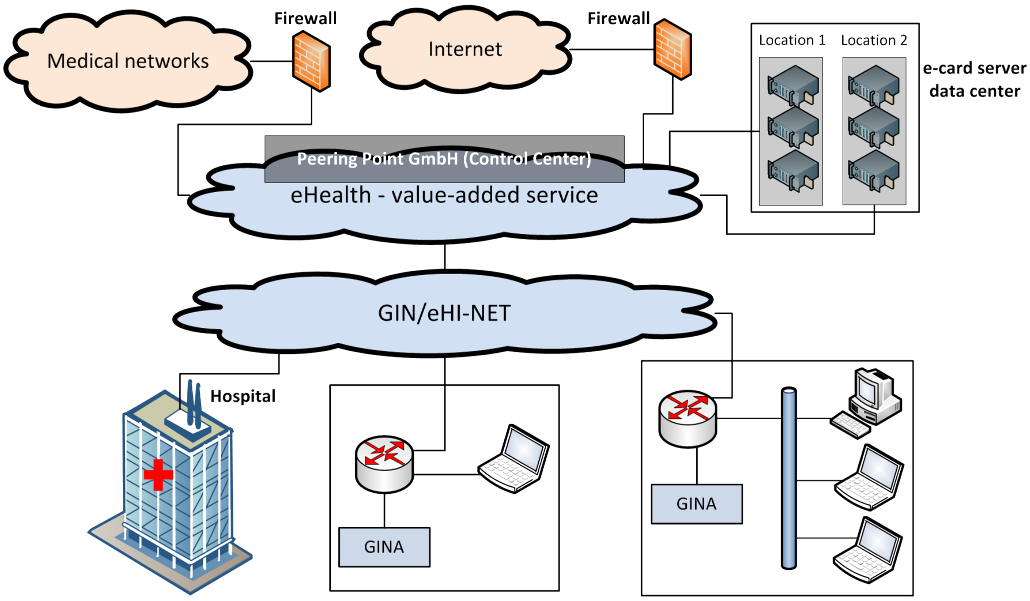


Figure 2.5: E-card infrastructure (adapted from [42])

The e-card includes, beside the health insurance certificate and the health insurance document for abroad, a number of services such as the electronic report of the inability to work (incapacity certificate), the limit of prescription charge and the pharmaceutical-approval -service. Moreover, a pilot project for another service, the e-medication, was performed from April to December 2011. As patients might not always know all drugs they are currently taking, e-medication collects prescribed and noln-prescribed drugs. Therefore, it is easier for doctors to prescribe further drugs, which do not interplay with drugs the patient already takes.

Furthermore, the electronic signature service, which is provided by the e-card, can be extended to a meet the requirements of the SigV [39] for non-medical digital signatures. These digital signatures are legally approved for the use of proceedings by authorities and can be equated with a handwritten signature.

Figure 2.6 illustrates the citizen card model. The citizen card is not only able to create digital signatures, but also provides functions for the their verification [5]. To go into more detail, for the creation of the digital signature a hash code is generated and encrypted with a signature function using a private key. The citizen is able to use all these described functions that are provided by the citizen card environment with the application. This application enables the ability to use the functions, which are included in the citizen card environment, at any time the user wants to. Furthermore, there are two interfaces for the access to the citizen card environment, the user interface and the security layer.

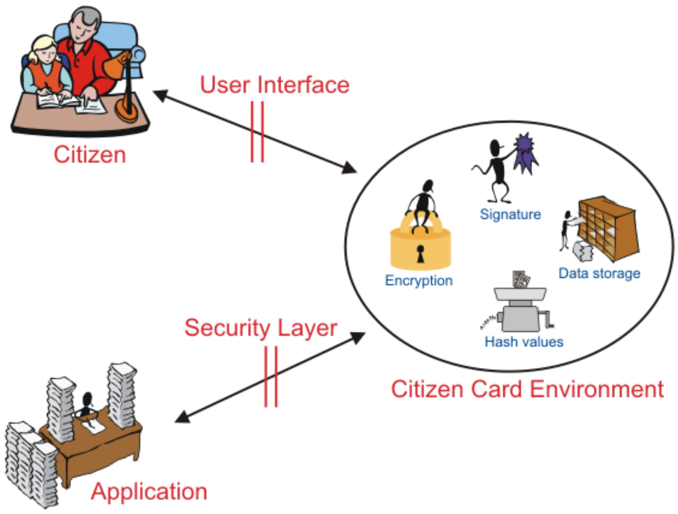


Figure 2.6: The citizen card model [5]

2.4.2 NFC

In the previous section a teledoctor was proposed as an extension to the German EMS and the evaluation of interviewed medical teams were given. This study revealed, among others, that physicians need access to medical documents of a patient in the field. Therefore, a electronic Health Card (eHC), which stores emergency data has been proposed in Germany. However, in an emergency physicians might not able to find the eHC smart card, especially in cases where the patient is unconscious. The proposition to this problem is to store medical data on tags and securely limit the access via the Near Field Communication technology (NFC) [13].

The Near Field Communication (NFC) technology was developed by NXP semiconductors and Sony in 2002 and enables the contactless transmission of messages over a small distance. This technology is based on the Radio Frequency Identification (RFID) [25][page 1] and does not only use standards of RFID but also standards of chip cards. The communication via RFID is based on active and passive components, whereby the active component (e.g. reader) provides energy for the transponder (e.g. chip card). The great advantage of NFC is that, in contrast to RFID, no separation between transponder and reader is given. A NFC device combines both functions, reader and transponder [25]. This technology supports transmission rates up to 424 kbit/s, has a reach of up to 0.2 meters and operates in the 13.56 MHz frequency band. The combination of a reader and a smart card makes NFC compatible for the use of payment and ticketing [22].

There are three different modes of operations that are support by NFC [22]:

- The *peer to peer mode (P2P)* enables the communication between two devices (e.g. mobile phones), which support NFC, whereby small data amounts such as social networking information are transferred [13].
- In the *read/write mode* a NFC device is able to read and modify data, stored on a NFC tag [22]. A practical example are tags with additional information such as a URL, which are attached to SmartPosters [13].
- With the *card emulation mode* the NFC device can be used as smart card. This mode of operation can fulfil any function, which can be provided by a contactless card (e.g. payment) [22].

All three modes of operation have security issues, denial-of-service attacks and eavesdropping are the most common ones. In case of the proposed NFC tag, the issues concerning the read/write mode have to be considered to ensure a secure storage of medical data. Therefore, a secure area on the NFC tag must ensure that only authorized people get access to medical records as well as to the key for the decryption. A secure element, which provides such a secure area, can be either removable (e.g. SIM card) or non-removable (e.g. embedded hardware).

The German telematics infrastructure (TI) does not only provide services such as encryption, authorization of emergency data and digital signatures, but also interacts with information systems of several care providers to distribute and manage medical data records [13]. These services are provided by a local *Connector*, which establishes a secure connection to the central servers via a virtual private network (VPN). The access to the eHC can be established by the help of smart card readers, whereby the *Connector* communicates with the smart card readers to get access to the data, which is stored on the eHC. The private key, which is not only necessary for the encryption of the medical data, but also for providing the use of digital signatures, is securely stored on the smart card chip of the eHC, whereby the decryption of the encrypted key is performed by the microprocessor of the smard card. Patients are able to encrypt the medical data with public keys, which are provided by health care institutions. Thus, physicians of such health care institutions are able to get access to this medical data. However, the identity of the physician has to be be clarified first. This is done by the help of the physician's certificate, which can either be found on the health professional card (HPC) or gained via a public key infrastructure. In order to encrypt medical data for more than one institution, the smart card must store multiple private keys. Moreover, patients must be able to decide which institutions get access to their medical data. To technically support this requirement the medical data is encrypted with the public key of the patient and can only be decrypted with the patient's private key. Furthermore, patients must be able to bring forward all medical records, which are stored on the eHC. Therefore, three different interfaces are supposed to provide this requirement.

- Point of information (POI) terminals
- Patient front-end
- Online front-end for home usage

Figure 2.7 shows how the secure exchange of medical data works. In order to limit the access to medical data records the whole data set is encrypted with a symmetric key given by the Connector service (1). As the symmetric cryptography requires the same key for the en- and decryption, the symmetric key must be protected. This is done by the help of public cryptography. First a key duple (private key, public key) is generated and then the medical data are encrypted with the public key (2). The encrypted material (data records, key) is stored on a SemTag NFC tag, if necessary on more than one SemTag (3). The token is carried around by the patient at home and will be used by physicians in case of an emergency (4). In order to read and decrypt the data stored on the NFC tag a device, which supports RFID and provides a smart card reader, can be used (5). The encrypted symmetric key can be decrypted with the smart card of the physician, which provides the private key of the generated key duple (6). The decryption of the medical data, which is stored on the NFC tag, is established with the combination of the SemTag software component and the Connector (7). Finally, the medical data can be read through the use of a mobile device such as a tablet (8).

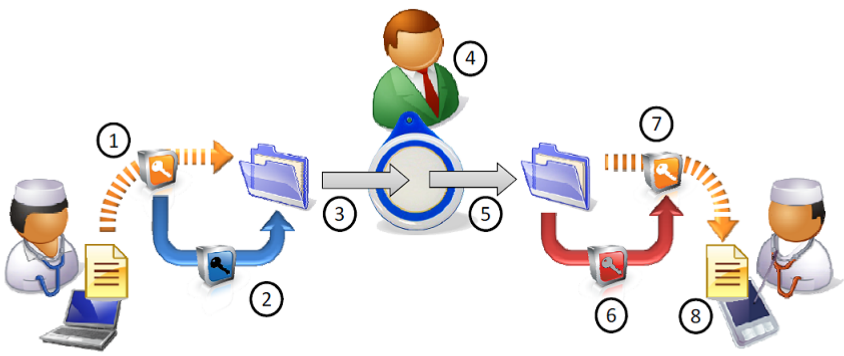


Figure 2.7: SemTag Process Routine [13]

In order to limit the access to the data, which is stored on SemTag NFC tag, a Secure Module Card (SMC-B) can be used. Moreover, such a tag can store data up to 32 kilobyte, which is more than the eHC card. For the proposed SemTag NFC tag, the emergency data is set up to 7 kilobytes.

2.5 Different Operational Area

The field of operation of tablets as a communication device ranges from medical- to logistic systems and even military systems. To get a read of the operation fields three different systems will be presented in this section.

2.5.1 Voice-Commandable Robotic Forklift

The development of tablets and smart phones with powerful processors have enabled the use of voice recognition as an input type for several systems. An example would be the system, in which a voice-commandable robotic forklift, which interacts with users through a tablet, is used in outdoor military warehouses [53]. Several cameras, mounted on top of the forklift, as well as sensors enable an automatic transport of pallets from one direction to another without the help of GPS. In order to guarantee a good interaction with the user, all camera outputs can be viewed on the tablet. The desired location can be selected through a circling gesture on the tablet and with a voice-movement command the forklift moves to the marked circle. The speech recognition as well as the pen-gestures are processed by the tablet and by the help of sensors and a pallet estimation algorithm an obstacle-free way to the next pallet can be calculated (see figure 2.8).

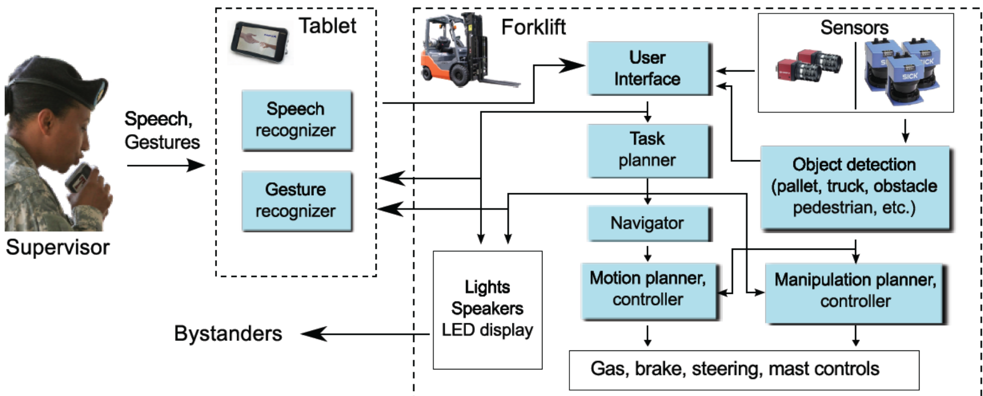


Figure 2.8: High-level system architecture [53]

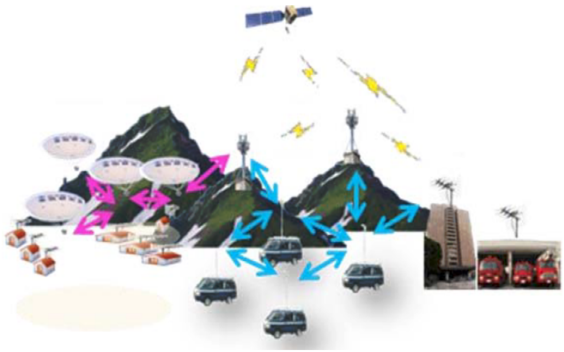


Figure 2.9: Proposed disaster information system [57]

2.5.2 Never Die Network

Emergency systems rely on the availability of communication systems to make an early intervention possible. However, in a disaster situation (e.g. earthquake, typhoon) the access to these systems might not be possible. Therefore, disaster-hit countries cannot rely on general communication systems such as the Internet or cellular networks. Special systems have to be established to guarantee the data communication in disaster situations. A special system, which combines satellite network systems with a cognitive wireless network system, has been proposed [57]. Fixed wireless base stations, wireless cars as well as a ballooned wireless network (see figure 2.9) serve as communication system. In order to guarantee the electricity supply of the wireless network components solar energy systems are used. Moreover, the wireless network devices on the ground are connected with devices on the balloons as well as the satellite network to enable the interaction between the components. Verbal communication is not only provided by the cellular network but also through a VoIP server within the illustrated network in figure 2.10. In order to guarantee the data connection in case of a breakdown of some wireless devices the link between the devices as well as the route within the network is recalculated.

2.5.3 Tactical Communication System

Rugged tablets cannot only be used as basic outdoor device but also as communication device for military use in battlefield environments. The communication system "One Force Tactical Communication System (OFTCS)", which uses a hybrid cellular-tactical network consisting of cellular and WiFi communications as well as the tactical mobile ad-hoc system (MANET), has been presented [62]. The OFTCS provides mission command services as well as video-,voice- and data sharing services for the communication between soldiers in the

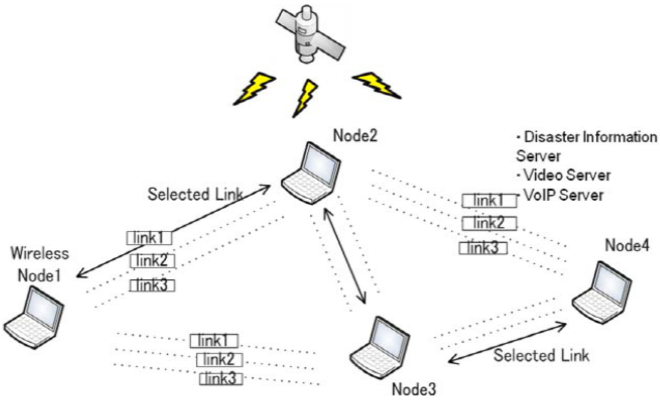


Figure 2.10: Proposed network configuration [57]

battlefield. In case of medical emergencies medics can be called via the command-and-control messaging service or via the VoIP service. To protect the data integrity of the data transfer within the network the Advanced Encryption Standard (AES) with a 256-bit security key is used. The tactical network backbone is provided by the Mobile Ad-hoc Interoperable Network GATEway (MAINGATE) and enables the integration of 3G/4G cellular networks. Figure 2.11 illustrates the use of the OFTCS in the AEWE Spiral G Network. Commanders, team leaders and the White Cell are provided with smart phones and tablets, which are equipped with a One Force Tracker (OFT) mission command client application to communicate via the network [62].

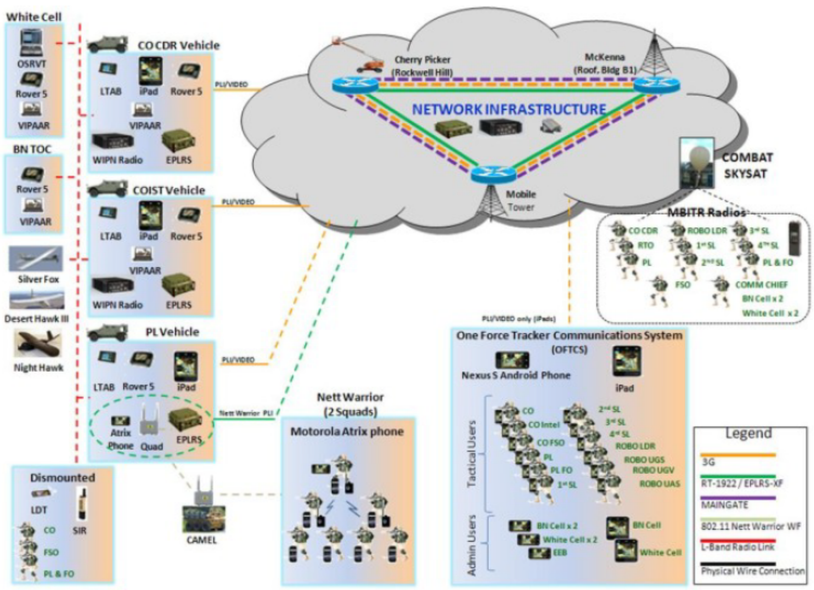


Figure 2.11: AEWE Spiral G Network Architecture View [62]

2.6 Standards

In order to define the application depended requirements of a system, several international standards as well as laws of the country, where the system will be used, have to be taken into account. Guidelines such as for the processing and transmission of medical data, the use of electronic signatures, connectors for electronic equipment as well as the international protection standard for electronic equipment have to be observed.

2.6.1 Ingress Protection Rating (IP)

The IP-classification defines the resistance of electronic equipments against water and dust and can be tested in accordance with several standards such as the European standard "EN 60529" [49]. Furthermore, the IP-classification is represented by a two-digit number, whereby the first number specifies the dust- and the second one the water resistance.

2.6.2 UL1604 & ATEX

For the functional operation of electrical equipments, used in hazard areas, special requirements concerning the robustness against explosive atmospheres have to be defined. In order to know which requirements are needed for which hazard areas, three different classes of hazards are distinguished: flammable gases (class 1), combustible dust (class 2), ignitable fibers & flyers (class 3) [15].
Moreover, for the use of electrical equipments in such areas, the UL1604- and the ATEX safety standard are defined. The UL1604 certification defines that an electrical equipment can be used in class I and II, Division 2, and class III hazard areas. In addition, a ATEX certification electronic equipment can only be used in “an area in which an explosive mixture is not likely to occur in normal operation and if it occurs it will exist only for a short time” [15]. Moreover, four ATEX classifications are defined to guarantee the safe operation for the specific application: *Industrial or Mining Application*, *Equipment Category*, *Atmosphere* and *Temperature*.

2.6.3 Mil-Std-810

Generally, the Mil-Std-810 is an environmental test method that is a standard for military equipments defined by the U.S. Department of Defense (DoD). However, this standard is also used for rugged electronic equipments. The MIL-STD 810G was defined on the 31st of

October in 2008 and contains a list of test methods to guarantee the equipment operation due to certain circumstances such as high- or low temperatures, humidity, dust, vibration and shock. Some test methods will be discussed in the following paragraphs [15].

High Temperature: MIL-STD 810G Method 501.5 - The effects on equipments caused by high temperatures are explored with this method, by which the equipment will be tested while it is turned on as well as turned off. Table 2.7 shows the climate dependent temperatures for different areas to determine the maximum temperature in which the equipment will be used.

Design Type	**Location**	**Ambient Air**	**Induced**
		°C(10°F)	**°C(10°F)**
Basic Hot (A2)	Many parts of the world, extending outward from the hot dry category of the of the southwestern United States, northwestern Mexico, central and western Australia, Saharan Africa, South America, southern Spain, and southwest and south central Asia.	30 - 43 (86 - 110)	30 - 63 (86 - 145)
Hot Dry	Southwest and south central Asia, southwestern United States, Saharan Africa, central and western Australia, and northwestern Mexico.	32 - 49 (90 - 120)	33 - 71 (91 - 160)

Table 2.7: High temperatures (adapted from [58, p. 74])

Low Temperature: MIL-STD 810G Method 502.5 - The performance as well as the operation of equipments under low temperature conditions are tested with this kind of method. Therefore, the climatic conditions have to be identified to gain the information about the temperature range in which the equipment will be used (see table 2.8).

Design Type	**Design Type**	**Temperature**	
		Ambient Air	**Induced Environment (Storage & Transit)**
		°**C**(10°**F**)	°**C**(10°**F**)
Basic Cold (C1)	Most of Europe; Northern contiguous US; Coastal Canada; High-latitude coasts (e.g., southern coast of Alaska); High elevations in lower latitudes	-21 to -31 (-6 to -24)	34
Cold (C2)	Canada, Alaska (excluding the interior); Greenland (excluding the "cold pole"); Northern Scandinavia; Northern Asia (some areas), High Elevations (Northern and Southern Hemispheres); Alps; Himalayas; Andes	-37 to -46 (-35 to -51)	-37 to -46 (-35 to -51)
Severe Cold (C3)	Interior of Alaska; Yukon (Canada); Interior of Northern Islands; Greenland ice cap; Northern Asia	-51(-60)	-51(-60)

Table 2.8: Low temperatures (adapted from [58, p. 87])

Temperature Shock: MIL-STD 810G Method 503.5 - The functional performance as well as the safe operation of equipments in case of sudden temperature changes (changes greater than 10°C/minute) is tested with this type of method [58, p. 93].

Rain: MIL-STD 810G Method 506.5 - The protection against dripping water, water spray as well as rain is found with this type of method [58, p. 154-156].

- *Procedure I - Rain and Blowing Rain:* This test procedure can be applied for outdoor equipment-protection-checks against rain and blowing rain, whereby a minimum water rate of 1.7 mm/min is applied for the test.
- *Procedure II - Exaggerated:* If the equipment of test is too large and a blowing-rain facility is not available this procedure can be applied.

- *Procedure III - Drip:* The equipment is tested regarding the protection of falling water or possible leakages, whereby two different tests can be distinguished: The first test checks the protection against falling water, which is generally caused by condensation, and the second test checks the resistance against heavy condensations or leakages from above.

Sand and Dust: MIL-STD 810G Method 510.5 - This test method is used to assess the effects of dry blowing dust or blowing sand conditions [58, p. 209-210].

- *Procedure I - Blowing Dust:* This test procedure is used to investigate the dust resistance of equipments through a concentration of blowing dust ($< 150\ \mu m$), which could get through openings or cracks into the equipments.
- *Procedure II - Blowing Sand:* The functional performance of equipments is tested for locations with blowing sand conditions (150 μm to 850 μm).

Vibration: MIL-STD-810G Method 514.6 - The vibration test method determines whether the equipment is able to withstand certain vibration procedures or not, whereby these procedures range from general vibrations through to aircraft store carriage [58, p. 267].

- *Procedure I - General Vibration:* This test procedure is defined for the transportation of equipments within a vehicle.
- *Procedure II - Loose Cargo Transportation:* The transportation of unsecured equipment within a vehicle is tested with this type of procedure.
- *Procedure III - Large Assembly Transportation:* With this procedure vibrations in case of large group of equipments, which are installed or carried within a vehicle, is checked.
- *Procedure IV - Assembled Aircraft Store Carriage and Free Flight:* The carriage of equipment within planes as well as free flight phases are tested through this procedure.

Shock: MIL-STD 810G Method 516.6 - The impact of mechanically caused shocks regarding the physical power to withstand and the functional performance of equipments is determined with this type of method [58, p. 370]. Moreover, these shocks do not exceed a frequency of 10 GHz and a duration of more than one second [58, p. 370]. There are several procedure to produce a shock, but the transit drop (procedure IV) is the most important one. The height of drop is defined between 0.46 and 1.22 meter and depends on the length and weight of the equipment. In addition, the maximum height of drop is performed for items smaller than 0.91 m and a weight less than 45.5 kg (e.g. rugged electronic equipments such as notebooks, tablets or smartphones) and the test is accomplished for the twelve edges, eight corners and six faces (total 26 drops) of the device of test [58, p. 399],[11].

2.6.4 Medical Data

In order to process confidential electronic health records several country-dependant standards and guidelines have to be observed. In Austria the national data protection law regulates the processing and storage of personal data.

However, regulations concerning personal data do not only depend on a country's legislation, but also on the European data protection directive, which governs the processing of personal data, has to be observed and applied by each European Union member. As stated in the European council regulation (EC) [40] all member states must "take all necessary technical measures to protect such data against any accidental or illicit destruction, accidental loss, deterioration, distribution or unauthorised consultation". The same principle has to be applied for the protection of medical data.

In order to meet these requirements the authentication and access rights, the data integrity, the data confidentiality as well as the proof of origin has to be guaranteed.

Therefore, the standards and guidelines for the usage of informatics in the Austrian health service (STRING) commission of the Federation Municipal Administration (Bundesmagistrat in German) has defined the MAGDA-LENA (the medical-administrative health data exchange-logical and electronic network Austria) guidelines that should help the establishment of a secure personal data exchange system [8]. Those guidelines are no legal obligation, but guarantee the Austrian data protection regulations for the medical personal data exchange by organizations that have the legal competence or the legal power by §7 of the Austrian Federal Ministries Act to exchange such data [37]. MAGDA-LENA includes suggestions regarding the data security, the use of encryption algorithms and corresponding key lengths, electronic signatures, as well as user authentication and access rights mechanisms. In order to have an overview of the included technical aspects for the realization of a secure data communication, some parts of the *data encryption* as well as the *electronic signatures* will be presented in the following sections.

Moreover, the medical data cannot be legally processed for any reason, but

> preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, and where those data are processed by a health professional subject under national law or rules established by national

competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy. [41]

Moreover, the § 14 of the Austrian national data protection law mentions, that the processing of medical data can also be used for statical analysis [37].

Furthermore, according to § 26 of the Austrian national data protection law organizations must provide information about the personal data. In addition to this, not only the information about the stored personal data, but also the purpose of the storage and the names and addresses of organizations that process those data, must be provided [37].

Data encryption

A login procedure must guarantee that only authorised authenticated users get access to electronic health records, whereby each access has to be electronically recorded, whether the access has been granted or not [8]. Moreover, medical records have to be securely sent from one end of the network to another through encryption methods, which meet certain requirements. Those requirements include the minimum length of the symmetric key, protocols for the encrypted communication as well as guidelines for the key agreement. In order to guarantee data confidentiality, the medical health records have to be encrypted with a symmetric key of a minimum length of 80 Bit, whereby the following cryptographic methods could be used [8]:

- IDEA
- 3DES with two keys
- AES candidates

In addition, the following aspects have to be considered for the key management for data encryption purposes:

- During the key exchange, the secure authentication of the two communication parties, based on certificates, must be guaranteed.
- For the creation of the symmetric keys pseudo or true random number generators could be used. In case of pseudo random number generators, the randomness of the numbers must be guaranteed.
- No forward- or backward prognoses should be possible with pseudo random numbers, generated by the help of seeds.

In order to securely send data from one end of the network to another protocols, which guarantee a secure communication, must be used, whereby the preferred ones are the following.

- S/MIME
- SSL
- TLS
- IPSEC

Electronic signatures

There are several limitations for the usage of electronic signatures defined by the Austrian digital signature law [36]. Two of them are presented in the following listing.

- In sections, where written forms are necessary, secure electronic signatures should be created in pursuance of the Austrian digital signature law [36].
- The methods, key lengths and strengths of the secure digital signature creation procedures should be adhered to, even though there is no need for secure signatures.

In order to observe the law, security tokens can be used. However, there are several requirements for the usage of security tokens. Some of these requirements are presented in the following listing.

- Technical ways (token) are necessary for the use of electronic signatures, of which the requirements of security criteria are regulated by the Austrian electronic signature law. Moreover, additional requirements are defined by the ENV 13727 health informatics standard.
- It is only allowed to use processor cards for stationary use with special security modules. The activation of the tokens can either be accomplished by pass phrases o biometric characteristics.
- The security token is used for the authentication of the user and to ensure the data integrity, in which the generation of the asymmetric key has to be guaranteed. The general conditions such as the used algorithm and the key length must be gathered from the Austrian statutory provision of the digital signature decree (SigV) [39].
- The evaluation of the security tokens has to follow the standards of the SigV regarding the inspecting authority, confirmation authority and the general conditions.

2.7 Summary

In this section some patient documentation systems that are used in Austria have been presented. Moreover, two basic concepts of an Emergency Medical Service (EMS) and several systems that are proposed in some countries have been discussed. The latter EMS systems have been compared regarding some technical aspects. To put the results in a nutshell, cellular networks are commonly used for the communication between the ambulance and the hospital. However, the performance of this communication type depends on the area in which the system is used and ranges from poor to very high. Moreover, the Austrian medical-information-system has been introduced. In addition, the importance of the e-card, the data stored on the e-card and the signature mechanism used by the e-card has been discussed. However, apart from the e-card, there are also other types of health-information-cards. The proposed extension to the German EMS system, the electronic Health Card that uses NFC, has been discussed. Furthermore, some different operational areas, which are somehow related to the documentation of patient data, have been presented. There are several standards, which have to be considered, for the processing of medical data. In Austria the data protection law regulates the access to such medical data. In order to observe the law some parts of the MAGDA-LENA guidelines regarding the data encryption and the usage of electronic signatures have been elaborated on.

3 Design

This chapter focuses on the requirements of the patient terminal regarding the hardware and the user interface as well as the storage of the medical data. In addition, solutions that meet these requirements will be elaborated and discussed. At first, several possible hardware systems and input devices will be compared in section 3.1. Then general system requirements will be discussed and the system architecture will be illustrated in section 3.2. In addition, the connection to medical devices and the related standards will be analysed. The basis for this analysis are medical devices that are used in the ambulance cars of the Styrian Red Cross. Furthermore in section 3.3 the requirements for the storage of medical devices will be presented. In addition, the possibility of a diagnostic database will be discussed. On the one hand, the data has to be stored, but on the other hand services must be provided to retrieve data sets of the database. Therefore, in section 3.4 two services that enable the forwarding of data over the network will be delineated and the advantages and disadvantages will be discussed. Finally, in section 3.5 requirements of the user interface as well as guidelines for designing mobile applications will be explained. In addition, authentication methods and the possibility of digital signatures for the signing of mission protocols will be elaborated on.

3.1 Hardware Components

In this section requirements regarding the hardware components will be pinned down. Based on these requirements a system for the patient terminal will be selected. Moreover, several aspects of different input devices will be elaborated on.

3.1.1 Requirements

Ambulance services must satisfy certain hygienic requirements to protect patients with weak immune systems from bacillus infections [12]. Therefore, physicians and paramedics are forced to not only to clean the interior of the ambulance but also to wear disposable gloves during the ambulatory treatment of patients. Moreover, the ambulance service is performed at any time and nearly everywhere regardless of the weather as well as the road condition.

Hence, in order to provide a terminal, which can be effectively used in the ambulance, several requirements from the system or communication perspective to the hardware perspective have to be considered. The following list of requirements concerns the hardware perspective and serves as selection criteria for the tablet, which will be used in the ambulance:

- The terminal must be robust enough to withstand vibrations and jars inside a vehicle as well as a fall from 1 meter.
- The perfect function after the disinfection of the terminal must be guaranteed and the terminal has to be operable with disposable gloves.
- The resistance against splashing water and dust must be ensured. In addition, the terminal has to be protected by a protection film.
- The terminal must include several communication interfaces such as WLAN, GSM and Bluetooth.
- There should be a possibility for a pen input.
- Not only the heat stability but also the resistance to cold has to be guaranteed.
- The weight and heat generation of the tablet must ensure a pleasant operation of the tablet on the lap of a physician.
- A docking station should enable the easy charging of the tablet.

3.1.2 Analysis

Based on the elaborated requirements above, a hardware selection has to be made. Therefore, four different rugged tablets have been selected to compare the strengths and possible weaknesses of each tablet more easily (see table 3.1).

The *Motion C5t* tablet [32] is especially designed for health care environments and enables the access to patient data everywhere and at any time. With the integrated camera pictures can be taken and added to the Electronic Medical Record (EMR), a process in which the access to the patient's data is protected by a biometric fingerprint system and optionally with a smart card. Moreover, the identification of physicians or patients can be established with the optionally included RFID reader.

In contrast to the *Motion C5t*, the *Fieldbook B1* [14] is ruggedized for outdoor environments and additionally features the NFC protocol as well as provides an optional 4G LTE module. Moreover, a light sensor adjusts the brightness of the display and enables to read data even in direct sunlight.

A very interesting communication approach for the use within an ambulance are the included front- and back cameras of both, the *Motion C5t* and the *Fieldbook B1*. With the front camera physicians may start a video conference session with doctors in a hospital and with the back camera pictures of patients may be taken and sent to the hospital. Moreover, with the provided near field communication technology RFID, physicians could be easily identified.

The *DLOG PWS-770* [1], on the other hand, has been especially designed to combine the requirements of in- and outdoor environments. Moreover, a fingerprint scanner enables the identification of users. In comparison to the *Motion C5t*, the *Fieldbook B1* and the *DLOG PWS-770*, the *JLT jFlex* [23] is not conform to any military standard. However, this rugged tablet has been especially optimized for vibration environments such as in vehicles.

The hardware costs for the purchase of *Fieldbook B1*-tablets strongly depends on the number of pieces. The Fieldbook B1 listed in table 3.1 ranges approximately from 1500-2000€/piece. With a very high number of pieces the price might be lower.

As one of the hardware requirements states that the tablet must be operable with disposable gloves a resistive touch screen is mandatory. Hence, the capacitive touch screen of the *Motion C5t* is not acceptable and cannot be productively used within the ambulance. The *JLT jFlex* is especially designed to withstand the vibrations within an ambulance, but neither a SIM slot nor RFID is provided. In contrast to the *JLT jFlex* and the *Motion C5t* the *Fieldbook B1* as well as the *DLOG PWS-770* satisfy all requirements and provide features that could be used in the future. However, in comparison to the the *Fieldbook B1* the RFID module of the *DLOG PWS-770* does not feature the NFC technology. Therefore, the *Fieldbook B1* would be the best solution for ambulance services.

	DLOG PWS 770 [1]	**Fieldbook B1 [14]**	**Motion C5t [32]**	**JLT jFlex [23]**
Processor	Atom N2600 1.6GHz	Atom N2600 1.6GHz	Core i3 1.9GHz	Atom N270 1.6GHz
Main memory	1-2GB DDR3	2GB DDR3 800MHz	2-4GB DDR3 1600 MHz	2GB
Operating system	Windows 7 Professional	Windows 7 Professional	Windows 7 Professional	Windows 7
Display				
Size	10.4"	10.4"	10.4"	8.4"
Resolution	1024x768	1024x768	1024x768	800x600
Resistive touch screen	✓	✓	-	✓
Weight	1.2 kg	1.475 kg	1.5 kg	1.9 kg
Battery	1900mAh	3800 mAh		
Extended battery	5000mAh	4200 mAh		
Communication support				
RFID	✓	✓	✓	-
GPS	✓	✓	-	✓
NFC	-	✓	-	-
Bluetooth	✓	✓	✓	✓
WLAN	✓	✓	✓	✓
SIM slot	✓	optional	✓	-
Camera				
Front	-	2 M	1.2 M	-
Back	2 M	5 M	3 M	-
Connections				
Docking	✓	✓	✓	✓
USB	✓(v 2.0)	✓(v 2.0,2x)	✓(v 3.0)	✓
LAN	-	✓	-	✓
RS232	✓	✓	-	-
VGA	✓	via docking station	via docking station	-
Environmental conditions				
Storage temperature	-20°C to 60°C	-30°C to 70°C	-20°C to 60°C	-30°C to 70°C
Operating temperature	-10°C to 50°C	-20°C to 50°C	-10°C to 40°C	-20°C to 50°C
Sand & dust, water	IP-54	IP-65	IP-54	IP-65
Vibrations	MIL-STD-810G, Method 516.5	MIL-STD-810G, Method 514.6 Procedure I	IEC 60068-2-6	5-500Hz/4.5g RMS 3 hours XYZ
Humidity (non operating)	5% - 95% at 40°C	95%, 30°C to 60°C	8% - 80%	10-95%

Table 3.1: Hardware comparison

3.1.3 Input Devices

A research on gestural interactions of people, who are at the wheel, has been presented [45]. Although, this research does not exactly fit into the specific field of application, the service protocol is filled in on seats in the back of the ambulance without the need to pay attention on the road, some approaches can be adopted:

Physicians might be distracted by patients, vibrations in the vehicle or other physicians during the creation of the service protocol. Therefore, physicians should not be forced to pay attention to an additional external device such as a keyboard or a mouse. Moreover, in case of strong vibrations external devices might fly around and hit the patient. In order to prevent such a scenario, the multi touch screen as well as the integrated keyboard on the tablet could be used. However, the touch screen must guarantee that even people with big fingers are able to easily hit the right button [45]. Therefore, the tablet has to be big enough to guarantee an effective gesture input on the touch screen, which excludes tablets under a size of 10 inches.

Another approach would be the use of electronic clothes as input device. There is also the possibility of touch applications on E-textiles performed through capacitive-sensing techniques [59]. This can be performed through several different methods including piezoresistive coatings and printing materials. However, with these techniques the clothes cannot be washed without damaging the material. Therefore, conductive polymeric fibers and metallic fibers overcome this problem (e.g. gold, copper) [59]. With the introduction of these fibers digital sewing machines, controlled by CAD programs, have been developed to interconnect sensing surfaces and connection pads [24]. An example of such a e-textile system is the jacket equipped with a textile data bus as well as a textile main board, which enables the control of media devices through touch gestures on a textile touchpad [24].

Although several applications for e-textiles exist the use of such a technology has not been fully developed for the integration of smart phones or tablets.

3.2 System Architecture

The Styrian Red Cross has provided a system architecture that forwards mission related information to the data terminal. This architecture will be extended by the patient terminal located in the transport area of the ambulance cars (see figure 3.1). Moreover, the connection with medical devices in the ambulance car will be elaborated.

3.2.1 Requirements

There are several requirements, which have to be considered concerning the integration of the patient terminal and the storage of the medical data, that will be filled in on the digital mission protocol application by the paramedics. These requirements lay the foundation for the documentation of patient related data.

- Authentication on the patient terminal
- Creation of a mission protocol database
- Compliance of data security standards
- Connection to the operating mission system

3.2.2 Patient Terminal System Overview

In figure 3.1 the system architecture for the processing of medical data is illustrated. The patient terminal is connected to a data terminal via WLAN in the ambulance car. In addition, the data terminal is connected to the gateway server, which forwards messages of the operating mission system. Due to the fact that the unauthorized access to valuable medical data has to be prevented, the WLAN connection has to be encrypted. In addition, the data integrity could be ensured by an additional encryption of the medical data.

Moreover, the mission protocol data, that has to be filled in by the paramedics, has to be stored somewhere in a database. Due to the high security standards for the processing of medical data, a secure location has to be found. Additionally, the storage of the medical data on the patient terminal violates the Austrian data protection law. Therefore, the medical data is stored in a database on the gateway server. As the data cannot be directly accessed on the gateway server, Services must be provided. In section 3.4 such services will be discussed in more detail.

Basically, the graphical mission tool located on the mission operating system server is not only able to dispose but also update missions. This mission data is forwarded by the Mdt-Server to the Gateway-Server. The gateway-server knows the address and the hostname of all connected data terminals and forwards the messages to the related data terminal. Then, the data terminal forwards the message to the patient terminal. However, further details about the message exchange and the medical test data will be discussed in section 4.3.

The patient terminal processes the data and displays the parsed data on the screen. Thus, the paramedics do not have to fill in many mission data fields, as most information is provided by the operating mission system.

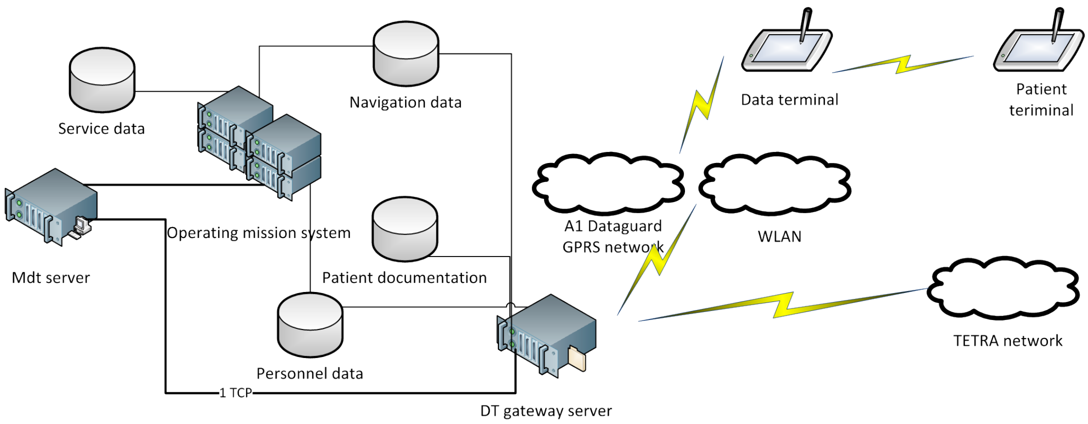


Figure 3.1: System architecture

Operating Mission System

The operating mission system (ELS would be the German abbreviation) enables not only the disposal of ambulance services within the Red Cross districts in Styria, but also the management of their assigned units by the control of the data terminals in the ambulances. In order to establish a communication between the data terminals and the service guidance system a gateway server is used. This gateway server is connected via LAN with the service guidance system, whereby a Mdt protocol enables the communication between them. In addition, the databases on the server guidance system can be accessed by the gateway server. The operating mission system is not provided by a single server, but consists of several interconnected components, which are all located in the headquarters of the Red Cross in Graz. Moreover, Windows Server 2008 is used as operating system and the database is provided through the Microsoft SQL Server 2005.

Mdt-Server

The service guidance system cannot be accessed directly, but by a Mdt-server. However, the communication with the Mdt-server can only be established through a single TCP connection, so that for each additional communication channel a separate Mdt-server must be used. The communication to the Mdt-server is established by a Mdt protocol. This protocol represents a custom data format, which has been especially developed, for the communication with the service guidance system, by the firm InterGraph. Furthermore, as operating system the Mdt-server relies on Windows Server 2003.

Gateway Server

The gateway server is responsible for the transmission of data packets between the data terminals in the ambulances and the service guidance system. This connection is established via WLAN and GPRS between the data terminals and the gateway server and via LAN between the gateway server and the operating mission system. Moreover, the same operating system as for the service guidance system is used for the gateway server.

Gotive H42 Data terminal

The data terminal is connected with the docking station in the ambulance and provides a service management application for all ambulance services, which have been assigned to the specific unit. This device does not only provide interfaces for the connection to E-cards, but also supports the communication with a CAN-bus, the switching state of the emergency light and the management of the pager through the mobile radio. The service management application has been developed with C# and are applied for approximately 250 data terminals.

Patient terminal

The patient terminal is a rugged tablet that is connected to the data terminal via WLAN. Moreover, on the patient terminal a patient documentation application for the creation of a digital mission protocol is provided. Due to the fact that the patient terminal may also be used in outdoor environments, the use of a GPRS-communication to the gateway server would be useful. However, for testing purposes a WLAN connection will do the trick. Thus, the patient terminal has to be in reach of the WLAN-network to communicate with the data terminal. Furthermore, the communication between the patient terminal and the data terminal will be established by a simple server-client application.

3.2.3 Medical Devices

There are several communication problems between medical devices due to the lack of well defined standards. In order to solve the interoperability problem between medical devices several international organizations work on standards concerning the transmission of medical data on upper-layers of the OSI-model. Three groups of standards are discussed in this section.

DICOM (Digital Imaging and Communications in Medicine)

The DICOM standards are developed by the U.S. National Electrical Manufacturers Association (NEMA) and define specifications for the transmission of medical image data including the file format, the storage as well as the transmission strategies. These standards are commonly applied to information systems in hospitals to process, store and transmit medical images [20].

HL7 (Health Level Seven International)

HL7 is a set of standards for the processing of electronic healthcare data within an information system [20]. Moreover, standards for the application layer (layer 7) of the OSI model are defined by the HL7. HL7 does not only refer to the set of standards but also to the standards organization, which include several work groups, such as the Electronic Health Record Work Group, for defining HL7 standards [20].

CEN ISO/IEEE 11073 Health informatics - Medical / health device communication standards

This group of standards defines specifications for the medical data transmission between medical devices. Moreover, in order to provide low power consumptions for battery powered medical devices standards for the communication mechanism are defined by the ISO/IEEE 11073 Personal Health Data working group. This working group has defined the message exchange strategies for a list of medical devices, which currently includes pulse oximeters, heart rate monitors, blood pressure monitors, thermometers, weighing scales and glucose meters, whereby standards for further medical devices may be added in the future. [48]

There are several medical devices inside the ambulance, which support wireless communication technologies. However, the lack of used standardized protocols for the transfer of medical data complicates the processing of these data sets. Moreover, not all district offices in Styria are equipped with the same medical system within the ambulance. The medical devices include products from the firm *corpuls*, *FRED* and *ZOLL*.

The wireless communication standard Bluetooth includes a Health Device Profile (HDP) for medical devices [47]. However, only the communication channel between medical devices is provided by this profile and no specifications for the content of the data transmission or the data format is given. In order to establish a standardized communication between medical devices the Continua Alliance has developed a framework for the medical data transmission based on the IEEE 11073 standard. In addition, “the Bluetooth SIG mandates that the IEEE 11073-20601 Personal Health Device Communication Application Profile is the only allowed protocol for data exchange between HDP devices and is part of the IEEE 11073-104xx Device Specification. [47]”

The table 3.2 shows a comparison of the medical devices, defined within the equipment list of ambulances from the Austrian Red Cross, state association Styria, regarding the data communication technologies. Although several possible communication types exist no standardized data formats, but proprietary ones, are used for the transfer of medical data. Thus, the processing of medical data differs from one medical device producer to another, which makes the connection to medical devices very extensive and complex. To solve the data format problem the IEEE 11073 standard has been extended to personal health device communication standards for several medical device types. However, these device types do neither include defibrillators nor patient monitors.

Several medical device producer cannot agree upon a data format for the medical data exchange [21]. However, the lack of well defined standards for the medical data exchange aggravates an agreement on this topic. The HL7 standard, for example, gives an ample scope about the definition of data formats for the medical data exchange, so that medical device producers are forced to create their own proprietary extensions. In order to test the compatibility of HL7 standardized medical products the International Health Enterprise (IHE) provides automatic tests with all registered HL7 products [21].

	corpuls^3	**FRED semi-automatic**
Producer	Stemple	Schiller
Defibrillator	✓	✓
Monitoring	✓	-
Patientbox	✓	-
WLAN	in progress	-
RS-232	-	✓
Communication method		null modem
USB	in progress	-
GSM	✓	✓
Transfer data type	12 channel ECG	12 channel ECG
Communication Service	GPRS	unknown
Protocol	TCP/IP, UDP/IP	unknown
Data format	proprietary	proprietary
Bluetooth	✓	-
Transfer data type	12 channel ECG	
Protocol	Serial-Port-Profile (SPP)	
Data format	proprietary	
Communication Standard	-	-
Encryption	✓	unknown

Table 3.2: Medical devices comparison [21]

Currently, the medical device data is stored on a memory card and transfered to a PC and in further consequence stored in a central database. However, in the near future data communication technologies such as bluetooth, WLAN or GSM could be used for the medical data transfer. Figure 3.2 illustrates the communication workflow of the corpuls.web product. Although this product is currently not used within the ambulance, this well shown possibility for a data communication could be used in the future. The patient data is securely send to the server, which either manually or automatically forwards the data sets to the destination, whereby not only standardized formats (PDF, SCP) but also proprietary ones (HL7 aECG and so on) are used.

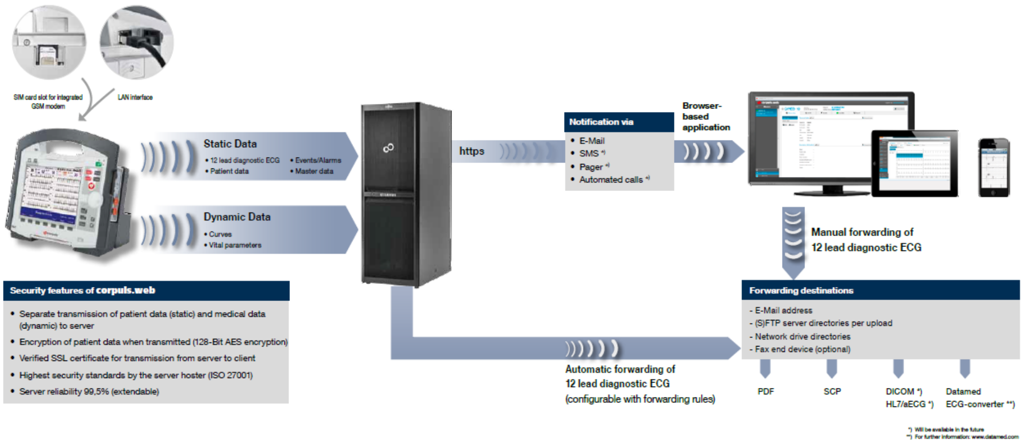


Figure 3.2: Workflow [10]

3.3 Database

The paramedics are legally bound to protocolling all actions taken during their ambulance services. Thus, the Styrian Red Cross provides a pre-defined mission protocol. This mission protocol basically consists of three different sections: *mission*, *mission accounting* and *medical data*. These three sections are filled in to the best of the recorder's belief and provide the basis for the settlement with the health insurance.

3.3.1 Requirements

There are several requirements regarding the storage of medical data. These requirements do not only provide information about how the data should be stored, but also how the stored datasets can be forwarded.

- All actions taken by the paramedics as well as mission and patient related data have to be stored. Moreover, the medical treatment information as well as the related mission must be directly linked to a patient.
- The medical injuries, that are graphically marked in the patient sketch, have not only to be stored as image but also as data sets.
- The mission protocol has to be signed by the paramedics. This information has to be stored as image.

- Due to the standardized provisions in the Austrian data protection legislation, the data must not be stored on the patient terminal. Thus, Services, that enable the transfer of data sets, must be provided.

3.3.2 Propositions

The *International Statistical Classification of Diseases and Related Health Problems* originally defined by the World Health Organization and revised by the Austrian Federal Ministry of Health provides a list of possible diagnoses and health issues [4],[61]. With this list a medical diagnostic database, which acts as a basis for the emergency diagnose free text field, could be created. In addition, symptoms and pains may be derived from the ICD-list. Moreover, a database, which contains all medicaments used within the ambulance car of the Red Cross, could be created and updated every time changes are needed. Currently, the patient's medical records are not provided on the field of emergency. In the future the medical records may be stored on NFC tags and read out by the mobile phones of the paramedics (see section 2.4.2).

3.4 Services

As the data cannot be stored on the patient terminal, but on a secure location within the network, services must be provided. These Services enable data requests and responses via the network. Thus, medical data sets would be available in the network.

The client sends a request via the network to a service and the service returns the result by the help of a protocol [52]. As the result is defined in a special data format, the client has to parse the result in a way that the contained data can be further processed. In contrast to a simple *Remote Procedure Call* (RPC), a service is self-contained, which means that the client calls up a service without the need to have special knowledge about the technical details. Thus, the service is sometimes referred to as black box. The service methods are often use-case oriented. This means, that the name of the service method is defined as an umbrella term. Internally, the service method will call up specialised methods that thereby hide further technical details from the client. Service methods, with such a behaviour are designated as *"service-facades"*. Instead of many small messages, a big message is sent, which results in a lower network load.

Similar to the RPC, the communication between the client and the service is performed via messages. Thus, routers can decide to which service the message should be forwarded.

There are several technologies, which can be used for the technical implementation of such services: *CORBA*, *Microsoft Message Queuing* and even Internet protocols such as *FTP* or *SMTP* [52]. CORBA uses distributed object systems that are based on binary protocols and *Microsoft Message Queuing* enables asynchronous requests via the network. In case of old systems that do not support those technologies, Internet protocols can be used. However, sometimes, even Internet protocols are not supported, so that a fall back to the communication via a data system would be necessary. However, in case of new systems (Web-)Services are the preferred technology. The basic reason for this is that these services are based on standards such as *SOAP*, *XML* or *HTTP*, that are in contrast to other transferred data human-readable.

The Windows Communication Foundation (WCF) supports several protocols and data formats. However, out of the box, SOAP- and REST-based services are integrated in the WCF [52]. As the prototype must be a Windows solution, REST and SOAP will be discussed and the best suitable solution presented.

3.4.1 SOAP

SOAP is a protocol-independent XML-based standard that enables the communication between systems via the exchange of messages or Remote Procedure Calls [52]. Additionally, it is mostly used in combination with HTTP(S), but can be used with any other protocol. Originally, the term SOAP is referred to as *Simple Object Access Protocol*. However, since the version 1.2 this description cannot be applied any more, as today SOAP is neither object oriented nor simple. The SOAP-messages can be either sent as *RPC* or as *Document*. In contrast to *RPC*, *Document* is more flexible and enables the exchange of all kinds of XML-messages. Apart from the message formats the coding standards *Encoded* and *Literal* can be used. These coding standards define the way the transferred data is illustrated. Encoded means that the data is represented as defined by the SOAP-specifications. In contrast to Encoded, Literal uses the rules of the XML schema. However, to due certain reasons, that will not be further discussed, both *RPC* and *Document* are nearly always used in combination with *Literal*.

In order to define web services the XML based language for the description of web services *WSDL* can be used. A WSDL-document defines the operations and the related messages for requests and results that are defined by the web service. Moreover, not only references to the used transport protocols and addresses of the services, but also the message format as well as the information about the coding standard are included.

WSDL-documents are used by Web Service Implementations to generate proxy classes for the web services that are consumed. With the help of a client proxy class, the web service method requests are directly sent to the desired service. Thus, no further information about the communication technique between the client and the server has to be known. In order to make the use of WSDL-documents more easily, Web Service Implementations support the generation of such documents from existing services.

Moreover, there are several additional standards for SOAP and WSDL. Moreover, in the list of standards several security aspects are included. Some of the security standards enable a secure communication with the services (*WS-Security*, *WS-Trust* and so on) and others ensure that the transferred messages will be received and processed in the right order (*WS-ReliableMessaging*).

3.4.2 REST

The *Representational State Transfer* (REST) is a lightweight alternative to SOAP-based Web Services. The exchange of messages is done via HTTP and the help of data resources. In addition, each resource has a URL, that references the corresponding Service. These resources can be defined in several formats, whereby most of the time *XML*, *JSON*, *ATOM* or *RSS* are used. Moreover, the HTTP-instructions *GET*, *POST*, *PUT* and *DELETE* are used for the work with these resources. In order to retrieve or send messages these instructions have to be used as a verb. The verb *GET* in combination with a URL and the used HTTP version data sets of a website can be retrieved. In addition, the result of such a REST-Service might be defined in a XML format. Moreover, resources can be created with the verb *POST* and the definition of a URL, the HTTP version, the host name, and the data sets [52].

If the provision of Services is done by the REST-technique and the data format is defined in XML the Service is also referred to as *Plain old XML-Services* or *POX-Services*. A example for this would be a Service, in which the URL */findHotels?datum=...* is sent and the results is retrieved in a XML format [52]. Moreover, this URL does not define a resource, but a method.

3.4.3 Comparison

The advantage of REST is the related simplicity. Nearly all programming platforms support HTTP-based requests. Moreover, the protocol overhead of the HTTP request and responses is low and not only XML, but also other coding standards such as JSON can be used. Thus, REST is used for the communication with mobile devices and even for modern web applications. Moreover, also interoperability problems are not as serious as with the use of SOAP. However, the drawback of REST is that currently no standards for the description of REST-Services exist. Thus, no basis for the proxy generation exists, so that they have to be defined manually. WSDL 2.0 should allow the automatic generation of proxies, but is only supported by few frameworks [52].

In order to protect the valuable medical data sets, the MAGDA-LENA guidelines, which have been discussed in section 2.6.4, state that the channel between the client and the server should be encrypted via SSL.

There are SOAP standards that enable a secure communication. Moreover, SOAP includes a additional protocol layer above HTTP(S). Thus, SOAP is much more complex and the protocol-overhead is much bigger than with REST-Services. Moreover, proxies can be automatically generated.

Tu sum up, REST combined with SSL, or SOAP with some security standards could be used to transfer the valuable medical data.

3.5 Mobile Application

The mobile application represents the digital mission protocols for the storage of treatment, mission and patient related data during ambulance operations. Usually, these data sets are filled in by the paramedics in the ambulance car. However, data may also be filled in outside the ambulance car. Moreover, several requirements have been defined in collaboration with the Styrian Red Cross. Due to the fact that the users are familiar with Windows solutions and the connection to systems of the Red Cross is much easier with these, one of these requirements states, that the application has to be a Windows solution.

In this section the requirements regarding the user interface of the mobile application will be discussed. Additionally, several guidelines for mobile applications will be presented. These guidelines include navigation concepts, the correct usage of colors, and the organization of elements on the the screen.

3.5.1 User Interface

A GUI-prototype for the documentation of medical data has to be implemented. This documentation does not only include treatment and patient related data, but also mission data. However, as the mission data will be provided by the operating mission system (see section 3.2), only few mission related fields have to be filled in by the paramedics.

Requirements

In order to design a mobile application for the filling in of medical data in moving ambulance cars, several aspects regarding the user interface have to be considered. These aspects are an extract of the requirements which have been defined in collaboration with the Styrian Red Cross.

- The user group, which will use the patient terminal, ranges form people with no experience with touch applications to people that are highly skilled with such applications. As a result, the mobile application must be easy to use and intuitive to operate.
- The filling in of the mission protocol is no sequential process. Thus, the user interface has to be designed in a way that the user can easily navigate to the correct form.
- The current status of the mission protocol should be illustrated. Moreover, the user should easily know, which "sections" are finished and in which sections data is missing.
- The mission protocol is filled in during the mission in the ambulance car. Therefore, the buttons and data fields have to be big enough to guarantee pleasant work with the application. Moreover, a pen input must be possible.

Additionally, in case of an emergency the time for the filling in of the mission protocol by the paramedics may be quite limited. Therefore, paramedics should not be forced to enter long phrases with the integrated keyboard, but should get several possibilities after the have entered a few letters. Especially free text fields including the *emergency diagnose*, the *symptoms/pain*, the *allergies*, the *medication*, the *patient history*, the *last meal* and the *incident* can be filled in with a pen very fast, but with the integrated keyboard the input will take some time. Thus, incremental search must be supported for as many fields as possible and databases must provide several choices of possibilities to enter. However, in case of free text fields corresponding databases, which cover a big amount of all possible entries, are neither easy to find on the web nor simple to create.

Guidelines

In order to provide a intuitive mobile application that can be used by paramedics of any age, several concepts have to be elaborated. These concepts include the navigation in the application, the correct usage of colors and the organization of elements on the screen.

Navigation: Navigation within an application must be well elaborated, so that users do not waste too much time to perform some operations [54, page 77]. In order to provide an easy interaction between the user and the application every tool should be within reach without navigating through dozens of pages or frames. Thus, signposts, which help users to orient themselves within an application, as well as well defined navigation models have to be considered.

As navigation techniques are tedious to realize for specific applications [50, page 57-58] have defined some guidelines for the navigation within applications. First of all users should not perform similar tasks in a completely different manner, but use *standardized task sequences*. Moreover, the titles and headings should be defined in such a way that users understand the context of use very easily. Pages or frames should be designed in such a manner that users are not irritated by their presented content, but exactly know which operations must be taken to perform some actions. *predictable pages*.

Organizing the display: The division of long multi column pages into several coherent pages should be made whenever possible [30]. Moreover, the placement of form elements as well as the right use of controls plays an important role for the look and feel of user interfaces. Labels should either be placed on the left or at the top of fields. However, there are several exceptions where labels should only be placed at the top of fields, including multi-column pages and labels with different lengths. Moreover, buttons should only be used to perform immediate actions, except in wizard navigations. Additional information such as a short text or an image within the button have to provide further information about the action, which can be taken.

Furthermore, not only the placement of form elements, but also the interaction with those elements has to be well defined. Touch keyboards are tailor-made for inputs, but might not always be rightly used.

The button placement of the OS standards have to be followed [35, page 64]. In addition [50, page 58-59] defines, that not only the *consistency of data display*, but also a *minimal memory load on the user* has to be provided.

Help patterns: Although the guidelines, which have been explained in the previous sections, state that the user interfaces must be consistent and the pages predictable, users may need some kind of help function [35, page 199]. There are three common approaches for providing help functions: How-To, Cheet Sheet and Tour. The How To pattern briefly and succinctly explains the main points of the application on one or more pages with screen shots and

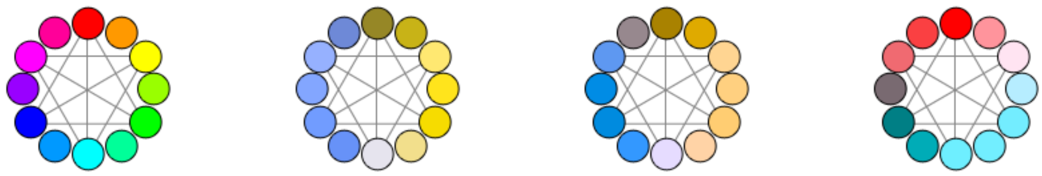


Figure 3.3: Color schemes [60, page 628-629])

text. In contrast to the How To pattern, the Cheat Sheet illustrates all elements within the application [35, page 200-207]. Probably the best way to illustrate a help function within an application is the Tour pattern, by which users are guided through the application by the help of several pages.

Getting the user's attention: The content within the user interfaces should draw attention to the user [50, page 60]. Therefore, several aspects as well as guidelines regarding the *intensity*, *size*, *color* and *choice of fonts* have to be examined regarding best user experience analysis. A high intensity pays attention to the user, but too much use of high intensities might lead to irritations and confuses the users. In general, high intensity should be rarely used and in total up to two levels of intensity are practicable. The text or graphics size plays an important role for the visual perception of users too. Larger sizes should be used to pay attention to the users and in total not more than four different sizes should be used. Another attention getter is the choice of fonts. It can be said that not more as three fonts should be used. The color giving within user interfaces is a topic for itself and will be explained in more detail in the following subsection.

Color: Not more than four different colors should be used [50, page 60]. On the other hand, three color hues are the limit for the usage within an interface, in which black and white do not count [54, page 503-505]. Moreover, from these up to three color hues a palette of colors by the usage of different brightness levels should be created.

The figures 3.3 show the different color hues that are seen by users with normal color vision, first picture on the left side, and people with color blindness, all the other pictures, whereby the color blindness can be distinguished into Protanopia (1% of male population), Deuteranopia (6% of male population) and Tritanopia (1% of male population).

Hue	Meaning	Use in Windows
blue/green	Windows brand	Background: Windows branding.
glass, black, gray, white	neutral	Background: standard window frames, Start menu, taskbar, Sidebar. Foreground: normal text.
blue	start, commit	Background: default command buttons, search, log on. Icons: information, Help. Foreground: main instructions, links.
red	error, stop, vulnerable, critical, immediate attention, restricted	Background: status, stopped progress (progress bars). Icons: error, stop, close window, delete, required input, missing, unavailable.
yellow	warning, caution, questionable	Background: status, paused progress (progress bars). Icons: warning
green	go, proceed, progress, safe	Background: status, normal progress (progress bars). Icons: go, done, refresh. Foreground: Paths and URLs (in search results).
purple	visited	Foreground: visited links (for links within Windows Internet Explorer® and documents).

Table 3.3: Color meanings in Windows [60, page 631-632]

3.5.2 Authentication

All information, which is needed for the authentication of users, is stored in a local database on the data terminal. This database contains the first name, the surname as well as the ID of each employee of the land headquarters of the Austrian Red Cross. However, as these data sets may be outdated regular updates have to be performed. Therefore, .sdf database files are generated by a database update generator application and stored in a file directory, located on the gateway server. In order to get the new data sets the new database files have to be manually copied through an FTP client. After the changes in the file directory have been made, an event is triggered and a maintenance process updates the model objects within the software of the data terminal. These manual changes will be replaced with an automatic daily synchronisation service for the new tablet generation, which will be presumably used in the near future.

The gateway server itself does only provide a copy of the employee database, but synchronises the data sets with those within the land headquarters of the Austrian Red Cross, so that all data sets are up to date.

Figure 3.4 shows the authentication mechanism in more detail. The authentication could either be performed through a login mask, where the personnel-ID and a password must be entered, or in a contactless way via the Near Field Communication technology. At the moment, the personnel cards of the employees within the headquarters of the Styrian Red Cross do not support the contactless authentication via RFID or NFC. In order to enable the contactless authentication, all employees could be equipped with MIFARE smartcards. This smartcard-system has been originally developed by the Austrian firm *Mikron* and belongs today to the product series of the firm *NFC semiconductors*. In comparison to RFID, where reader and transponder are are separated from each other, NFC integrates both the reader and the chipcard functionality. Thus, NFC devices can act as readers and as transponders. In order to enable the data transmission between NFC devices protocols are needed. There are several standards, which enable the data transmission between such devices. The ISO/IEC 14443 norm contains the protocols for the reader and the transponder and the protocol for the transmission between NFC devices is defined within the ISO/IEC 18092 respectively ECMA-340 [25, page 6-7].

Due to the high protection standards of medical data and the fact that the paramedics are personally liable for any mistakes regarding the treatment by signing the mission protocol, additional security mechanisms have to be implemented. Especially, in cases in which the paramedics loose the personnel card, the unauthorized usage of these cards has to be prevented. The cards could be used in combination with a password that is frequently changed. However, this is an extremely sensitive subject that may has to be embodied in the Austrian data protection law.

There are three products, which could be used for the contactless authentication: *MIFARE Classic*, *MIFARE Plus* and *MIFARE DESFire*. Besides the access control application MIFARE Classic can be used for ticketing applications such as public transport and for the electronic payment. However, since the introducing of MIFARE Classic, more than ten years ago, several weak points have been found and this product is outdated. Thus, the successor of this product, MIFARE Plus, should be used instead. In contrast to *MIFARE Classic*, the backwards compatible *MIFARE Plus* provides a AES encryption as well as a authentication. The high-end solution of the MIFARE product line is the MIFARE DESFire. There are several security and encryption mechanisms integrated into this product [25, page 75-76]. Moreover, not only one but up to 28 applications, each including 32 data files, can be stored on this smartcard [25, page 76]. To sum up, the MIFARE Plus product would be the best solution to provide contactless access control.

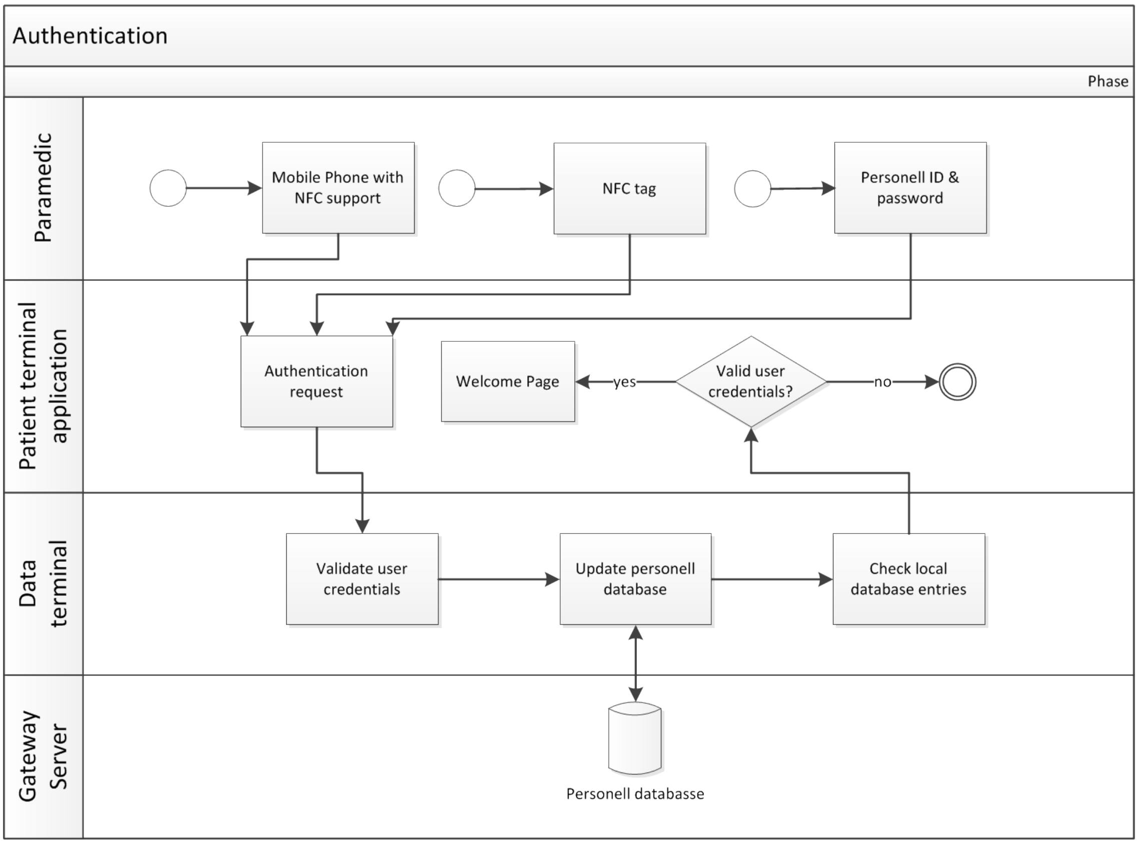


Figure 3.4: Authentication flow chart

3.5.3 Digital Signatures

Generally, the mission protocols are signed by the paramedics using a pen. In order to establish the signing process without a pen input, digital signatures could be used. To do so, the Austrian data protection law has to be considered. In Section 2.6.4 some guidelines for the compliance with legislation have been presented. Another solution would be the usage of both, digital signatures and signing mechanism using a pen. As digital signatures must provide a certain level of security, well-tested implementations have to be introduced, thus complicating a usage of digital signatures in connection with such a mobile application due to high expenditure.

3.6 Summary

In this chapter system comparisons have been made to identify the best suitable solution for the usage in the transport area of the ambulance car. As one of the requirements states, that a mobile Windows solution has to be found, Windows tablets have been taken as a basis for the selection. Due to the high temperature range in which the tablet can be used and the fact that *RFID*, *NFC*, *WLAN*, a *SIM slot* and several standards regarding the withstand of vibrations in the moving ambulance car and the water and dust protection are included the **Fieldbook B1** has been chosen as patient terminal. Moreover, the patient terminal will be connected to the data terminal via WLAN, whereby a client-server application will be implemented for the communication between these two terminals. Due to non-standardized data formats for the communication with medical devices, a connection to existing medical systems in the ambulance car cannot be performed very easily. Thus, the communication to medical devices will not be included in the prototype application. The application itself represents the digital mission protocol and can be filled in by the paramedics. In addition this application will be available on the Windows tablet. Furthermore, the medical data, which will be filled in by the paramedics has to be stored somewhere. Due to the high security standards for the processing of medical data, they cannot be stored on the tablet, but on a secure location in the network. Thus, the data will be forwarded to a gateway server. As the access to this gateway server is limited, Services have to be provided. Despite the high protocol-overhead of SOAP, the usage of SOAP-Services would be possible. However, the best solution for the mobile application would be the use of REST-Services in combination with SSL, which encrypts the data channel between the client and the Service. Then, some basic requirements regarding the user interface have been defined and basic guidelines for the implementation of mobile applications presented. Finally, some possible authentication methods on the patient terminal as well as the usage of digital signatures for signing the mission protocols have been discussed.

4 Implementation

This chapter deals with the implementation of the mobile application for the documentation of ambulance operations as well as the storage of the gathered medical data. First, the development tools will be presented in section 4.1. Then, the UI-masks of the mobile application will be illustrated and discussed in more detail in section 4.2. In addition, the general use of the mobile application as well as an important related pattern for the illustration of the user interface will be explained. Moreover, in section 4.3 a test system with medical data sets will be shown and the processing of these data explained. Then, the mechanism for the connection to the database will be clarified and the object relational model will be illustrated in section 4.4. Finally, the entity relationship diagram (ERM) of the database will be discussed in more detail. Basically, the ERM consists of three parts: the *mission*-, the *mission invoicing*-, as well as the *medical data*. Of these three parts, several entities will be picked out and presented.

4.1 Development Environment

In this section several development environments, which have been used for the implementation of the mobile application, will be presented. These environments include the *Visual Studio 2012*, the *Microsoft SQL Server*, *LINQ* and *WPF*. Basically, the application has been implemented in C# with the .NET 4.5 framework, in which for the user interface the Windows Presentation Foundation (WPF) has been used.

4.1.1 Visual Studio

Visual Studio is a platform for the development of desktop-, web-, devices- and cloud applications. This platform enables the use of .NET languages, C++ and HTML/JavaScript [33]. Moreover, Visual Studio includes a graphical toolkit for the designing of WPF applications. This does not only include a source but also a design view on the screen.

4.1.2 Microsoft SQL Server

The Microsoft SQL Server 2012 is a relational database management system. This product is used for the storage of the data. In order to manage the different database schemas the Microsoft SQL Server Management Studio has been used. There are several possiblities for the connection to such a database system. The mobile application uses a Object Relational Model (ORM) by the help of the integrated service *LINQ to SQL*. However, in section 4.4.1 the database connection will be presented in more detail.

4.1.3 LINQ

Microsoft provides a product of Object Relational Mapping, namely *LINQ to SQL*, which has been included in the .NET Framework since version 3.5. The great advantage of *LINQ to SQL* is the support of *stored procedures*, *views* and *user-defined functions*. Thus, stored procedures that are defined within the database, can be directly called up with the database context object within the application. This product is used for the connection with the Microsoft SQL Server 2012.

4.1.4 Windows Presentation Foundation (WPF)

The Windows Presentation Foundation is not only a graphical framework for the development of Windows desktop applications, but also a subset of the .NET Framework. The big advantage of WPF is the strict separation of the graphical view shown on the screen and the business logic of the application. The graphical view is implemented by the help of the Extensible Application Markup Language (XAML) and the code-behind can be implemented with certain programming languages [29]. For the implementation of the mobile application the version 4.5 of the WPF is used.

4.2 GUI-Prototype

In this section the graphical user interface prototype will be presented as well as the basic functionality of the prototype will be elucidated. On the whole, the prototype consists of several forms that joined together results in a digital version of the mission protocol. This digital mission protocol includes the following forms: *mission*, *patient*, *breathing*, *heart rate and skin*, *symptoms*, *Glasgow Coma Scale*, *medical aid*, *injuries* as well as the *completion* form. The concept as well as the design and the basic ideas behind these forms will be discussed further on in more detail. The prototype itself consists of several parts: *a global navigation bar*, *the mission list*, *the mission protocol* and the part for the *medical devices*.

As the filling in of the mission protocol does not take place in a sequential manner, each part of the mission protocol is assigned to a button with a corresponding icon. Moreover, the color of a button defines, whether all necessary data is filled in (green), or some parts are missing (red). This can be done by the definition of mandatory fields within the mission protocol. All mandatory fields could be defined within an XML-file so that such fields can be added and deleted more easily. This navigation concept should advance the creation process of the mission protocol.

Moreover, the state of progress of each mission protocol is illustrated in the mission list. Therefore, users can easily tell at a glance whether the protocol is finished or some data is missing. However, at first, the point at which the mission protocol is completed has to be defined. There are several possibilities that come to one's mind. The user could click a button to notify the application that the protocol is finished or the protocol is finished if all mandatory fields are filled out. Due to the fact that paramedics are legally responsible for any mistakes they have made during the documentation, the mission protocol is completed if the user signs the protocol. After the user has signed the protocol all changes within the protocol are logged with the corresponding time span and the information about the editor.

There are three different mission protocol states: *completed*, *incompleted* and *finished*. Additionally, each state corresponds to a sign. The green thumb marks that the protocol is finished. The yellow lock states that the protocol is incomplete and the red thumb refers to the completed state. Furthermore, completed implies that all necessary data is filled out, but the protocol has not been signed yet. Incomplete means that some data is mission, and finished states that the protocol has been signed and all necessary data have been filled in.

4.2.1 Mission

All missions that have to be performed during a working day by the ambulance crew are displayed (see figure 4.1 on the left side). Initially, for all assigned missions a corresponding mission protocol including the mission as well as patient data from the data terminal will be created. In order to show the mission protocol data of a certain mission, a mission has to be selected from the mission list. Figure 4.1 shows a snapshot of a mission form with sample mission data sets. Generally, the *mission number*, the *dispatch time* as well as the *site of operation* are always known at the beginning and all further data will be sent during the operation.

As illustrated in figure 4.1 the mission number as well as the name and the birthday of the patient is shown in the mission protocol navigation tool bar. This information states which mission protocol is selected and helps the user to distinguish between each mission so that the correct information is entered in the right mission protocol.

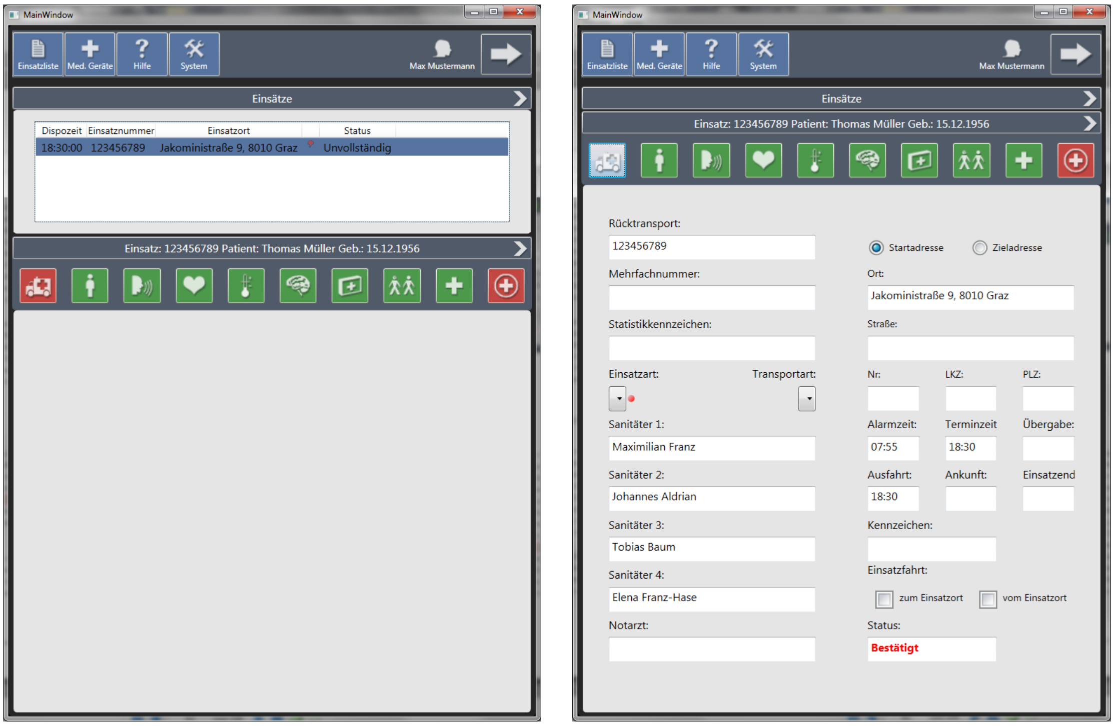


Figure 4.1: Mission

4.2.2 Patient

The patient data can be usually gained by the data stored on the e-card. On the e-card the patient name, the birthday and the social security number as well as the insurance company can be found (for more details see section 2.4.1). According to a member of the Styrian Red Cross the address of a patient can be found out at the time when the patient is delivered at the hospital. With an e-card system that includes the GIN-adapter, the patient master data can be read including the address of the patient (see figure 2.5 in section 2.4.1). On grounds of the mission invoicing, additionally, the payment value, the payment type as well as the payer has to be specified. Moreover, additional information about the person whose insurance covers the patient's treatment may have to be entered. In figure 4.2 not only the patient form, but also graphical marks of invalid fields are illustrated. The surname as well as the first name of the person whose insurance covers the patient are defined as mandatory fields and each time the input within those fields is invalid a red dot is shown. Furthermore, additional validation information will be displayed if the user moves over the input field.

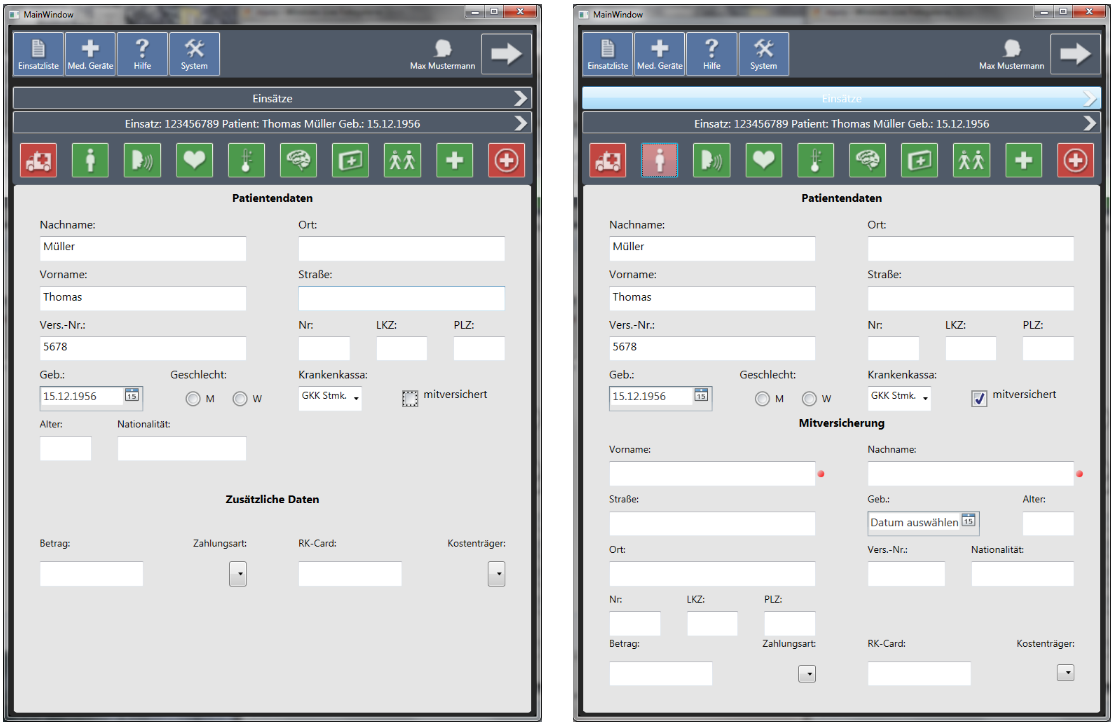


Figure 4.2: Patient

4.2.3 Injury

Figure 4.3 shows the injury form of the digital mission protocol. Within this form the three different types of injuries of a patient can be graphically selected on a patient sketch. These injury types are *paralysis*, *wound* and *injury*, distinguishable through three different colors. Moreover, further injury types can be selected from a different injury type list. This additional injury type list includes *burn*, *scald*, *chemical burn*, *frostbite* and *inhalation injury*. Moreover, the field with the name KOF defines the percentage to which the body surface is injured. As a result, the KOF of a burn injury would state how much of the whole body surface is burned. According to [16] the M, D and S refer to the DMS-test (perfusion-mobility-sensors). More precisely, with this test the mobility of a hand or a leg, the perfusion of extremities such as fingers as well as their sensitivity are checked. In case of a bone fracture this test might be of great importance. Other injuries such as nerve injuries may be detected at an early stage, so that the mission may be classified as time-critical. In further consequence patients may not be treated at the scene anymore, but transported to the hospital as fast as possible.

The default patient sketch in figure 4.3 is white and with a click into the sketch the corresponding part will be filled.

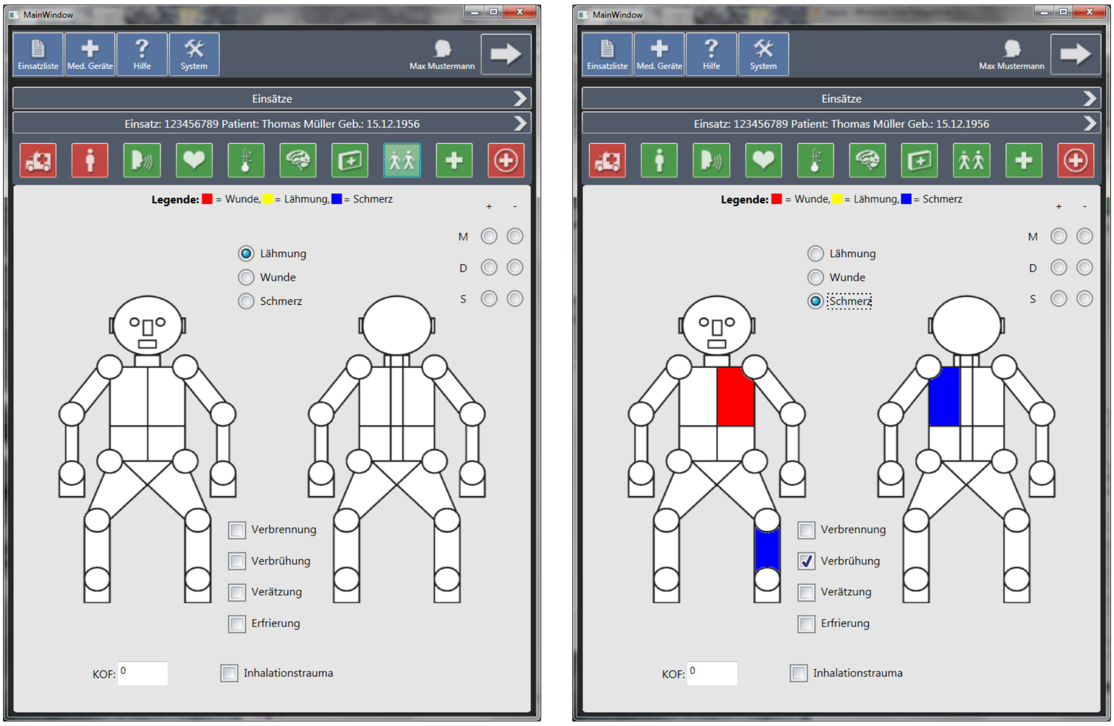


Figure 4.3: Injury

4.2.4 Glasgow Coma Scale (GCS)

The Glasgow Coma Scale is a score to identify the responsiveness of a patient. This score is calculated with the help of three different categories of behaviour to which points are assigned for each behaviour. The user selects one behaviour for each category and the sum of the selected behaviours results in a certain level of the GCS. As illustrated in figure 4.4 two different Glasgow Coma Scales will be calculated during the mission. The first scale calculates the GCS at the time the patient is taking care of at the scene and the second one is calculated to identify the responsiveness of a patient at the end of the mission. According to [43] *best response* is given at a total score of 15, a score of 8 or less is defined as *"comatose client"* and a score of 3 means *"totally unresponsive"* (see table 4.1 in section 4.6.3).

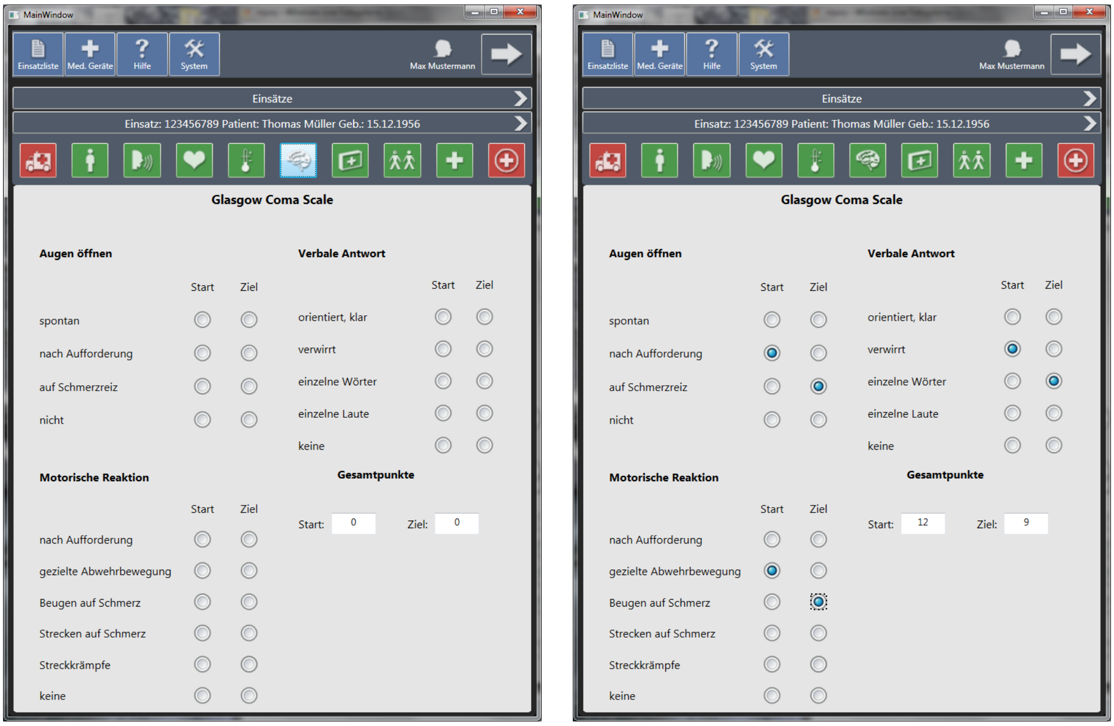


Figure 4.4: Glasgow Coma Scale

4.2.5 Medical Devices

The medical-devices-mask shows sample data of the medical devices that could be connected to the patient terminal: the *defibrillator* and the *EKG-Monitor*. In order to show realistic data sets, the operating instructions of the medical devices, shown in section 3.2.3, have been read. In case of the defibrillator sample data sets have been extracted.

Defibrillator

The defibrillator-mask does not only illustrate a list of events but also a graphical output. There are several events that can occur during the usage of the defibrillator. In figure 4.5 some possible events are shown. In order to resuscitate a patient, a electrical shock has to be performed. However, the defibrillator has to be charged first. Then, the EKG of the patient can be recorded by a click on the analysis-button and the output of the analysis will be shown on the screen. With the record-button, a graphical illustration will be shown on the screen, and with the delete-button a default page will be shown. The diagram for the illustration has been extracted by the help of some medical experiments, which have been published on the Internet [44].

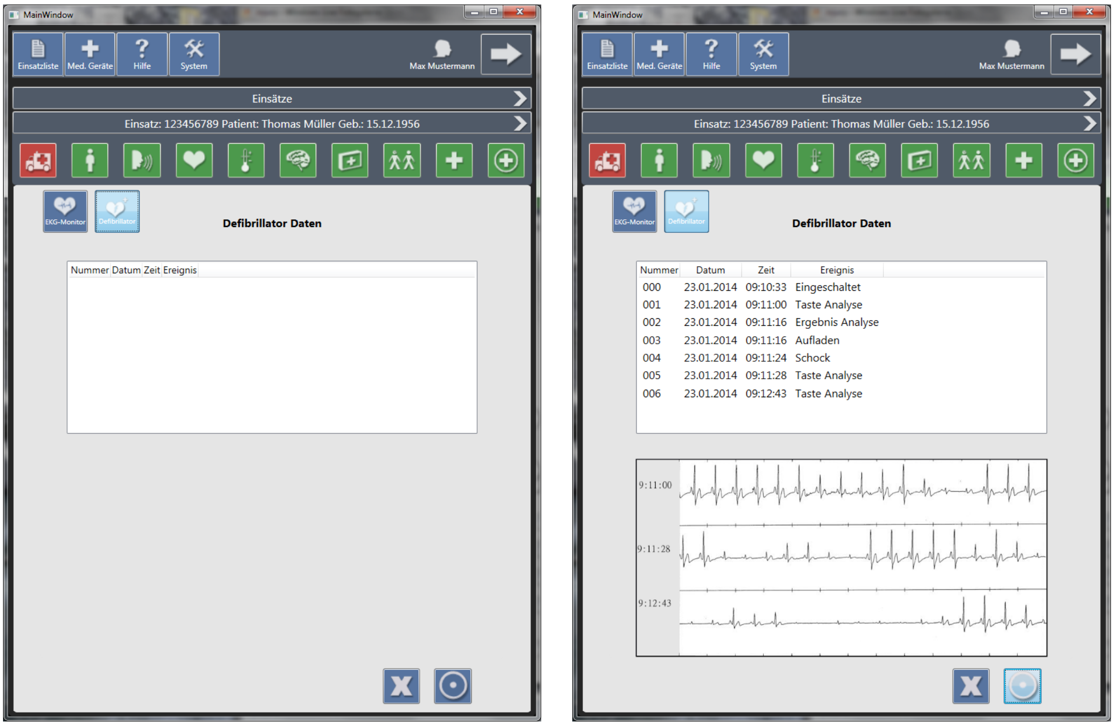


Figure 4.5: Defibrillator

EKG-Monitor

This mask illustrates a sample diagram of a 12-channel-EKG (see figure 4.6). This could be performed by the *corpuls*[3] monitoring device. Similar to the defibrillator-mask, with the record-button, a graphical illustration will be shown on the screen, and with the delete-button a default page will be shown. The EKG-diagram shown in figure 4.6 has been extracted from a EKG-software [51].

Figure 4.6: EKG-12-channel

4.2.6 Completion

The "completion"-form includes an emergency diagnosis field, a signature field as well as a confirm button. The signature field can be signed with a pen input and cleared with the button at the right upper corner of the field. The emergency diagnosis can be entered with the integrated keyboard on the Microsoft tablet and with the confirm button all entered data are stored into the database. Due to legal purposes the local storage of medical data on the tablet cannot be performed. Therefore, the data have to be transferred to a secure private network with limited access. If the data are transferred via a public network to the secure private network, the medical data must be encrypted, otherwise the encryption is not necessary on legal grounds [37]. Due to the fact that the tablet might not always have an available network connectivity, the data are not transferred each time a change has been made, but only with a click on the confirm button. Additionally, the data could be transferred every few minutes to ensure the actuality of the data stored within the database.

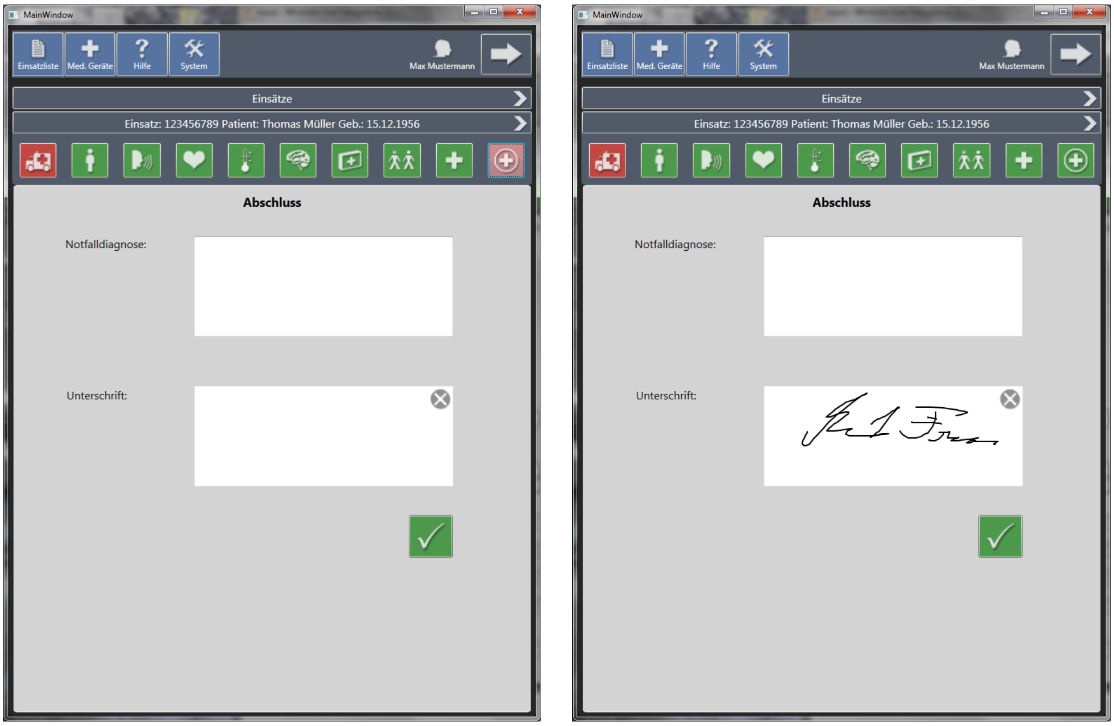


Figure 4.7: Completion

4.2.7 MVVM Pattern

The implementation of the mobile application is based on the MVVM pattern. This pattern is especially suited for WPF applications. Therefore, the basic concept behind the MVVM pattern will be discussed in this section. Figure 4.8 illustrates the structure of the pattern. The view represents the user interface, the model view the code-behind the view and the model the business logic. These three parts of the MVVM-pattern will be presented in more detail.

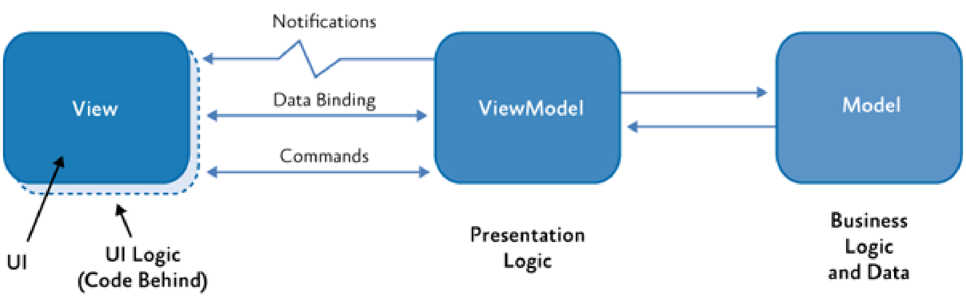


Figure 4.8: MVVM pattern illustration [28]

XAML

In WPF the user interfaces are structured with a specialised type of XML, namely XAML. With XAML not only the appearance on the screen but also component as well as window styles can be configured. Furthermore, data bindings as well as command call ups can be added to user interface components. In contrast to the non-XML-based graphical design, XAML-designs can be easily read, modified as well as created. Moreover, the graphical design can be strictly separated from the back-end logic. In addition, XAML supports animations, 2D and 3D graphics as well as a rich list of user interface components. Moreover, with XAML especially designed components to the application can be easily created through the definition of templates. In addition, the component behaviour and the appearance on the screen can be easily restyled with the included component-properties in the XAML-files. In Visual Studio, a graphical designer, which includes a toolbox of of UI-components, is available. The styles and templates can also be defined with the graphical design software *Microsoft Expression Blend* [34]

View

The view is responsible for the visual presentation of the user interface elements and their style on the screen. Usually, the code-behind the view calls up the initialization of all elements without any further code. However, in case of animations or direct manipulations of elements that are difficult to implement within the XAML, the view includes some additional code. In order to get a reference between the view and the view model, the data context property of the view is set to the view model. Due to this reference a data binding between the controls in the view and the properties as well as commands within the view model are established. Furthermore, the data binding can be customized by the view. This could be done by the help of value converters that change the displayed data format in the user interface or the introduction of input validation rules [28].

View Model

The view model includes properties and commands that reference to and interact with the elements in the view. However, most importantly, the view model does not have a direct access to the view. In order to notify the view of any changes that have been made by the user or by the application the *INotifyPropertyChanged* interface has to be implemented. The data can be modified or the data format can be changed so that the view can handle the data more easily. There are two models of data bindings: *one way* and *two way*. In contrast to the two way binding, the one way binding does not notify both parties of changes, but only one. A example of the one way binding would be the entering of data by the user without any validation or data modifications on the view model side. Moreover, the data can be validated by the view model. This can be done with the implementation of the *IDataErrorInfo* interface [28].

Model

In contrast to the view model the model object classes contain the application's data and are neither responsible for click events on the graphical user interface and the storage of data nor for the supplying as well as the retrieving of data sets [26]. Moreover, the model has no direct access to the view model and provides properties as well as validation rules. In addition, similarly to the view model both the *INotifyPropertyChanged* as well as the *IDataErrorInfo* interface are usually implemented. The model classes are used to combine the collected data within the application with the corresponding business logic [28].

4.3 Medical Test Data

The Styrian Red Cross has provided an infrastructure that is able to send test data to the patient terminal. In this section the test system structure as well as the messages that are processed by the mobile application will be presented and discussed in more detail.

4.3.1 Test System Structure

The laptop establishes a Virtual Private Network (VPN) connection to an operating mission test server. With the VPN-connection a graphical remote control of the test server is enabled and a new mission within the graphical mission management toolkit can be disposed. The Mdt-server forwards the mission telegram to the gateway server, which is directly connected to the Mdt-server via LAN. Furthermore, all connected data terminals are stored in a database on the Mdt-server. In addition, the gateway-server has a list of all connected data terminals including their IP-address as well as their hostname. On the basis of the unique MdtID of each data terminal, the Mdt-server forwards all related telegrams to the gateway-server. The gateway-server checks whether the data terminal can be found in the list of connected data terminals or not. If the data terminal is found, the message is passed to the corresponding IP-address. Otherwise, the message is buffered and sent to the corresponding IP-address the next time the data terminal connects to the gateway-server. Furthermore, the data terminal forwards all received telegrams to the patient terminal via WLAN. This is done by the help of a client-server TCP-communication. The patient terminal establishes a connection to the data terminal via the known IP-address and the port of the server socket. If the telegram message is received by the patient terminal the telegram is parsed and all parsed information is stored within a data structure.

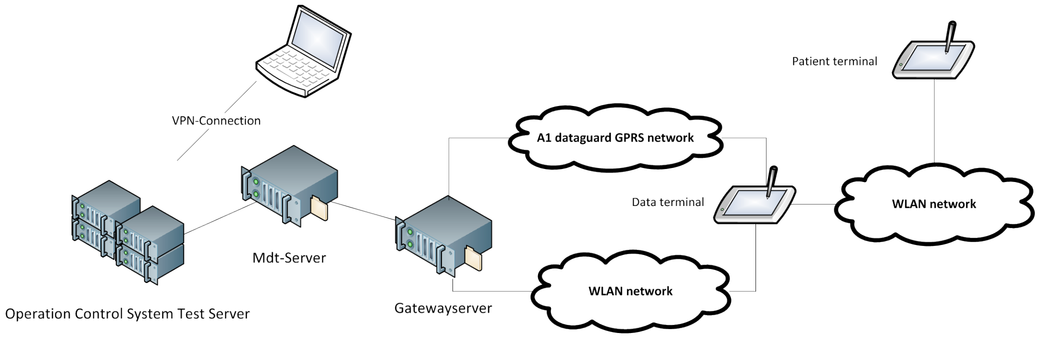


Figure 4.9: Test infrastructure

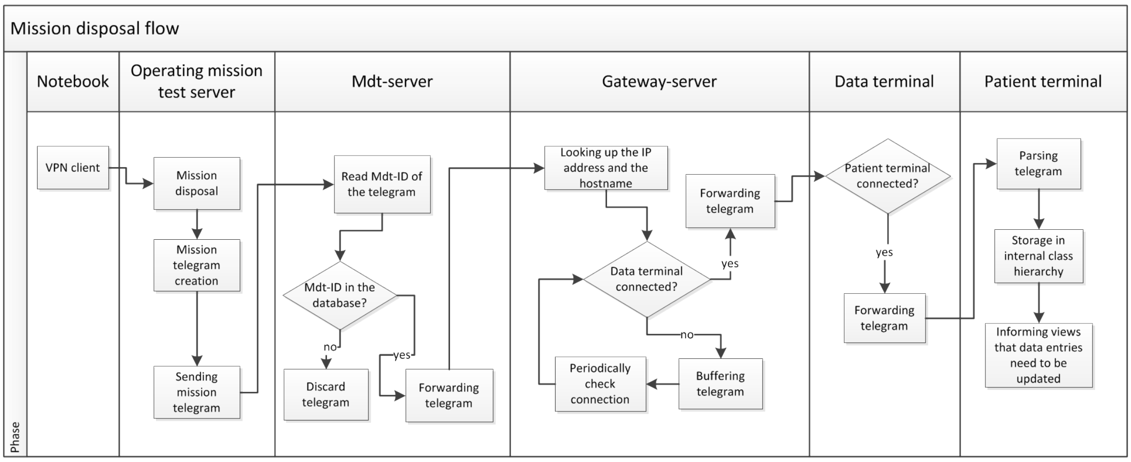


Figure 4.10: Message handling within the test infrastructure

However, the graphical mission management toolkit does not only support the disposition of missions, but also mission updates. These mission updates are performed through several telegrams. These telegrams will be discussed in the following sections.

In general, the mission information flow starts with the disposition of the mission by the mission management system located on the operating mission server and ends at the time the mission has been accomplished by the ambulance crew. During this time, general mission updates, mission status updates as well as related patient information are transferred. To be more precise, a message channel between the mission management system and the ambulance car is enabled. Missions are assigned to a ambulance car, equipped with a data terminal.

This data terminal receives all telegrams of the operating mission system and forwards them to the patient terminal. The paramedics inside the ambulance car are able to get general insurance information, stored on the patient's e-card, and send this information to both, the mission management system and the patient terminal. Moreover, the current mission status information is sent to the ambulance car each time the mission status is changed. In order to enable the message transfer between the data terminal and the patient terminal a simple server-client communication is established. Thus, all telegrams that have been received by the data terminal can be forwarded to the patient terminal. In further consequence, these telegrams can be processed and shown on the screen of the patient terminal.

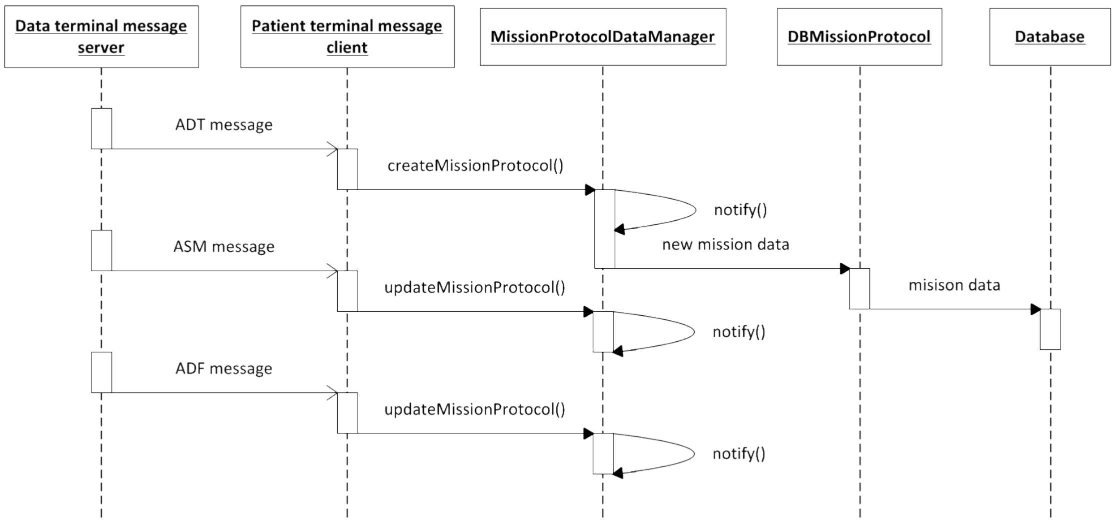


Figure 4.11: Message handling

Figure 4.11 shows an example of the communication flow between the data terminal and the patient terminal. The Adt-telegram, including general mission data, is forwarded to the patient terminal shortly after the patient terminal has received the telegram from the operating mission system. The information is sent to the *MissionProtocolDataManager*-object, which informs all GUI-masks that their data sets have to be updated. In further consequence, a new mission-protocol-entry is added to the *MissionProtocol*-table within the patient terminal database. Next, the mission status is updated and all related GUI-masks are notified. Due to the fact that most of the time, the insurance data of the patient is not known at the time the mission is assigned to the ambulance car, the ambulance crew has to determine this information. As all needed information is stored on the e-card, the patient's e-card is read by the e-card-reader, that is directly connected to the patient terminal. The data terminal forwards the insurance data to the patient terminal, which updates all related information sets. Due to connection problems that might occur in some areas, the information is not instantly stored within the database, but cached within the internal mission protocol data class structure (see section 4.5.3). At the time the user presses the OK-button on the finish-mask all data is forwarded to the database.

4.3.2 ADT Telegram (Mission Data)

The ADT telegram includes all general information about the mission, which has been assigned to an ambulance car. In addition, several different mission as well as patient data fields, some of which are defined as mandatory, are included within the ADT telegram. Those mandatory fields include the *telegram name*, the *type of telegram* as well as the *mission and transport number*. There are three different types of ADT-telegrams: *new mission*, *mission update* and *mission deletion*. The *new mission* and *mission update* telegrams additionally include the location and coordinates of the mission, the time of disposition as well as the mission priority. Usually, the patient data is not included in this kind of telegram. However, if the insurance data of the patient is known at the time the mission is disposed, the insurance data will be included. There are also other optional fields, which might be included: the *destination of transport*, the *coordinates of transport*, the *appointment-* and *pickup time* as well as *additional information about the mission.*

4.3.3 ASM Telegram (Mission Status)

The ASM telegram informs the data terminal in the ambulance car that the mission status has been changed. In order to know to which mission the mission status update belongs the mission number is included within this kind of telegram. There are several possible values for the mission status: *confirm*, *journey*, *at the scene*, *transport*, *at the location of transport*, *not used* and *disposed.*

4.3.4 ADF Telegram (Patient Data)

The ADF telegram includes the gathered insurance data of the patient's e-card, the mission number, a time-stamp as well as, optionally, the current position coordinates of the ambulance car. The insurance data consists of the *birthday*, the *social security number*, the *insurance company*, the *e-card-number*, the *expiry date of the e-card* as well as the *surname* and the *first name* of the patient. This kind of telegram is sent to both, the operating mission system and the patient terminal to update the insurance information of the patient.

4.3.5 FSA-DA Telegram (Crew Members)

The FSA-DA telegram serves as a notification message that informs the patient terminal about all crew members that are signed in on the data terminal. However, not only the crew members but also a time-stamp, the position coordinates, the ambulance car-ID, the password of the paramedic, who drives the ambulance car and the current mileage of the ambulance car are included. Of those fields the car-ID, the personnel number and password of the driver and the time-stamp are mandatory. Moreover, the data terminal supports the sign in of up to four crew members, whose identification credentials include the name as well as the personnel number. On the data terminal a list of all possible crew members one of which can be selected supports the sign in process.

4.3.6 ASA Telegram

The ASA telegram notifies the operating mission system that a mission status update has occurred. This kind of telegram may include the transport destination as well as the current position coordinates of the ambulance car. In contrast to all other telegrams, the ASA telegram is sent from the ambulance car to the operating mission system. Moreover, the operating mission system does not only process this kind of telegram, but also replies with an ASM telegram, that the current mission status has been updated.

4.4 Storage of Medical Data

The operating mission system does not provide a database for the storage of the medical records. Moreover, the MDT-protocol, which enables the data transfer to the central operating mission system does not include the functionality to forward medical data entries. Therefore, the data has to be stored somewhere else. Due to the high security standards the medical data has to be stored at a secure location. The best solution would be to store the medical data in a database on the gateway server. In addition, web services have to be provided to establish a secure connection between the gateway server and the patient terminal.

Due to the fact that no direct access to the gateway server was possible, the collected medical data is stored in a database on the patient terminal.

4.4.1 Database Connection

In figure 4.12 three possibilities to get a connection to a database are shown. The Open Database Connectivity (ODBC) is not only program language independent, but also independent of the operating system as well as the database system. Thus, in order to communicate with several different database systems within an application the same code, but distinctive ODBC drivers have to be used. Moreover, native database APIs might be used to establish a connection between an application and a database.

In case of the database system ORACLE, *Pro*C*, especially designed for *C* applications, would be an example of such a native API. There are also other possibilities to connect to a database, such as the use of *JDBC* and *ADO.NET*. However, regardless of the connection mechanism to a database system, the queried data from a database has to be stored in any kind of format within an application. The returned database records may be stored in variables, or within a class hierarchy.

In case of a product order database scheme, each product could be stored in a product-object and each product order in a product-order-object. Thus, for each database scheme the class hierarchy as well as the relations between these classes has to be created manually. To counteract the manual creation of classes for different returned database records as well as the relation between these classes, Object Relational Mapping (ORM) has been introduced. With ORM database entities are automatically mapped to objects by a set of classes. "Each database is represented by an ORM context object in the specific programming language, and database entities such as tables are represented by classes, with relationships between these classes. [31]" Thus, the application only has to work with the provided classes to interact with the database. Moreover, the connection to the database as well as the accomplishment of concurrent database queries is automatically established by the ORM. Summing up, the whole interaction with the database is processed by the ORM.

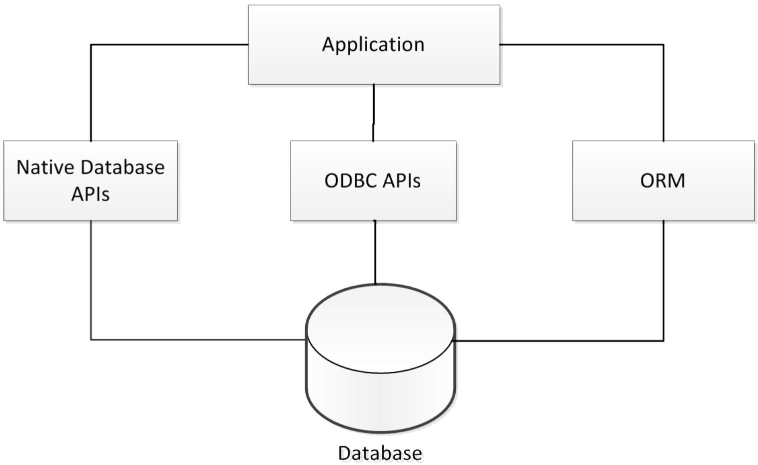


Figure 4.12: Database connection APIs [31]

In figure 4.13 the database connection process for .NET applications that uses the Object Relational Mapping product *LINQ to SQL* of Microsoft is illustrated. *LINQ to SQL* translates the queries within the object model to SQL and in further consequence a communication to the SQL Server is established by ADO.NET SQLClient adapters to sent the data to the SQL Server Database.

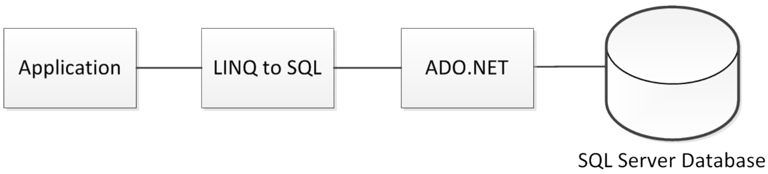


Figure 4.13: LINQ to SQL in .NET applications [31]

4.4.2 LINQ to SQL

Figure 4.14 shows the database model, that enables a mapping between database tables and classes, called Object Relational Model (ORM). This model does not only map the classes with the related database tables but also the relations between them. Thus, no attention to relations between tables has to be paid any more. In order to insert, delete or modify data entries in the related database tables, objects of the related classes are used.

Similar to non-ORM applications, data sets can be retrieved by SQL statements. However, instead of the table and column names, the objects of the ORM are used to establish a direct communication with the database.

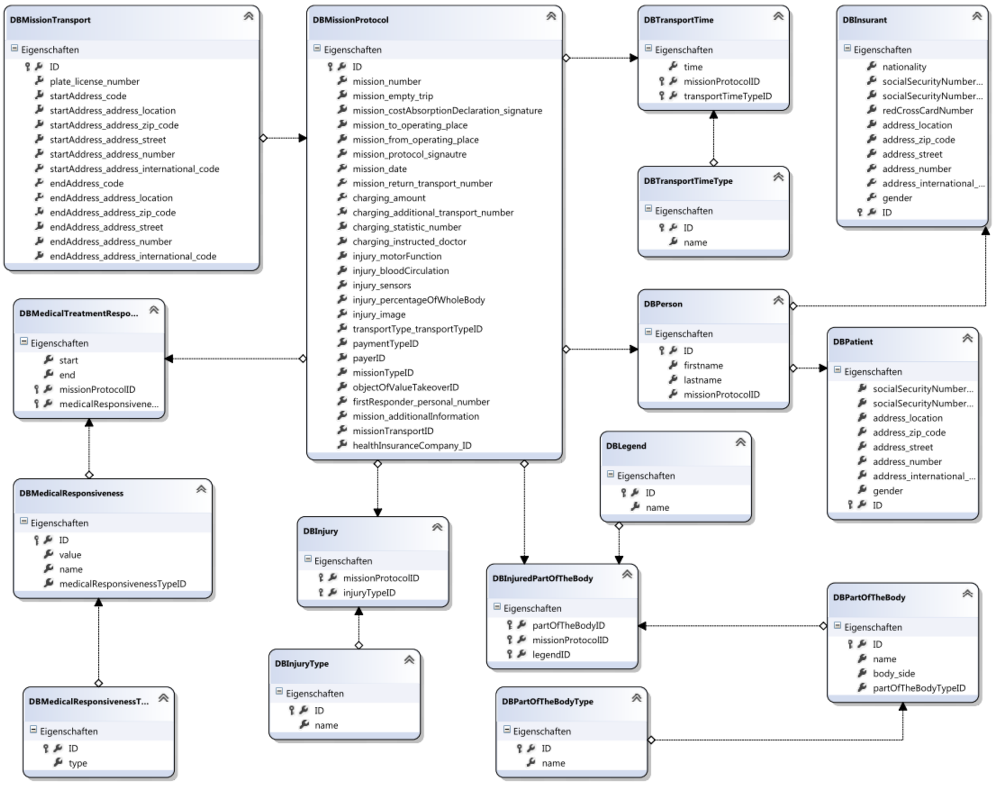


Figure 4.14: Database model

4.5 Patient Terminal

Section 4.5.1 will deal with the most important components of the implementation. Furthermore, the process from the generation of the mission protocol to the parsing of the data and the forwarding of the data to the GUI will be presented in section 4.5.2. In addition the structure behind the storage of the gathered data will be shown in more detail in section 4.5.3.

4.5.1 Structure

The MVVM pattern, which has been discussed in section 4.2.7, is applied to the patient terminal application. The Views include the graphical design, defined in XAML. In addition, their data context is set to the corresponding ViewModel. Thus, a binding between the View and the ViewModel is established. The ViewModel contains the presentation logic of the application, handles commands that are triggered by the user during the interaction with the View and notifies the View of any changes that have been made. The Model stores the gathered data and provides properties as well as validation rules.

In section 4.2 the GUI-prototype has been illustrated and the basic concept as well as ideas behind the design have been discussed. The graphical masks within this section represent the Views of the application. Basically, the application distinguishes between the following views: the *mission list view*, the *mission view*, the *patient view*, the *breathing view*, the *heart view*, the *symptoms view*, the *Glasgow Coma Scale view*, the *medical aid view*, the *injury view*, the *medical device view* and the *finish view*. Of those views the breathing-, heart-, symptoms- and medical-aid-view are not part of the GUI-prototype. Thus, these views have not been implemented. Moreover, each View has a corresponding *ModelView* to which the data context is bound. In contrast to all other views, the patient-, the mission- as well as the medical-device-view include two additional sub-views.

Figure 4.15 shows the most important view models that are used within the application. Subsequently, three of those view models will be discussed in more detail.

MainViewModel

The *MainViewModel* manages all view models and decides which view will be shown on the screen. Moreover, an instance of the *MissionProtocolDataManager* is created and passed, by reference, to the view models. As the data context of the base window is set to the *MainViewModel*, the interaction between the user and the *MainWindow* is handled by the *MainViewModel*. There are two different bars, which can be selected by the user (see section 4.2): the *mission-list-bar* and the *mission-protocol-bar*. As the position of the views depends on the bar which is currently active, the *MainViewModel* updates the positions of the views, that are shown on the screen. This is done by the help of the class *PositionModel*. The row-, column, rowspan- and columnspan- properties of the views are bound to the corresponding position model.

MissionListViewModel

The *MissionListView* shows a list of missions that are assigned to the ambulance crew. The *ModelView* provides properties that establish a data binding and the class *MissionListItem* represents the corresponding model. In addition, the *MisisonListViewModel* manages all assigned missions and provides additional properties for the mission-protocol-navigation-bar. With these additional properties the mission number, the name as well as the birthday, that are shown within the mission-protocol-navigation-bar, will be automatically updated as soon as the user selects one of the possible missions.

InjuryPageViewModel

The *InjuryPageView* includes a patient sketch for the graphical marking of injured body parts. Moreover, several basic injury types as well as additional injury types can be selected. In addition the percentage of the injured body surface area can be defined. The *InjuryPageView-Model* handles the interaction between the View and the user. A color map containing the color as key and the related body part as value, is provided as an addition. With this map, the body part related to the current position in the patient sketch, triggered by a mouse-click of the user, can be determined.

The default patient sketch is white and with a click into the sketch the corresponding part will be filled. This is done by the help of the flood fill algorithm. If the pixel color of the clicked (x,y)-position is white, all white pixels around this position will be filled until the pixel color does not match the white color any longer. Due to the fact that all body parts are separated from each other by black pixels the fill-in can be easily performed. At the moment, a implementation without threshold is used as flood fill algorithm [46]. Thus only exact matches with the color white are filled with the corresponding color. To get a smooth transition between the color that will be filled and the black pixels a threshold could be added. Moreover, in the eye of the beholder, the use of a threshold might result in a non pixelated picture. In order to know which body part the user has selected, a color mask in combination with a map, that contains the name of the body part as a value and the corresponding color as a key, is used. The color mask is simply a picture in which all body parts are filled with different colors. In order to get the color information of each pixel the color mask is will be read as a Bitmap image within the application.

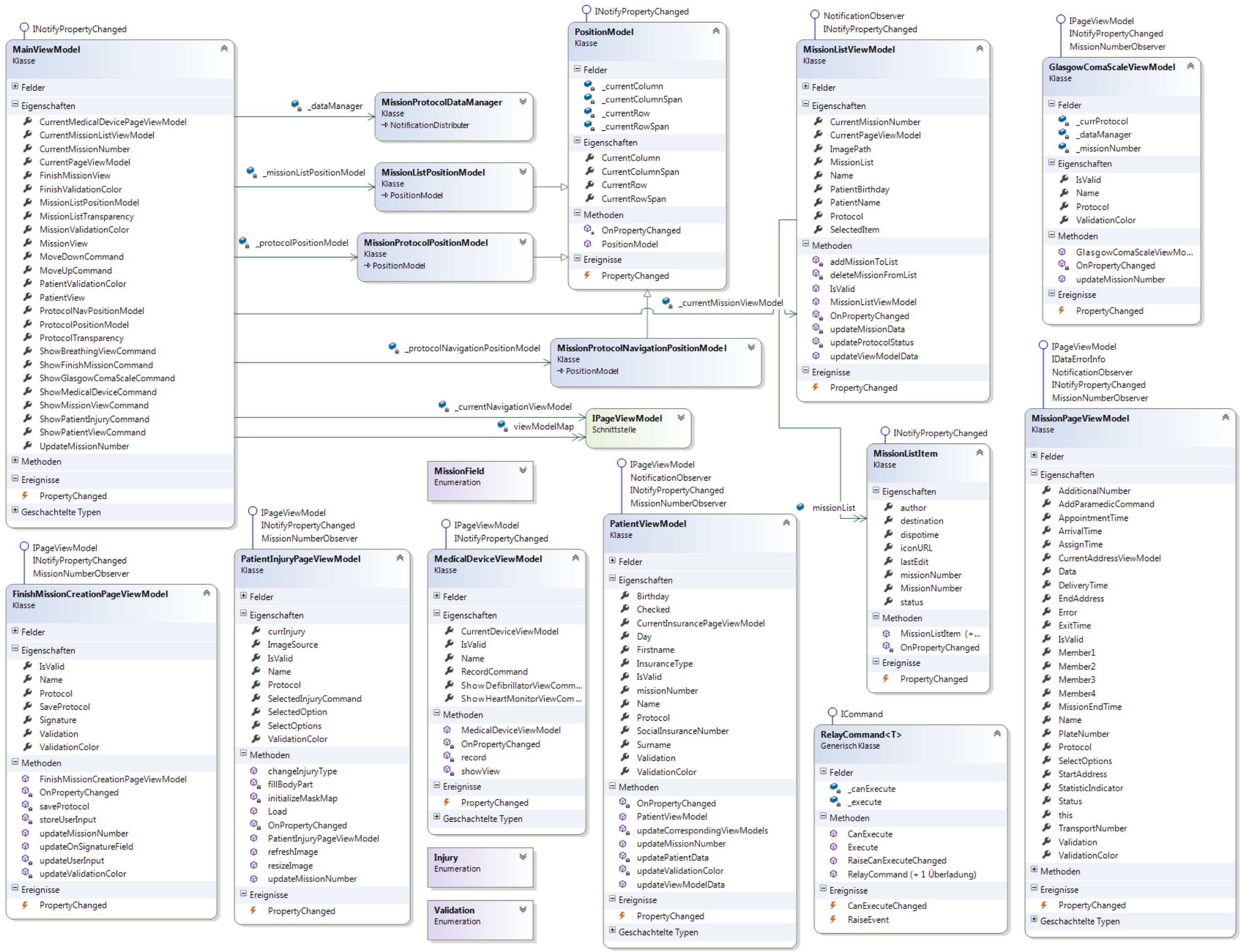


Figure 4.15: View Models

4.5.2 Mdt-Messages

As explained in section 4.3 telegrams are sent by the mission operating system over several sub-components to the data terminal, which forwards the data to the patient terminal. However, each time a telegram is sent the patient terminal has to be connected to the data terminal. In order to simulate the message sending process on the patient terminal without any connection to other devices message builders that recreate the Mdt-messages have to be provided. Figure 4.16 shows the class diagram for the creation of several Mdt-messages. The header includes a *Mdt-ID*, a *message-ID* as well as a *transport type*. With these information the messages can be easily identified and in further consequence processed by the patient terminal. Moreover, Mdt-messages include a checksum, which will be verified during the processing of the messages on the patient terminal.

In order to continuously send messages to the patient terminal several threads have been used. These threads consume messages from message buffers that contain messages of a certain type. Basically, each time a thread is awaken a message of the corresponding message buffer is processed and the thread is sent to sleep. However, as the threads cannot process messages at the same time, the threads have to be scheduled. This is done by a static scheduling assignment at the runtime.

Message processing

In order to illustrate the parsed information of the Mdt-messages on the screen the information has to be sent to the responsible classes. This is done by the help of a *Observer-pattern*. The *PatientViewModel*, *MissionListViewModel* as well as the *MissionPageViewModel* are notified each time a message has been processed. Thus, the data fields of the patient and mission section as well as entries of the mission list on the screen can be updated. Moreover, each notification has a corresponding notification type that uniquely identifies the action to be executed such as update, delete or insert. In addition, the *ViewModels* have a reference to the unique *MissionProtocolDataManager*, which stores all information about the mission protocol. Thus, the data, which has to be updated, deleted or inserted can be easily gained through this object (see figure 4.17).

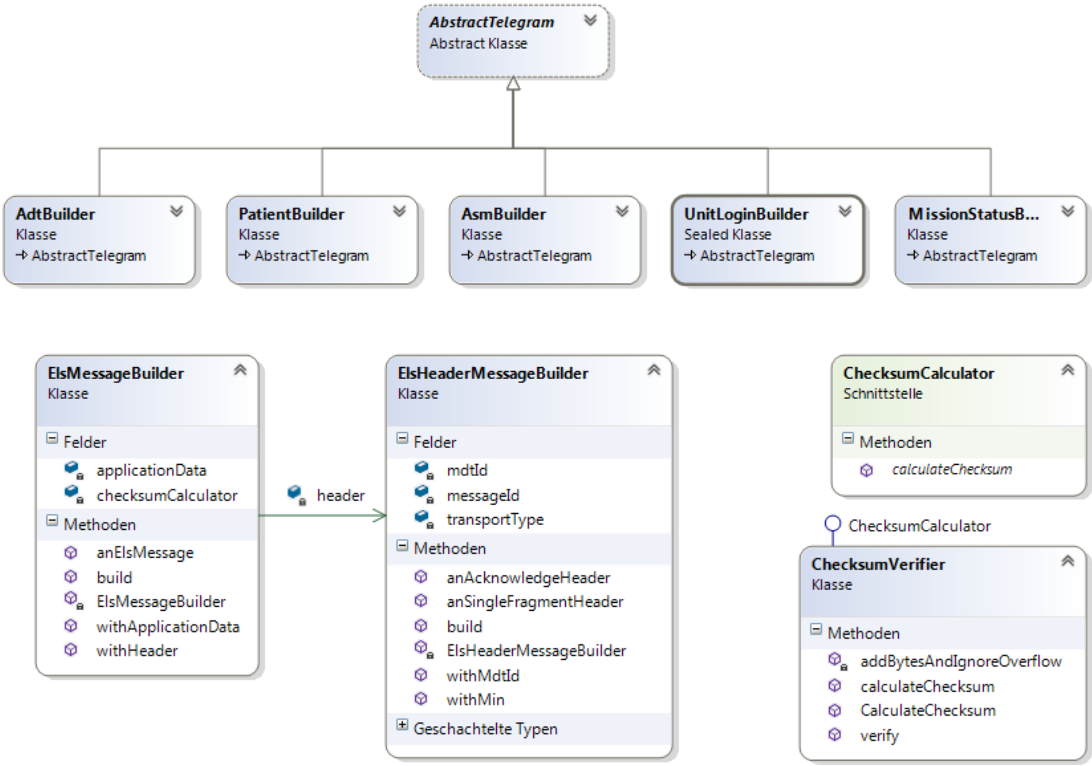


Figure 4.16: Message builder

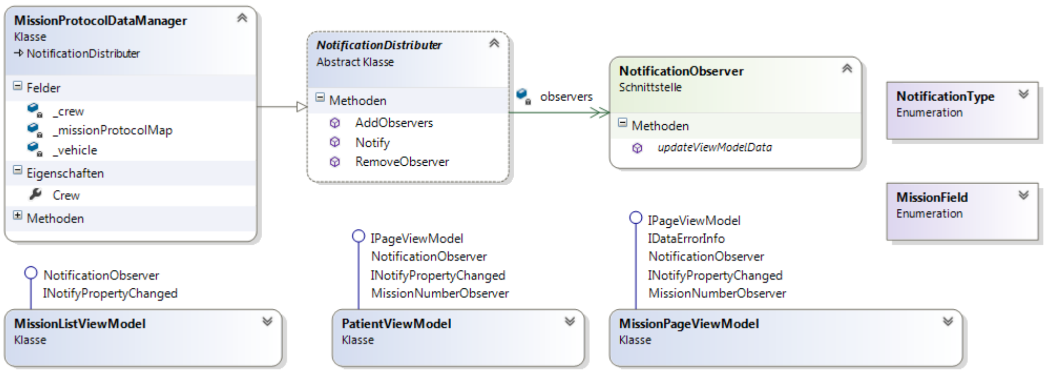


Figure 4.17: Message observer

The *PatientViewModel* and the *MissionPageViewModel* include additional sub-models that have to be notified about the action to be executed too. Thus, each sub-model implements the *Update-Notification*-interface with the corresponding update method. This method will be called up each time the view-models receive a notification message (see figure 4.18).

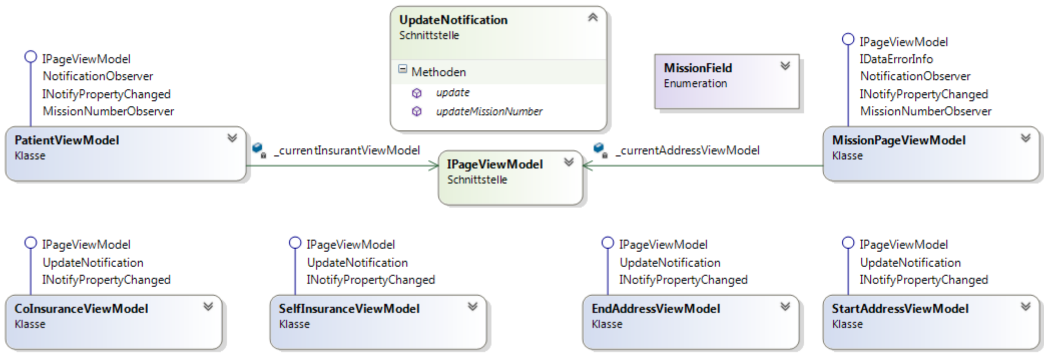


Figure 4.18: Submodel notification

However, the *View-Models* cannot update their data fields without knowing the currently selected mission number. Therefore, the mission number has to be updated each time the mission-selection in the mission-list that is shown on the screen is changed. This is achieved by the same principle as used by the notification messages, namely the *Observer-pattern*. Moreover, the *View-Model* include a reference to the currently selected *MissionProtocol* that stores all data related to the mission protocol (see figure 4.19).

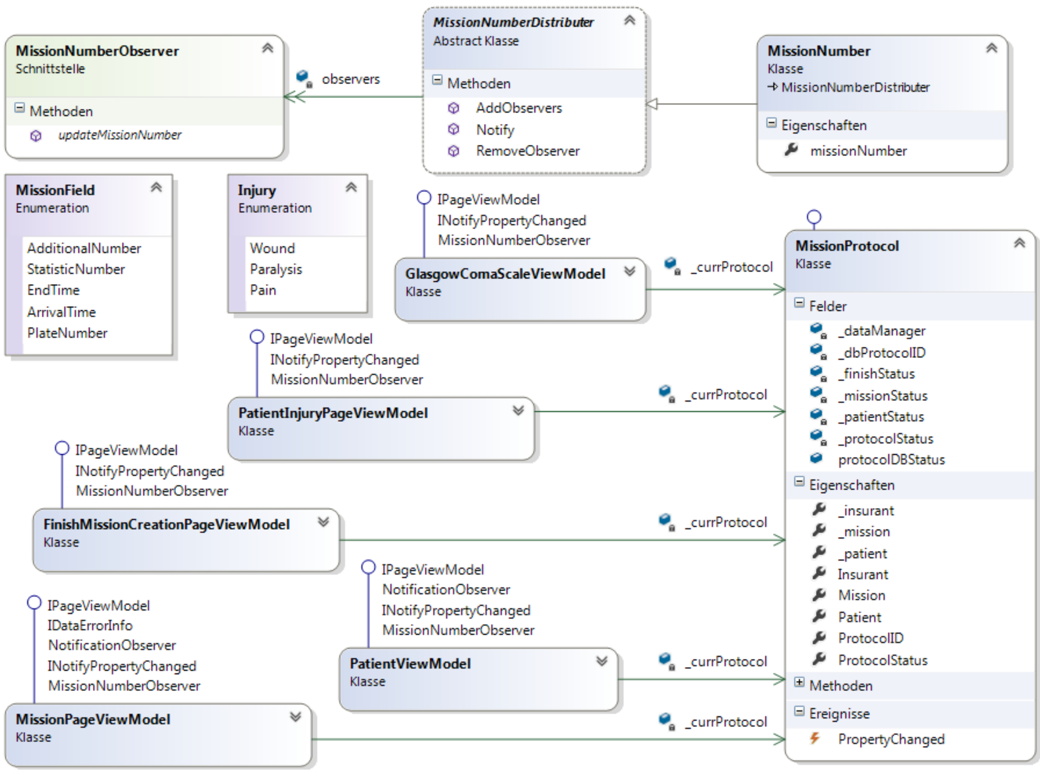


Figure 4.19: Mission number notification

Figure 4.20 illustrates a simple navigation process through a mission protocol. The *Main Window* shows two bars, the mission protocol bar and the missions bar, that can be selected. With a click on the missions bar, all missions assigned to the ambulance crew will be illustrated. Next, a mission is selected and the corresponding *Mission-View* (see figure 4.2.1) shown on the screen. At this time, the mission protocol bar, consisting of several mission protocol sections, can be be used to navigate through the selected mission protocol. With a click on the section *GCS*-button the Glasgow-Coma-Scale view is shown. Next, the injury-view will be rendered by a click on the *injury*-button and the last section of the mission protocol will be shown after a click on the button *"finish"*. At last, the *confirm-button* within the finish-mask is selected and the simple mission protocol navigation process is finished.

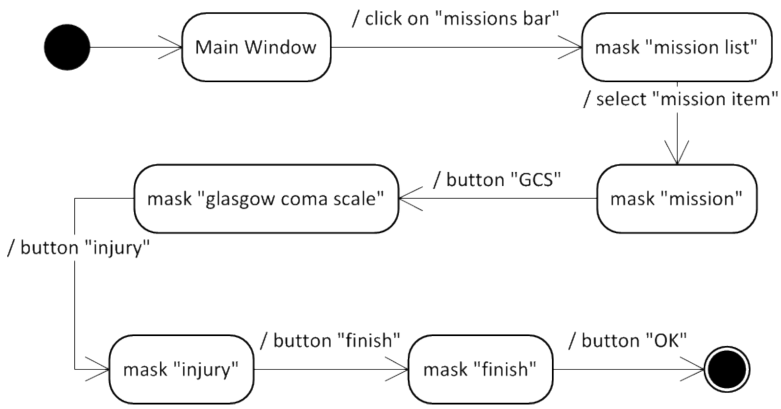


Figure 4.20: Simple mission protocol process

4.5.3 Mission Protocol Model

In the previous section the message handling without a connection to the data terminal and the mechanism that updates the information shown on the screen has been discussed. However, no attention has been paid to the storage of the mission protocol data. This section will discuss this aspect in more detail as well as illustrate the structure of the mission protocol data.

MissionProtocolDataManager

The heart of the mission protocol model, the *MissionProtocolDataManager*, manages all mission protocols, the crew as well as the vehicle object for the ambulance mission. The crew consists of up to four members and cannot only include paramedics, but also an attending medical doctor. In addition, each mission is assigned to a vehicle with a unique *ID*. Moreover, by the help of the current mileage the totally travelled kilometres for each mission can be easily calculated.

The *MissionProtocolDataManager* does not only include a list with all mission protocols, but also provides methods to update data sets of the corresponding mission protocols. Moreover, each time a Mdt-message is processed the *MissionProtocolDataManager* notifies the *PatientViewModel*, the *MissionListViewModel* as well as the *MissionPageViewModel* that some data sets have been changed.

MissionProtocol

The mission protocol includes all related data sets of the parsed messages as well as the user input. Thus, not only the information about the patient and the insurant, but also mission related data are included. Moreover, each mission protocol has a *Protocol-ID* (the mission number) that uniquely identifies the protocol.

In order to know, whether all mandatory data fields have been filled or some data still has to be defined, each mission protocol has a protocol status. The mission protocol distinguishes between the statuses *finished*, *unfinished* and *completed*. *Finished* refers to the fact that all mandatory fields have been filled in, but the protocol has not been signed yet. *Unfinished* means that some data is missing and *completed* states that all mandatory data fields have been filled and the protocol has been signed.

Moreover, not only the mission protocol status within the application, but also the database status has to be defined. Three different database states can be distinguished: *generated*, *unknown* and *stored*. *Unknown* means that currently the mission protocol is currently not stored within the database. *Generated* means that a new mission protocol has been created (new mission telegram, see section 4.3.2) and all included data sets have been forwarded to the database. Finally, *stored* refers to the fact that the confirm-button of the finish mission protocol page has been pressed and the medical treatment as well as the patient data has been stored into the database.

Mission

The mission provides general information about the transport, which has to be performed during the mission. This information includes the *transport type*, the *transport number* as well as the *additional transport number*. The transport number uniquely identifies the transport during the ambulance mission and the transport type states whether the patient has been transported by wheelchair, a stretcher, ambulating or by boarding wheelchair. Moreover, a additional patient, which has been picked up with the same ambulance vehicle, will be documented by the additional transport number. In addition, all blue light driving operations have to be documented. These blue light driving operations can be performed either to the field of operation or from the field of operation.

Furthermore, the mission includes a reference to the *DateTimeManager*, which handles all related mission times. There are several mission times, which can be distinguished: the *appointment time*, the *time of arrival*, the *pickup time*, the *delivery time*, as well as the *time when mission is finished*. As these properties are declared as *DateTimes* the input of the user cannot be directly validated, but with a temporary variable. If the value of the temporary variable meets several validation conditions the corresponding mission time will be set to this value. Otherwise, the input of the user would be deleted each time the user enters a invalid time. Due to the fact that the validation is triggered each time a letter is entered or changed this would cause a non-acceptable behaviour.

Patient

General information about the patient such as the address and the name are included within this class. In addition, references to the medical treatment information, including the Glasgow Coma Scale and the injured body parts as well as the injury type, are provided. Moreover, the patient's insurance information and results of the *perfusion-motor function-sensibility* (DMS)-check is stored within this class.

Insurant

The insurant class deals with the insurance information about the person whose insurance covers the patient's requirements. In addition, the payment information, including the payment type, the amount to be paid, and the payer, will be stored. In contrast to the patient information, the insurance information includes also the nationality of the insurant.

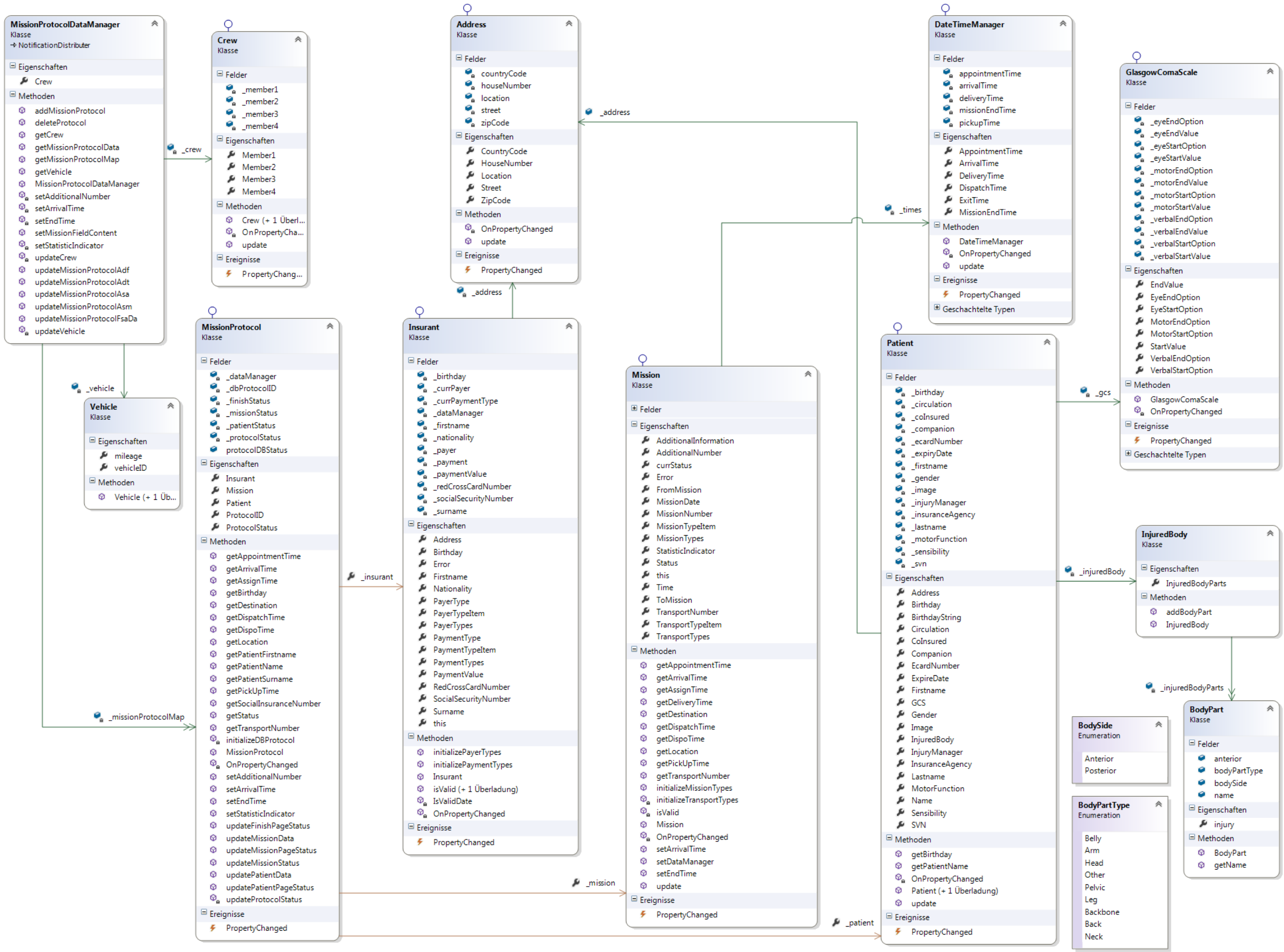


Figure 4.21: Mission protocol model

Figure 4.22 shows the interaction between the classes in case of a user input in the *Patient* page. The *MainView* refers to the default window at the start up of the application. At first, the user clicks on the mission bar and selects one from the list of possible missions that are assigned to the ambulance crew. This will trigger a mission number update. The view models will be notified that the mission number has been changed and will update them immediately. Next, the user clicks on the patient-button within the mission protocol navigation bar. (This button includes a command property, which is triggered at the time the button is pressed.) Simultaneously, a new command object is created and given back to the *MainViewModel*, the data context of the *MainView*. The command is executed and in further consequence the *PatientView* will be shown on the screen. Finally, the user types in a new address and the location will be updated. However, this update will not be directly performed, but through an update request that is forwarded over several stages starting at the *MissionProtocol* through to the *Patient* and the *Address*.

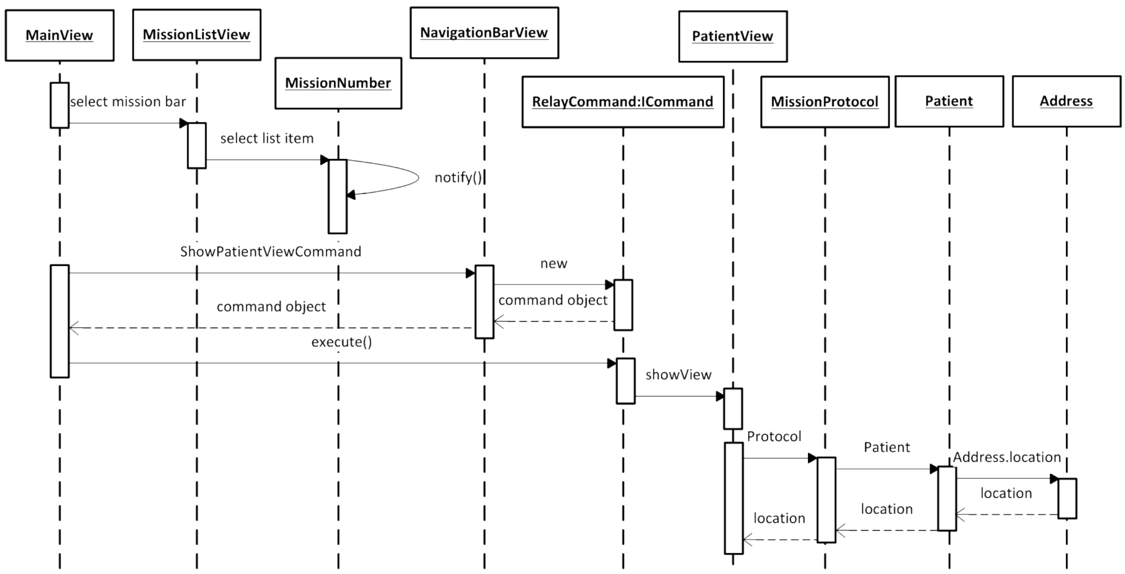


Figure 4.22: Mission protocol sequence

4.6 Database

In this section the database structure as well as the basic ideas behind the structure will be explained. In order to do so, some parts of the structure will be picked out and discussed in more detail. Additionally, tables with related table entries will be illustrated.

4.6.1 Mission Protocol Data

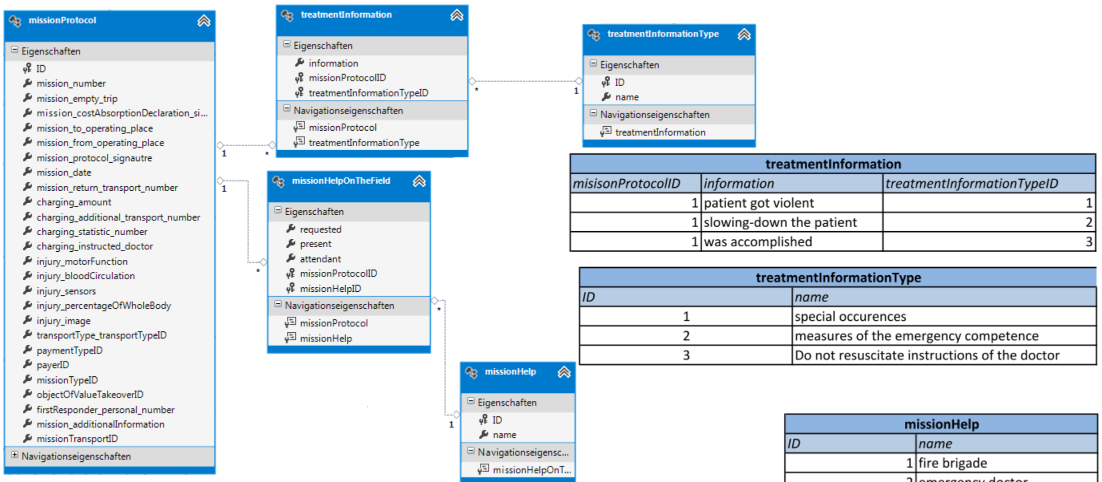
Basically, the mission protocol consists of three sections: the *mission invoicing*, the *mission* itself, and the *medical data*. The section *mission invoicing* contains the selected data of the e-card, the payment information as well as general information about the mission. This general information includes the mission number and date, the start- and end-address, the times associated with the mission as well as the personal-IDs of all mission crew members. Next, the section *mission* contains the cost absorption declaration, the revers section including information about the witness, the attended/ordered emergency help as well as general information about the treatment of the patient. Finally, the medical data includes the ambulatory recordings, treatment information, the Glasgow Coma Scale of the patient, a graphical representation of the injured body parts, the symptoms, information about the medical state of the patient, as well as the emergency diagnose and in case of death all related death information. Moreover, the mission protocol has to be signed. Without a signature, the creation of the mission protocol is neither finished nor is the document itself valid.

4.6.2 Mission Data

The mission data of the database illustrate not only the section *mission invoicing*, but also the section *mission* of the mission protocol. This data is not only linked to the mission data, but also to the invoicing data as well as to the patient medical data. Without these relations neither statistical evaluations nor the link between the medical data and the patient itself would be possible. In this section the structure of the database as well as some database snippets for the storage of the mission data will be discussed.

The table *missionProtocol* is the central entity to which many entities are connected (for more details see figure 4.31 in section 4.6.4). Figure 4.23 shows the database structure behind the storage of the organizations and people that help on location and the times associated with the mission (see table *missionHelp*). In addition, the "mission help" can be kept on file as requested, attendant or present. With the definition of these three possibilities corresponding database entries can be stored in the table *missionHelpOnTheField*. Furthermore, the table *transportTimeType* shows all times, which can be defined.

Although the mission number uniquely identifies a mission protocol, the *missionProtocolID* is used as primary key for a very specific reason: the mission number includes an alphanumeric value that prevents the use as primary key in *Windows SQL Server 2012*.



treatmentInformation		
misisonProtocolID	information	treatmentInformationTypeID
1	patient got violent	1
1	slowing-down the patient	2
1	was accomplished	3

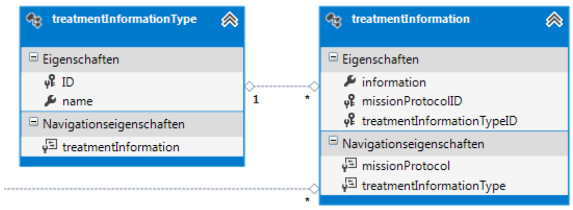
treatmentInformationType	
ID	name
1	special occurences
2	measures of the emergency competence
3	Do not resuscitate instructions of the doctor

missionHelpOnTheField				
missionProtocolID	missionHelpID	requested	present	attendant
1	2	true	true	false
1	3	false	false	true
2	5	true	false	false

missionHelp	
ID	name
1	fire brigade
2	emergency doctor
3	doctor
4	executive
5	mountain rescue
6	first responder
7	first responder paramedic

Figure 4.23: Mission protocol

General information about the mission and the treatment of the patient is included in the mission area of the mission protocol. Figure 4.24 shows the three kinds of information in this area.



treatmentInformation		
misisonProtocolID	information	treatmentInformationTypeID
1	patient got violent	1
1	slowing-down the patient	2
1	was accomplished	3

treatmentInformationType	
ID	name
1	special occurences
2	measures of the emergency competence
3	Do not resuscitate instructions of the doctor

Figure 4.24: General treatment information

The *mission invoicing* area of the mission protocol contains, among others, the personnel-IDs of each crew member, the start- and end-address of the mission, the license plate number of the emergency car as well as information about the patient and the insurant. Figure 4.25 illustrates the structure for the storage of this information. There are two types of crew members: the *physician* and the *emergency doctor*. Those crew members are uniquely identifiable by their corresponding personal-ID. The patient and the insurant, on the other hand, can be uniquely identified by their social security number including their birthday.

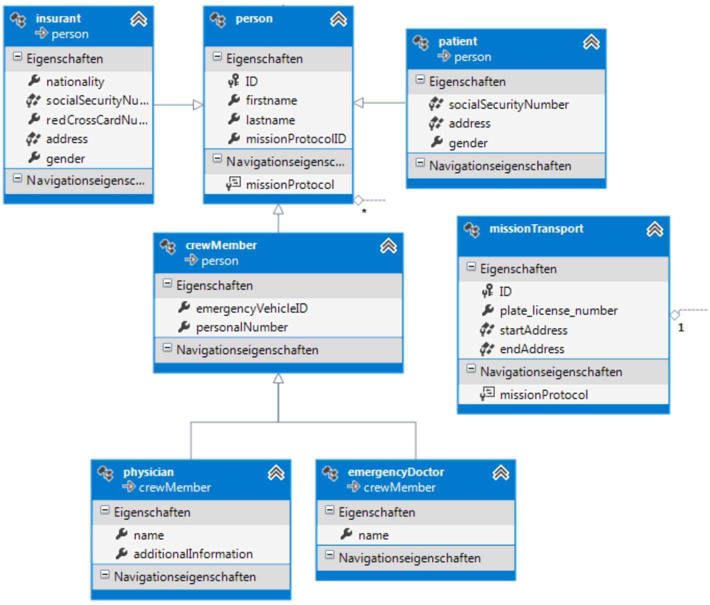


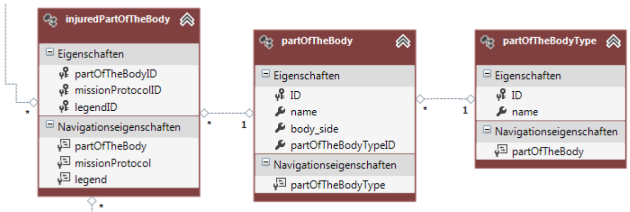
Figure 4.25: Crew member, insurant and mission address information

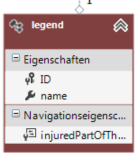
4.6.3 Medical Data

In this section the medical data area of the mission protocol and the storage of the corresponding data within the database will be discussed. Moreover, some medical aspects will be graphically shown and the database structure of some medical parts will be explained. All floating connections shown on the pictures of the database structure define a connection to the central table *missionProtocol*. For more information about the connection to the central table *missionProtocol* have a look at the section 4.6.4.

Figure 4.26 shows the structure of the database for the storage of the injured body parts. The reference table *partOfTheBody* contains all body parts including a unique number as well as a the specific anatomy name. In order to support statistic analysis each body part is associated with a corresponding body part type. With this association not only head injuries but also leg and arm injuries can be queried more easily. Moreover, there are three different kinds of injuries: *pain*, *paralysis* and *wound*. These kinds of injuries combined with the corresponding body part result in the injured body part, which can be seen in the table *injuredPartOfTheBody*.

Furthermore, several additional injury types, which are not connected with a specific part of the body, but for the whole body itself, can be distinguished. Figure 4.27 shows the corresponding database tables for the storage of the theses additional injury types.





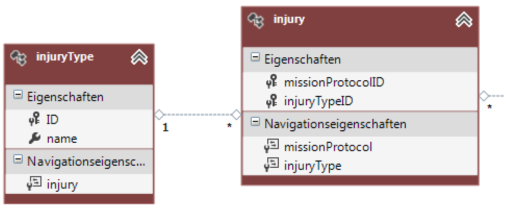
injuredPartOfTheBody		
legendID	*partOfTheBodyID*	*missionProtocolID*
2	10	1
3	5	1
1	6	1

legend	
ID	*name*
1	pain
2	paralysis
3	wound

partOfTheBodyType	
ID	*name*
1	head
2	leg
3	arm
4	belly
5	other

partOfTheBody		
partNumber	*partOfTheBodyTypeID*	*name*
1	2	posterior left foot
2	2	anterior right ankle
3	2	posterior lower leg left
4	2	anterior left knee
5	2	anterior upper leg left
6	1	anterior right ear
7	1	anterior left ear
8	2	posterior right knee
9	3	posterior lower arm right
10	3	posterior lower arm right
11	1	anterior left eye
12	1	anterior right eye

Figure 4.26: Injured body parts



injuryType	
ID	*name*
1	burn
2	scald
3	chemical burn
4	frostbite
5	inhalation injury

injury	
injuryTypeID	*missionProtocolID*
2	1
3	1
4	2

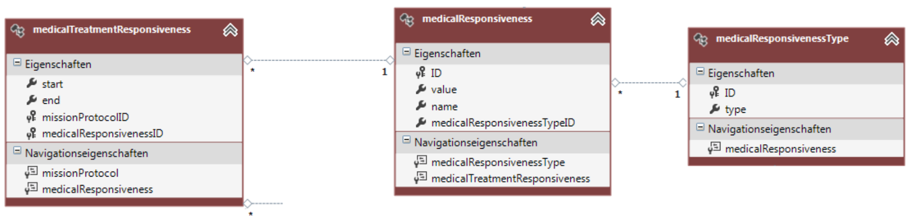
Figure 4.27: Injury types

In order to analyse the consciousness of a patient more easily, the standardized **Glasgow Coma Scale** will be calculated for each patient. There are three distinguishable categories of which a behaviour with a corresponding score will be chosen. The Glasgow Coma Scale is not only be calculated in the field, but also for the time the patient arrives at the hospital.

A total score of 15 means *best response*, 8 or less *comatose client* and a score of 3 *totally unresponsive* [43].

Category	**Response**	**Score**
Eye opening	Spontaneously	4
	To speech	3
	To pain	2
	No response	1
Verbal	Oriented to time, place, and person	5
	Confused	4
	Inappropriate words	3
	Incomprehensible sounds	2
	No response	1
Motor	Obeys commands	6
	Moves to localized pain	5
	Flexion withdrawal from pain	4
	Abnormal flexion	3
	Abnormal extension	2
	No response	1

Table 4.1: Glasgow Coma Scale [43]



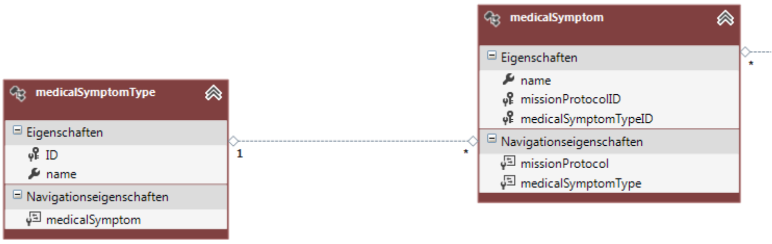
medicalResponsivenessType	
ID	*name*
1	eyes opening
2	verbal
3	motor

medicalTreatmentResponsiveness			
start	*end*	*medicalResponsivenessID*	*missionProtocolID*
true	true	3	1
false	true	2	1
true	false	1	1

medicalResponsiveness				
missionProtocolID	*ID*	*value*	*name*	*medicalResponsivenessTypeID*
1	1	1	none	3
1	2	4	spontaneous	1
1	3	4	confused	2

Figure 4.28: Consciousness of the patient

During the examination by a doctor several symptoms may be determined, among which *hemorrhage*, *poisoning* and the *delivery* can be distinguished. Figure 4.29 shows a few specialized symptoms of the whole list of symptoms, which can be selected in the mission protocol.



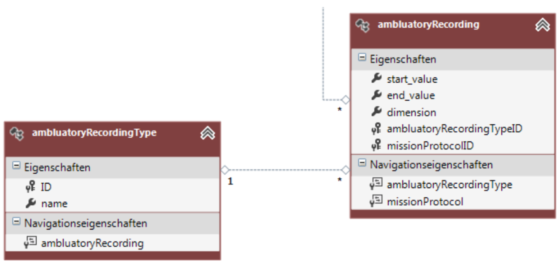
medicalSymptom		
medicalSymptomTypeID	*name*	*missionProtocolID*
1	hemoptysis	1
1	hematemesis	1
2	meds	1
2	foodstuff	1
3	abdominal pain	1
3	contractions	1

medicalSymptomType	
ID	*name*
1	hemorrhage
2	poisoning
3	delivery

Figure 4.29: Medical symptoms

In order to find out the current medical state of a patient more easily several ambulatory recordings have to be made. Not only the *breathing rate*, but also the *heart rate* and the SpO^2 level may be determined. As the dimensions of those recordings differ from each other not only the start and end value, but also the corresponding dimension has to be stored in the database. In case of the medical recordings defined within the mission protocol, the corresponding dimensions are already listed, so that only the specific value has to be entered. Figure 4.30 illustrates all ambulatory recordings, which include a start and a end value and shows examples for the storage of recordings in the corresponding tables.

ambluatoryRecordingType	
ID	*name*
1	breathing rate
2	heart rate
3	SpO2
4	Riva-Rocci



ambluatoryRecording				
start_value	*end_value*	*dimension*	*ambluatoryRecordingTypeID*	*missionProtocolID*
150	130	1/min	2	1
15	17	1/min	1	1
90	90	%	3	1
140/90	140/90	mmHg	4	1

Figure 4.30: Ambluatory recording

4.6.4 Whole Database Structure

Figure 4.31 shows the entity relationship diagram of the database, which is used by the patient terminal. The entities shown in this diagram are marked with the colors blue and brown. The color blue refers to entities that are related to the mission and the color brown defines all treatment related data.

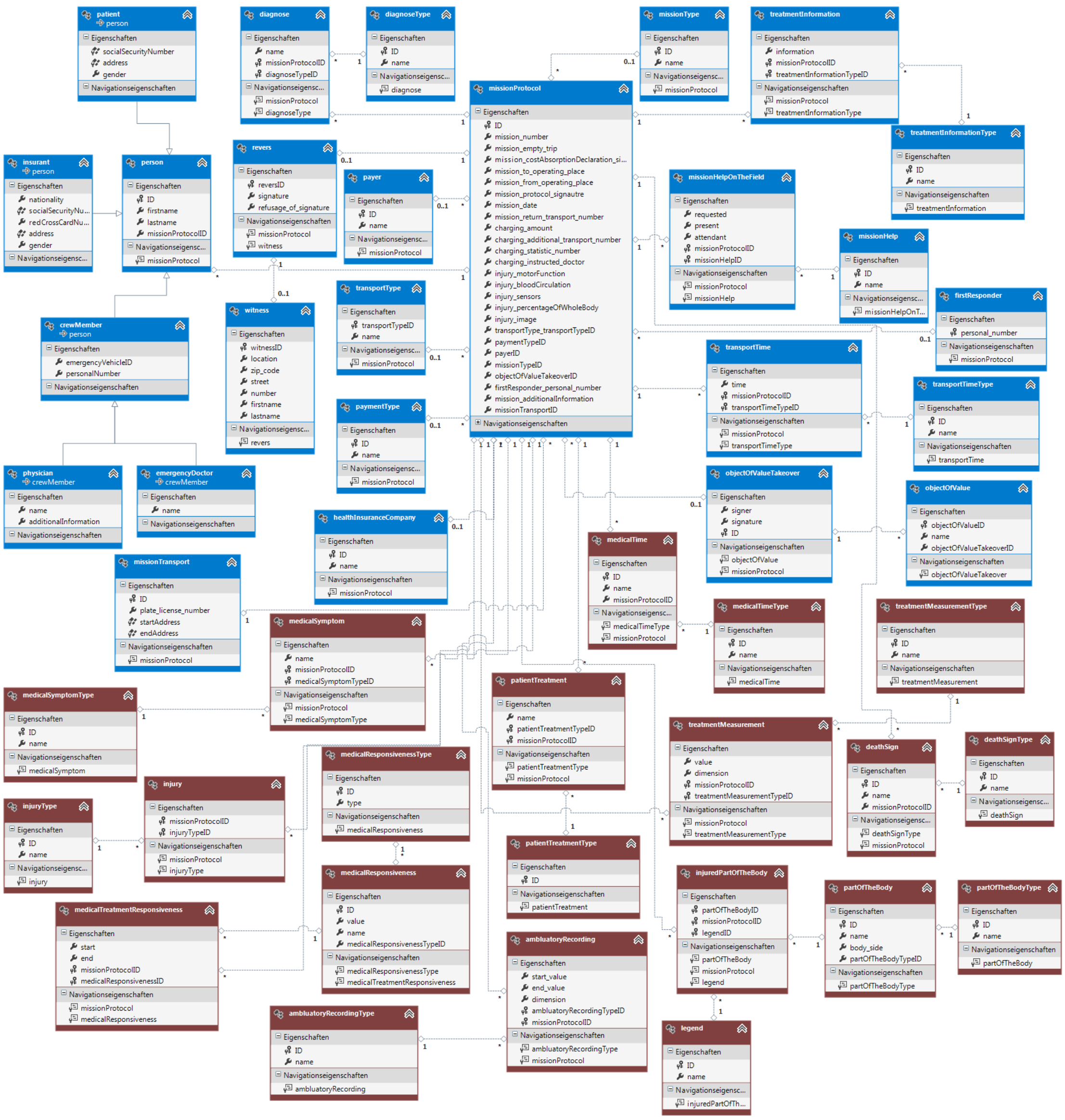


Figure 4.31: Database structure

4.7 Evaluation

The implementation of a patient documentation system is no easy task. There are several country-dependent laws which have to be considered for the processing and storage of medical data. In order to design a GUI-Prototype that can be used for ambulance operations, reviews with four members of the Styrian Red Cross have been held. The results of these reviews have helped a lot in the process of designing the user interface and the related business-logic. Some selected parts of these results are included in the following list:

- Users have to be able to tell the name and birthday of a patient in a mission at a glance
- The filling in of data is no sequential process. Most of the time the paramedics fill in several sections at different times during missions, sometimes even after the mission has been completed. Therefore, users must be able to see the missing parts of a mission protocol at once.
- Due to the fact that paramedics are personally liable for any mistakes in the mission protocol, the definition of the time when the mission protocol is finished is an extremely sensitive subject.
- At the time when the mission protocol is finished changes have to be logged with the corresponding period of time and the information about the editor.

Moreover, the final version of the GUI-Prototype has been presented to the same four members of the Styrian Red Cross. These members have mentioned that the user interface is intuitive and could be accepted by paramedics in Austria.

5 Conclusion and Future Work

This chapter will summarize the work in this thesis. Moreover, the outlook will present some possible extensions of the mobile application that could be implemented in the future.

5.1 Conclusion

On the one hand a mobile application for the documentation of ambulance operations had to be implemented, but on the other hand the connection to medical devices in the ambulance cars, the data protection standards for medical data as well as a concept for the data transfer between the mobile application and a rescue centre had to be developed. At first, analyses regarding the design and the requirements of such as a system have been made. Therefore, discussions with the Styrian Red Cross have been taken place. Due to the fact that paramedics are legally bound to protocolling all their actions, during ambulance operations, this application represents a digital mission protocol system. In addition, the system is also referred to as "patient terminal". The following sections will provide an informative overview of the work in this thesis.

5.1.1 Hardware Components

As mission protocols are filled in by the paramedics in the transport area of ambulance cars, a terminal, which is robust enough to withstand the vibrations in moving cars and the accidentally falling down, had to be found. In addition, there are certain hygiene requirements in the transport area of ambulance cars. Thus, the terminal must also be water- and dust-resistant. The decision was made in favour of the rugged *Fieldbook B1* tablet. This tablet does not only fulfil the requirements, but also provides technologies that could be useful in the future. These technologies include NFC that enables the contactless authentication on the mobile application.

5.1.2 Medical Devices

There are several medical devices in a ambulance car that provide certain communication technologies for the transfer of data. In case of the Styrian Red Cross defibrillators and heart-rate-monitor devices are used. These devices have been analysed regarding their connection to the patient terminal. The results have shown that there are several standards for the communication with medical devices, but none for the usage of data formats. Due to the fact that the manufacturer of the analysed medical devices uses proprietary data formats, the connection to medical devices cannot be performed very easily.

5.1.3 Data Protection

In Austria the access to medical data is regulated by the data protection law. To protect the data against unauthorized access, the MAGDA-LENA guidelines have been defined by the Austrian health service commission of the Federal Municipal Administration. These guidelines are no legal obligation, but guarantee the Austrian data protection regulations. To put the results of the analysis in a nutshell, the medical data cannot be locally stored on the patient terminal, but somewhere in a secure location. Moreover, the transfer of the data has to be performed via a secure channel.

5.1.4 Medical Test Data

In order to test the mobile application, data related to ambulance operations have been provided by the Styrian Red Cross. This data is sent by an operating mission system to a data terminal that is located in the front of the ambulance car. The data terminal represents the user interface of the operating mission system and supports the ambulance operations by the help of a navigation system. In addition, an e-card reader can be directly connected to the data terminal to retrieve the patient's insurance data. Moreover, the patient terminal is connected to the data terminal via WLAN. In order to establish a communication between these two terminals, a client-server application has been implemented. The mission protocol data does not only include mission related, but also treatment and patient data. As the mission data is sent by the operating mission system, the paramedics do not have to fill in many mission-related data fields. The focus lays mainly on the documentation of the treatment information.

5.1.5 Mobile Application

The mission protocols, which will be filled in by the paramedics, on the mobile application, do not only contain input fields, but also a graphical patient sketch in which the injured body parts can be marked. The implementation is based on the MVVM pattern. This means that there is a strict distinction between the user interface, the data that is bound to the user interface, and the model that is used for the business logic. The mobile application has been implemented as WPF application. Thus, the user interface is defined by several XAML-files, containing the UI-elements.

5.1.6 Database

Due to the regulations in the Austrian data protection law, the data shall be stored on a secure location, like the gateway server (see section 4.3.1). However, for testing purposes the data is stored on the patient terminal. Therefore, a entity relationship diagram that does not only cover the mission-, but also the patient- and the treatment information had to be designed. This database enables statistical evaluations and provides basic medical history information about patients. In order to do so, the treatment data has to be linked to the mission and the patient data. For the storage of the data a Microsoft SQL Server 2012 database has been used. Moreover, as the data has to be stored on a secure location, Services for the retrieving of medical data via the Internet have to be provided. Due to the high protocol overhead of SOAP-services, REST-Service combined with SSL, that encrypts the channel between the client and the Service, could be used.

5.2 Future Work

Due to test purposes the data entered in the mobile application is locally stored on the patient terminal. In practice all data should be moved to a secure location such as the gateway server, which has been shown in the section 4.3.1. Thus, a secure connection between the patient terminal and the gateway server has to be established. In addition, REST-Services in combination with SSL have to be implemented. Thus, the data can be retrieved from anywhere within the Internet. Moreover, pdf-documents could be automatically generated by the help of the mission protocol data that are stored in the *Microsoft SQL Server 2012* database. In addition, these mission protocols could be signed by the help of digital signatures. Currently, no authentication mechanism on the patient terminal is implemented. In the future, NFC-tags could be used as authentication mechanism, in which the NFC-tags represent the personnel cards of the paramedics and the medical doctors. Due to the high protection standards of medical data and the fact that the paramedics are personally liable for any mistakes regarding the treatment by signing the mission protocol, additional security mechanisms have to be implemented. Especially, in cases in which the paramedics loose the personnel card, the unauthorized usage of these cards has to be prevented. The cards could be used in combination with a password that is frequently changed. However, this is an extremely sensitive subject that may have to be embodied in the Austrian data protection law.

List of Abbreviations

S/MIME Secure / Multipurpose Internet Mail Extensions

SSL Secure Sockets Layer

TLS Transport Layer Security

IPSEC Internet Protocol Security

IDEA International Data Encryption Algorithm

3DES Triple Data Encryption Standard

AES Advanced Encryption Standard

ICD International Statistical Classification of Diseases and Related Health Problems

SOAP Simple Object Access Protocol

REST Representational State Transfer

MAGDA-LENA The medical-administrative health data exchange-logical and electronic network Austria

LINQ Language Integrated Query

WPF Windows Presentation Foundation

ERM Entity Relationship Model

ORM Object Relational Mapping

MVVM Model View ViewModel

GCS Glasgow Coma Scale

EMS Emergency Medical Service

NFC Near Field Communication

IP Ingress Protection Rating

Bibliography

[1] DLOG PWS 770. Website. Available online at http://www.dlog.com/main-navigation/produkte/104-tablet-pc/pws-770/pws-770-beschreibung/; visited on September 23th 2013. 32, 33

[2] ELEKTRA+. Website, 2008. Available online at http://www.pressetext.com/news/20081017018; visited on February 6th 2014. 3

[3] S. Al-Shaqsi. Models of International Emergency Medical Service (EMS) Systems. *Oman Med J*, 25(4):320–3, 2010. vi, 1, 4, 5

[4] Austrian Ministry for Health. International Statistical Classification of Diseases and Related Health Problems (ICD), 10. Revision - BMG-Version 2013. Website. Available online at http://bmg.gv.at/cms/home/attachments/1/1/2/CH1241/CMS1287572751172/icd-10_bmg_2013_-_systematisches_verzeichnis.pdf; visited on November 13th 2013. 42

[5] Austrian Office of the Federal Chancellor. The Austrian Citizen Card. Website. Available online at http://www.buergerkarte.at/konzept/securitylayer/spezifikation/20040514/introduction/Introduction.en.html; visited on September 10th 2013. iv, 15, 16

[6] K. Banitsas, S. Tachakra, E. Stefanidis, and K. Boletis. Using HSPA to improve the telemedical links on a moving ambulance. In *Engineering in Medicine and Biology Society, 2008. EMBS 2008. 30th Annual International Conference of the IEEE*, pages 739–742, 2008. vi, 6

[7] S. Beul, S. Mennicken, M. Ziefle, and E. Jakobs. What happens after calling the ambulance: Information, communication, and acceptance issues in a telemedical workflow. In *Information Society (i-Society), 2010 International Conference on*, pages 98–103, 2010. iv, 10, 11

[8] H. Burggasser, W. Dorda, J. Gambal, G. Gell, H. Ingruber, W. Kotschy, E. Leitge, J. Mittheisz, K. Pfeiffer, O. Pjeta, M. Pregartbauer, and H. Tinhofer. Standards and guidlines for the usage of informatic in the Austrian health service. Website. Available

online at http://www.meduniwien.ac.at/msi/mias/STRING/; visited on August 29th 2013. 3, 26, 27

[9] Chipcard. E-card. Website. Available online at http://www.chipkarte.at/portal27/portal/ecardportal/start/startWindow?action=2&p_menuid=51682&p_tabid=1; visited on September 9th 2013. 14, 15

[10] Corpuls. corpuls.web. Website. Available online at http://www.corpuls.com/en/products/corpulsweb.html; visited on October 18th 2013. iv, 41

[11] G. Crowe. The meaning of 'rugged': 8 test behind MIL-STD ratings. Website. Available online at http://gcn.com/Articles/2013/05/08/8-tests-behind-MIL-STD-ratings.aspx?Page=3; visited on September 2nd 2013. 26

[12] diopgmbh.com. Application - Ambulances, operating theatres. Website. Available online at http://www.diopgmbh.com/en/anwendungsbereiche/krankenwagen-ops/; visited on September 2nd 2013. 30

[13] S. Dünnebeil, F. Köbler, P. Koene, J. Leimeister, and H. Krcmar. Encrypted NFC Emergency Tags Based on the German Telematics Infrastructure. In *Near Field Communication (NFC), 2011 3rd International Workshop on*, pages 50–55, 2011. iv, 16, 17, 18

[14] Fieldbook. Fieldbook B1 - Full Rugged Tablet PC. Website. Available online at http://www.logic-instrument.com/us/products/fieldbookrugged-tablets/rugged-tablet-pcs/fieldbook-b1.html; visited on September 23th 2013. 31, 33

[15] Getac. Certification. Website. Available online at http://en.getac.com/solutions/certifications.html; visited on September 2nd 2013. 22, 23

[16] Gilbert Sandner. private communication, October 2013. Styrian Red Cross. 58

[17] A. Gries, M. Helm, and E. Martin. Zukunft der präklinischen Notfallmedizin in Deutschland. *Der Anaesthesist*, 52(8):718–724, 2003. 11

[18] R. Hussain, J. Son, H. Eun, S. Kim, and H. Oh. Rethinking Vehicular Communications: Merging VANET with cloud computing. In *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*, pages 606–609, 2012. 7

[19] impactit - mobile computing. Edocta. Website. Available online at http://www.impact.co.at/produkte/edocta/; visited on January 27th 2014. vi, 3, 4

[20] ITU. E-health Standards and Interoperability. *ITU-T Technology Watch Report*, April 2012. 38

[21] Janek Schumann. private communication, October 2013. GS Elektromed. Geräte G. Stemple GmbH. vi, 39, 40

[22] A. J. Jara, M. A. Zamora, and A. F. G. Skarmeta. Secure use of NFC in medical environments. In *RFID Systems and Technologies (RFID SysTech), 2009 5th European Workshop on*, pages 1–8, 2009. 17

[23] JLT mobile computers. jFlex - FLEXIBLE FIXED. Website. Available online at url = http://www.jltmobile.com/jlt/en-us/jflex/jflex-1.246.1.php; visited on September 23th 2013. 32, 33

[24] J. E. Kim, Y.-K. Son, B. Kim, S. Shin, and I.-Y. Cho. Entwear: A durable smart jacket to control media devices. In *Consumer Electronics (ICCE), 2012 IEEE International Conference on*, pages 568–569, 2012. 34

[25] J. Langer and M. Roland. *Anwendungen und Technik Von Near Field Communication (NFC)*. Springer, 2010. 3, 16, 50, 51

[26] R. Lim. A Simple MVVM Example. Website. Available online at `http://rachel53461.wordpress.com/2011/05/08/simplemvvmexample/`; visited on January 6th 2014. 65

[27] W. Liu, Y. Yang, and M. Zhu. Research on inter hospital and ambulance data transmission using LT-coding over VANET. In *Complex Medical Engineering (CME), 2013 ICME International Conference on*, pages 119–123, 2013. iv, 6, 7

[28] Microsoft. Implementing the MVVM Pattern. Website. Available online at `http://msdn.microsoft.com/en-us/library/gg405484(v=pandp.40).aspx`; visited on January 6th 2014. iv, 63, 64, 65

[29] Microsoft Developer Network. Introduction to WPF. Website. Available online at `http://msdn.microsoft.com/en-us/library/aa970268(v=vs.110).aspx`; visited on January 26th 2014. 55

[30] Microsoft MSDN. Guidelines for form layouts (Windows Store apps). Website. Available online at `http://msdn.microsoft.com/en-us/library/windows/apps/jj839734.aspx`; visited on October 28th 2013. 47

[31] Mike Liu. LINQ to SQL: Basic Concepts and Features. Website. Available online at `http://www.codeproject.com/Articles/215712/LINQ-to-SQL-Basic-Concepts-and-Features`; visited on January 8th 2014. iv, 70, 71

[32] Motion. Motion C5t Tablet PC. Website. Available online at http://www.motioncomputing.com/products/tablet_pc_c5.asp; visited on September 23th 2013. 31, 33

[33] MSDN. Visual Studio. Website. Available online at http://www.visualstudio.com/en-us/explore/application-development-vs; visited on January 26th 2014. 54

[34] A. Nathan. *WPF 4: Unleashed*. Sams Publishing, 2010. 64

[35] T. Neil. *Mobile Design Pattern Gallery: UI Patterns for Mobile Applications*. Oreilly and Associate Series. O'Reilly Media, Incorporated, 2012. 47, 48

[36] Office of the Federal Chancellor. Federal Act on Electronic Signatures, signature law - SigG, BGBl. I Nr. 190/1999. Website, 1999. Available online at https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10003685; visited on August 29th 2013. 28

[37] Office of the Federal Chancellor. Data protection act 2000 - DSG 2000, BGBl. I Nr. 165/1999. Website, 2000. Available online at http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597; visited on January 15th 2014. 26, 27, 62

[38] Office of the Federal Chancellor. Austrian Act on Ambulance Service Members - SanG. Website, 2002. Available online at http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001744&ShowPrintPreview=False; visited on January 15th 2014. II, III, 1

[39] Office of the Federal Chancellor. Statutory provision of the digital signature decree - SigV 2008. Website, 2008. Available online at https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20005618; visited on August 29th 2013. 15, 28

[40] Official Journal of the European Union. COUNCIL REGULATION (EC) No 199/2008 concerning the establishment of a Community framework for the collection, management and use of data in the fisheries sector and support for scientific advice regarding the Common Fisheries Policy. Website, 2008. Available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:060:0001:0012:EN:PDF; visited on January 15th 2014. 26

[41] Official Journal of the European Union. Opinion of the European Data Protection Supervisor on the proposal for a directive of the European Parliament and of the Council on the application of patientsâ rights in cross-border healthcare. Website, 2009.

Available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:128:0020:0027:EN:PDF; visited on January 15th 2014. 27

[42] H. Otter. Basic information about the E-card. Website. Available online at http://www.telemedizinfuehrer.de/free/s_2006/otter_98_103.pdf; visited on September 9th 2013. iv, 15

[43] Pearson Education. Glasgow Coma Scale. Website. Available online at http://wps.prenhall.com/chet_burke_medicalsur_2/47/12084/3093682.cw/content/index.html; visited on November 10th 2013. vi, 59, 88

[44] P. D. rer. nat. habil. Bruno Ismer. Messpraktikum Herzrhythmustechnologie. Website. Available online at http://www.bruno-ismer.com/de/messpraktikumreveal.htm; visited on January 10th 2014. 61

[45] A. Riener. Gestural Interaction in Vehicular Applications. *Computer*, 45(4):42–47, 2012. 34

[46] Rosetta Code. Bitmap Flood fill. Website. Available online at http://rosettacode.org/wiki/Bitmap/Flood_fill#C.23*/; visited on January 8th 2014. 74

[47] Rudi Latuske. In order to solve the interoperability problem between medical devices special standards have to be defined. Available from http://www.ars2000.com/. 39

[48] L. Schmitt, T. Falck, F. Wartena, and D. Simons. Novel iso/ieee 11073 standards for personal telehealth systems interoperability. In *High Confidence Medical Devices, Software, and Systems and Medical Device Plug-and-Play Interoperability, 2007. HCMDSS-MDPnP. Joint Workshop on*, pages 146–148, 2007. 39

[49] Science Partner. IP-classification. Website. Available online at http://www.sp.se/en/index/services/ip/sidor/default.aspx; visited on August 28th 2013. 22

[50] B. Shneiderman and C. Plaisant. *Designing the User Interface: Strategies for Effective Human-Computer Interaction (5th Edition)*. ADDISON WESLEY Publishing Company Incorporated, 2010. 47, 48

[51] S. I. M. Solutions. MAC OS Ruhe-EKG Software. Website. Available online at http://www.sr-med.com/cardioscout-multi-ecg-5#.UuDJsRCIWUk; visited on January 10th 2014. 61

[52] M. Steyer, H. Schwichtenberg, J. Krause, and M. Fischer. *Verteilte Systeme und Services mit .NET 4.5: Konzepte und Lösungen für WCF 4.5 und ASP.NET Web-API*. .net Bibliothek. Hanser Fachbuchverlag, 2013. 42, 43, 44, 45

[53] S. Teller, M. Walter, M. Antone, A. Correa, R. Davis, L. Fletcher, E. Frazzoli, J. Glass, J. How, A. Huang, J. hwan Jeon, S. Karaman, B. Luders, N. Roy, and T. Sainath. A voice-commandable robotic forklift working alongside humans in minimally-prepared outdoor environments. In *Robotics and Automation (ICRA), 2010 IEEE International Conference*, pages 526–533, 2010. iv, 19

[54] J. Tidwell. *Designing Interfaces*. O'Reilly Media, 2010. 47, 48

[55] K. Tokuda and S. Ohmori. Demonstration experiments of SAFER (Speedy Ambulance First-aid, Emergency, Rescue operations supporting) system. In *Wireless Personal Multimedia Communications (WPMC), 2011 14th International Symposium on*, pages 1–5, 2011. iv, 7, 8, 9

[56] R. Tolentino, J.-H. Hwang, S.-H. Kim, Y.-T. Kim, G. cheol Park, and D.-J. Hwang. A Proposal of Building an Early-Stage Diagnosis System of First-Aid through Wireless Internet. In *Convergence and Hybrid Information Technology, 2008. ICHIT '08. International Conference on*, pages 70–74, 2008. 5

[57] N. Uchida, K. Takahata, Y. Shibata, and N. Shiratori. Local Area Network Reactivation in Never Die Network for a Large Scale Disaster. In *Network-Based Information Systems (NBiS), 2012 15th International Conference on*, pages 89–96, 2012. iv, 20, 21

[58] U.S. Department of Defense. Test method standard. Website, 2008. Available online at `http://www.atec.army.mil/publications/Mil-Std-810G/Mil-Std-810G.pdf`; visited on September 2nd 2013. vi, 23, 24, 25, 26

[59] R. Wijesiriwardana, K. Mitcham, W. Hurley, and T. Dias. Capacitive fiber-meshed transducers for touch and proximity-sensing applications. *Sensors Journal, IEEE*, 5(5):989–994, 2005. 34

[60] Windows Corporation. Windows User Experience Interaction Guidelines. Website. Available online at `http://msdn.microsoft.com/en-US/windows/desktop/aa511258`; visited on October 29th 2013. iv, vi, 48, 49

[61] World Health Organization. International Classification of Diseases (ICD). Website, 2010. Available online at `http://www.who.int/classifications/icd/en/`; visited on November 13th 2013. 42

[62] L. Young and M. Ishii. One Force Tactical Communications System: Connecting the Tactical Edge at AEWE Spiral G. In *Military Communications Conference, 2012 - MILCOM 2012*, pages 1–4, 2012. iv, 20, 21