MOBISERV – FP7 248434

An Integrated Intelligent Home Environment for the Provision of Health, Nutrition and Mobility Services to the Elderly

Final Version

D6.2: Final Coordination and Communication system prototype

Date of delivery: July 2013

Contributing Partners: LUT, SMH

Date: 2013-08-05 Version: 1.0

Document Control

Title:	**D6.2: Final Coordination and Communication system prototype**	
Project:	**MOBISERV** (FP7 248434)	
Nature:	Prototype	**Dissemination Level:** Public
Authors:	Pekka Jäppinen, Jussi Laakkonen, Petri Heinilä, Herjan van den Heuvel	
Origin:	LUT, SMH, ROBS	
Doc ID:	MOBISERV D6.2.docx	

Amendment History

Version	Date	Author	Description/Comments
v0.1	2013-01-11	LUT	Initial draft
v0.2	2013-02-13	LUT	Structure build and security analysis added.
v0.3	2013-03-19	LUT, SMH	Added secondary user UI and RBAC
v0.9	2013-07-25	LUT	Introduction, glossary, finalization
v1.0	2013-08-05	SMH	Internal review update

Table of Contents

1 Introduction

This report provides the description of the results of WP6 activities (development of the information coordination and communication support system) after the first prototype has been delivered. The focus of the WP6 has been on three separate tasks:

1. Designing the interaction of the MOBISERV components for the new functionalities envisioned for second prototype.
2. Creating the GUI for secondary users and its access control.
3. Analysing the security and privacy risks of the complete MOBISERV system.

The results of the first task are realized in the form of sequence diagrams that display the interaction between the different system components. Effort was also put on the development of the Communication Definition Language (ComDL) which eases the process of creating MOBISERV compatible products.

The secondary users GUI was developed by using standard web development tools and it is running on the web server of the robot. This approach provides remote access for many of the features of the system and enables secondary users to setup, personalize and use the MOBISERV system. In order to protect unauthorized use of the interface, role based access control (RBAC) was developed.

Finally a thorough security and privacy risk analysis was conducted for the MOBISERV system. An illustration has been generated on this analysis to clearly show the parts of the system that require extra care and protection. For example, the aforementioned RBAC solution was developed due the findings of the security risk analysis.

It should be noted that D6.2 was heavily delayed due the change of responsibilities in WP6 and revision of the work plan. Further delay was incurred due the decision of focusing MOBISERV efforts on finalizing prototype rather than writing reports. However, the draft version, containing the designed sequence diagrams, secondary user interface and security analysis, has been available and used during the development of the second and final system prototype.

2 Glossary

Term	Explanation
AP	Access Point
BAN	Body Area Network
COM	Communications Object Model
ComDL	Communications Definition Language
DDoS	Distributed Denial of Service
GUI	Graphical User Interface
HMI	Human Machine Interface
LAN	Local Area Network
MiTM	Man in The Middle
MOBISERV	An Integrated Intelligent Home Environment for the Provision of Health, Nutrition and Mobility Services to the Elderly
ORU	Optical Recognition Unit
PRU	Physical Robotic Unit
RBAC	Role-Based Access Control
SHACU	Smart Home Automation and Communication Unit
UML	Unified Modelling Language
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Networking
WHSU	Wearable Health Supporting Unit
WLAN	Wireless Local Area Networking
WWW	World Wide Web

3 MOBISERV communication architecture & open interface approach

To establish communication between information systems, a number of development phases have to be passed. The communication between entities has to be modelled, specified and agreed by involved parties. The validness of created communication specification has to be analysed. Most importantly, the specification information must be utilized during project partners' implementations, in a way the implementation is in line with the specifications made.

Communication specification modelling consists of the following definition areas: (1) message definitions, (2) message exchange order definitions, (3) entity structure definitions and (4) parameter and side-effect definitions:

- Message definition consists of identifying the messages that are needed to establish communication between peer entities. Also the information contained in messages has to be described.
- On communications there are defined valid possible message exchange paths. Message exchange order defines how entities reacts externally to incoming messages.
- Important issue on communications modelling is to declare what are the communicating entities and what is their structure and how they are related to each other.
- The communications specification does not exist just for itself but it is created to serve distributed information systems needs to transfer information. Therefore the relevant side-effects and systems parameterization have to taken into account along the pure communications definitions.

In software communications development, it is important to have clear domains of what to specify and what not. The specification language may not dictate too much the behaviour of the communicating entities. The behaviour is hard or impossible to transform to working code. Also this will overlap the implementation language code, resulting in duplicate information bases.

Communications Definition Language (**ComDL**) is an approach to develop a system to specify software communications and then transform specification information into multiple development application areas. To establish a maximum availability, a tool-independent textual presentation for communications definitions specification is created. The purpose of communications specification work is to construct and establish interoperability between different system entities. The transformations from specification information are studied to serve this purpose.

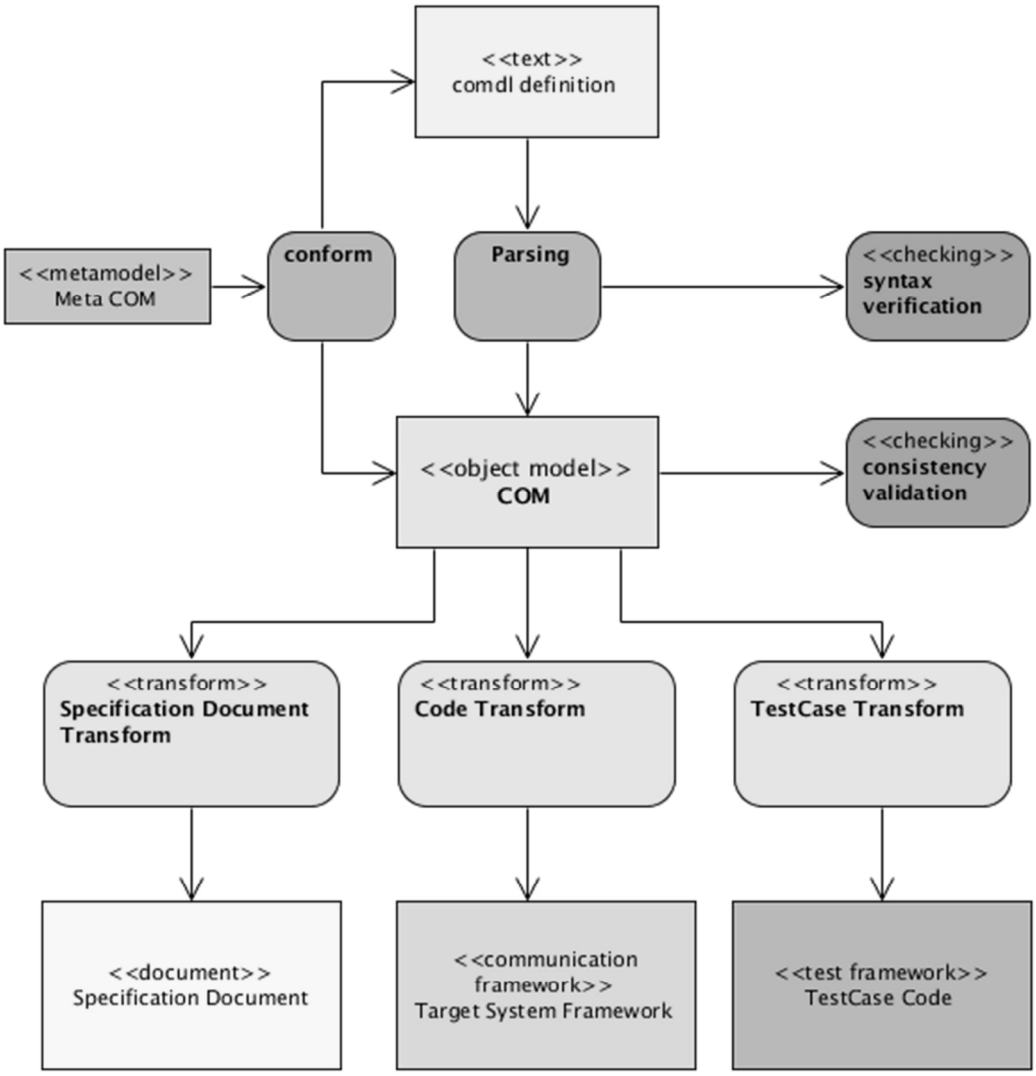


Figure 1: Communications Definition Language (ComDL) explained

- ComDL language and COM (Communications Object Model) are both defined by Meta COM UML based meta-model. Meta COM defines semantically definition elements and guides the creation of COM and ComDL language.
- Parsing component reads ComDL text source files and constructs COM object model.
- Checking components handles syntax verification and consistency validation. Syntax verification for parsing checks the text file conforms given ComDL grammar. Consistency validation ensures the name references among the COM definitions are valid.
- COM (Communications Object Model) holds the definitions in manageable object structure so that those are able to transform into target domain representations.

Transformations:

- Specification Document: Re-Specification transform is to created human friendly specification. ComDL expression definitions are defined only once, which makes reading quite hard due to the non-linearity of text. Re-specification transform arranges and creates text in manner that reading context has relevant content.
- WikiText transform or other web-based documentation systems feed the

communication information into on-line content.

- Statistics transform creates information about ComDL specification characteristics so that developers are able to evaluate and manage the specification development process.
- Target System framework: Communication framework domain source code generation transform is the main use for the ComDL system. Nowadays there exist great number of different communication systems with different policies and strategies. Idea is to transform common information base to different domains to establish inter-interoperability by adaptation.
- Codec implementation transform is used on novel communication systems to reduce the workload on message encoding and decoding functionalities. Usually codec implementations are very straightforward and regular system where automatic implementation generation can be used.
- TestCase Code: TestCase transform is used in addition to communication framework- and codec- framework transformations to find out possible errors in implementations.
- Validation transform is a form of testcase-transform, where the goal is to validate the correct functioning of the implementation.

4 Sequence Diagrams and description of the functionalities

Here we describe how the MOBISERV components interact with each other to provide the new functionalities that are implemented in final prototype. These 4 scenarios complement the 5 scenarios that were implemented before and described in Deliverable D6.1. The scenarios covered are presented in the figure below.

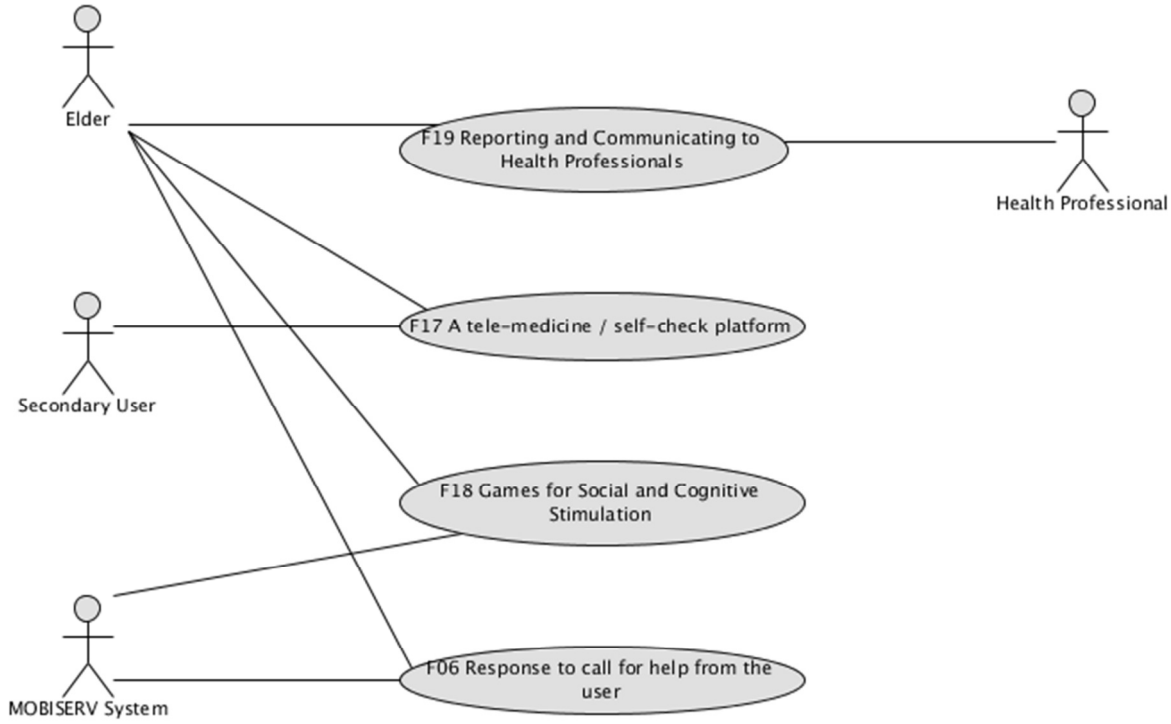


Figure 2: The Mobiserv scenarios covered in this deliverable

4.1 F19 Reporting and communicating to health professionals

In this scenario, a primary user discusses health related issues with a health professional. The MOBISERV system assists the communication to be as seamless as possible. The main scenario steps are: opening communication, on-going communication, and closing the communication. Microsoft Lync is the main global media where the communication is delivered through.

On the opening phase, the elder initiates MOBISERV system with communication activity. Interaction Manager co-ordinates MOBISERV components along the actions. First the PRU camera is activated and assigned to Lync. Lync is initiated and a video conference call to health professional is made.

Communication phase is done with provided video conferencing features. The Lync interface is embedded into PRU tabled user interface.

At the end of the discussion, the user signals closing. Then the interaction manager co-ordinates the components involved to perform connection closing and shutdown actions.

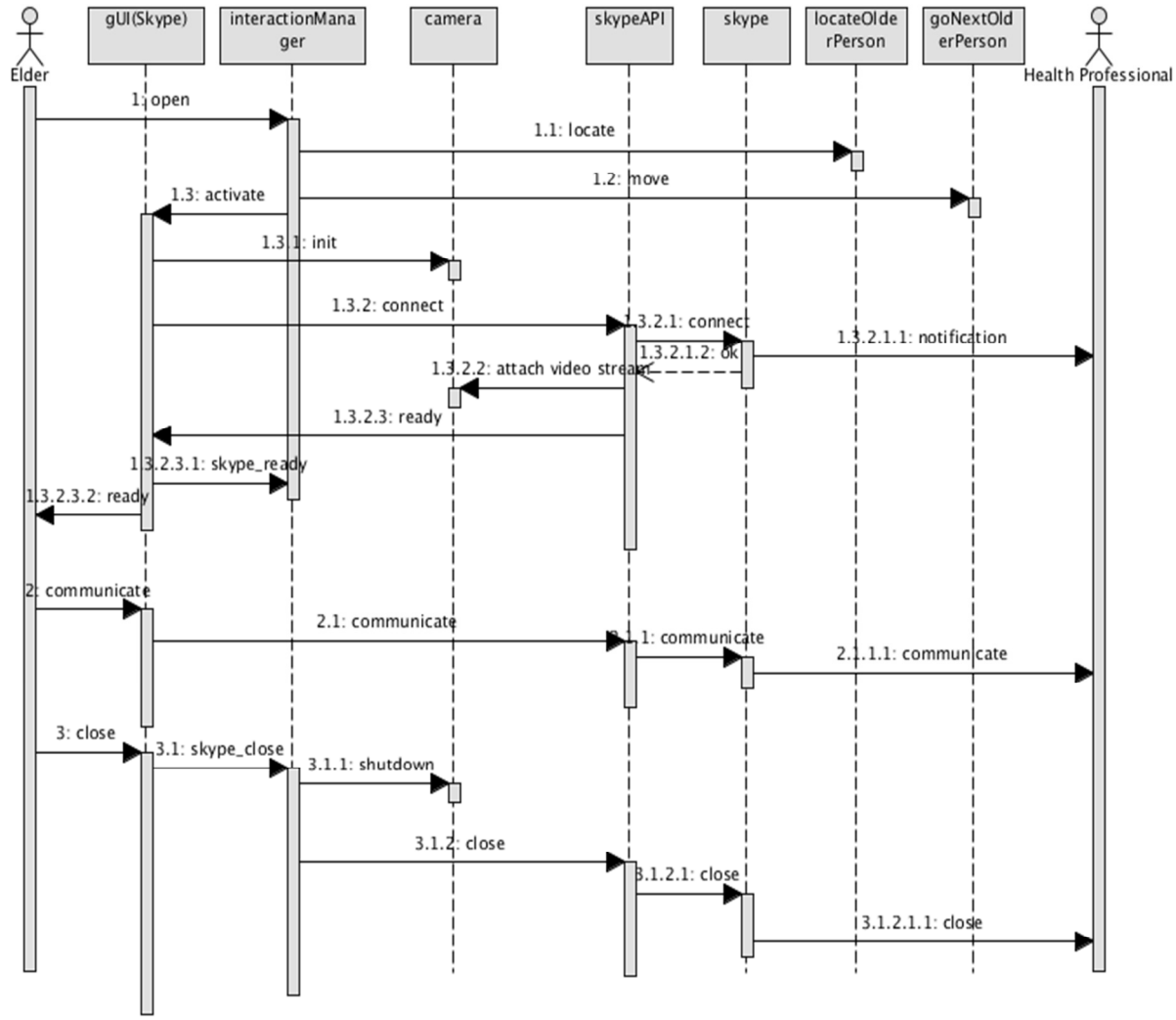


Figure 3: Sequence diagram for F19 Reporting and communicating to health professionals

4.2 F17 A tele-medicine/self-check platform

In this scenario, the MOBISERV system monitors the user's well-being trough vital signs, and alerts others when a critical situation is detected. The scenario consists of a monitoring phase and an alerting phase.

On the monitoring phase, well-being signals are gathered from WHSU sensors (in shirts, vests, pyjamas) and from the facial expression recognition by the PRU's camera. The Interaction Manager collects and combines signals and when certain thresholds are exceeded, it can initiate the alerting phase.

On the alerting sequence, the PRU is first moved towards the elder. Self-check GUI component is activated along speech communication. Elder is alarmed and dialog about well-being status is done. If well-being situation is ok the activity is closed and put back to the monitoring state. If well-being situation is not ok, the secondary user, e.g. carer, is alarmed for further actions.

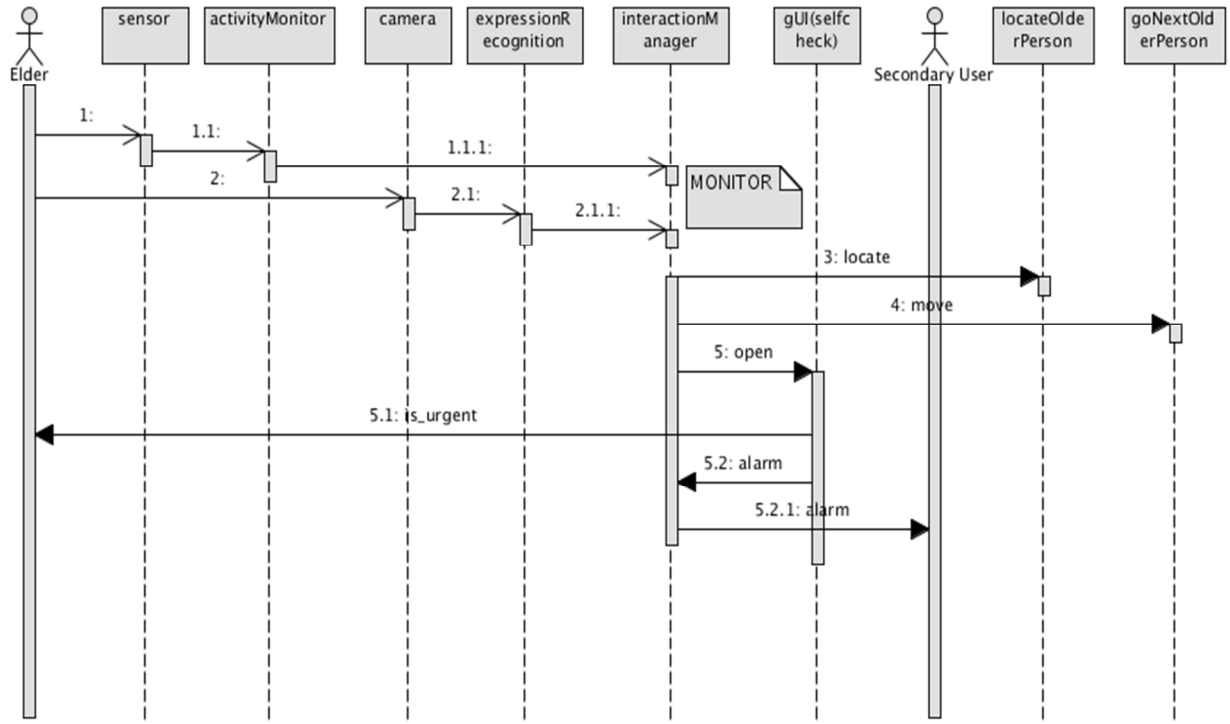


Figure 4: Sequence diagram for F17 A tele-medicine/self-check platform

4.3 F18 Games for Social and Cognitive Stimulation

In this scenario, the MOBISERV system provides games for the elder for cognitive simulation and entertainment. Scenario consists of selection and starting the game, preparing camera with recognition, play session and closing the components.

Here it is assumed that the PRU is in front of the user.

The elder selects the game through PRU tablet GUI navigation or voice recognition with Interaction Manager co-ordination. Selected game component will be started as well as facial expression recognition by the camera will be activated.

Facial expression recognition from camera will append the inputs of the game along with PRU input methods; touch-screen GUI and speech system. Game is played. After ending the game, the game component signals Interaction Manager to close active components; the expression recognition and the camera.

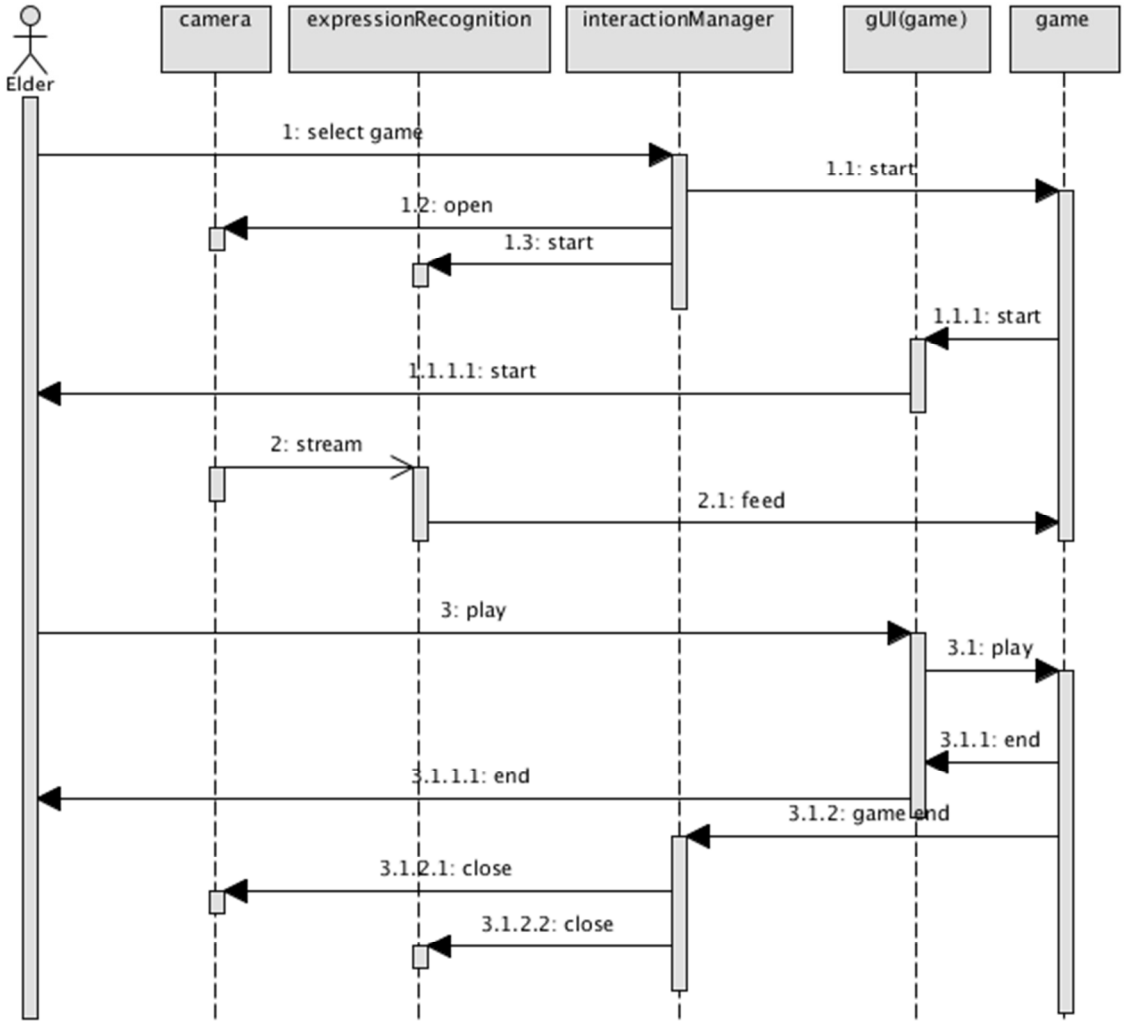


Figure 5: Sequence diagram for F18 Games for Social and Cognitive Stimulation

4.4 F6 Response to call for help from the user

In this scenario, the MOBISERV system assists the user to get help from secondary user on critical situations.

The MOBISERV system initiates a sequence by detecting an emergency situation. Alert signals are either vocal audio detection or an alert button press on PRU. The alert signal is delivered to the Interaction Manager that co-ordinates further actions. If the PRU is not located near the elder, it is will move towards the elder.

Interaction Manager starts help GUI on PRU as well as speech communication. Alert situation dialog is made where confirmation of alert situation is made. If there really is an emergency situation, the Interaction Manager is commanded to alert the preferred secondary user.

Alert communication to the secondary user is made through Lync, where first the connection to the secondary user is established, then a specific alert information is shown to secondary user. From here on, the secondary user continues to resolve the situation further.

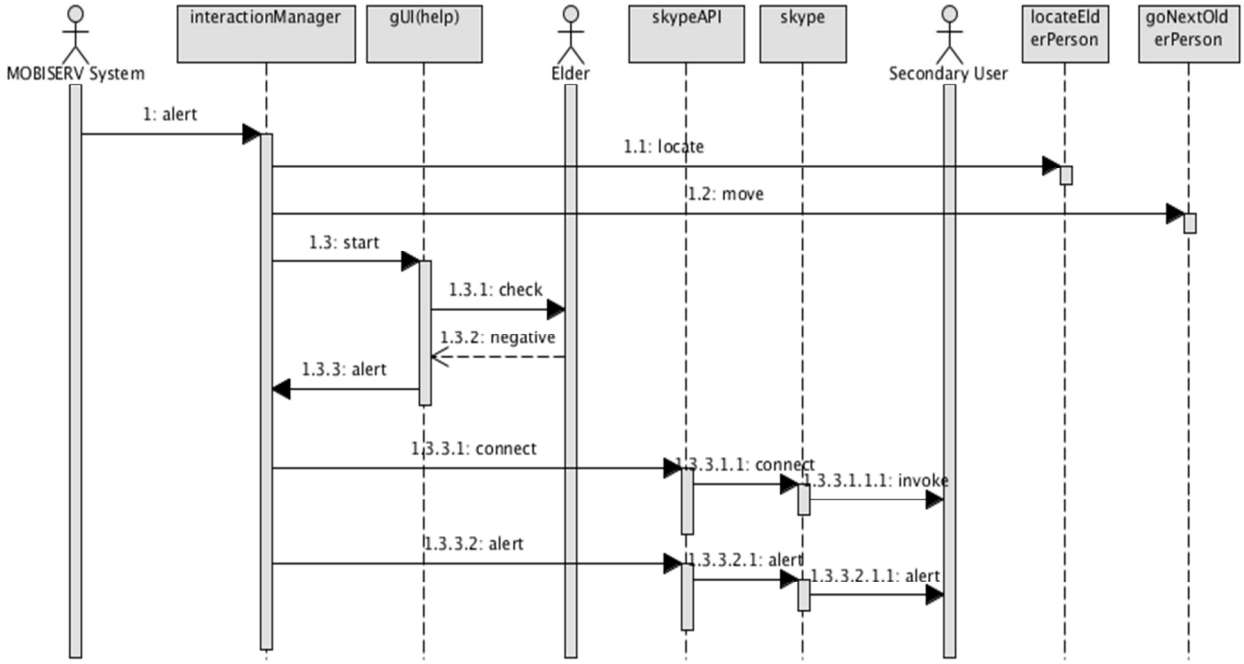


Figure 6: Sequence diagram for F6 Response to call for help from the user

5 Remote access for secondary users

During the user evaluation studies of the first MOBISERV prototype, it was found that to make the system really work in practice, personalisation of the robot behaviour is utmost importance. It was also found that the informal carer is the only right person to do this, and therefore should have very easy tools to be able to do so. Furthermore, getting an overview of how the primary user is doing is also important, as MOBISERV collects a huge amount of data. Therefore, we have designed and developed the secondary user interface – or carer interface. This interface has 3 main functions, which are interrelated:

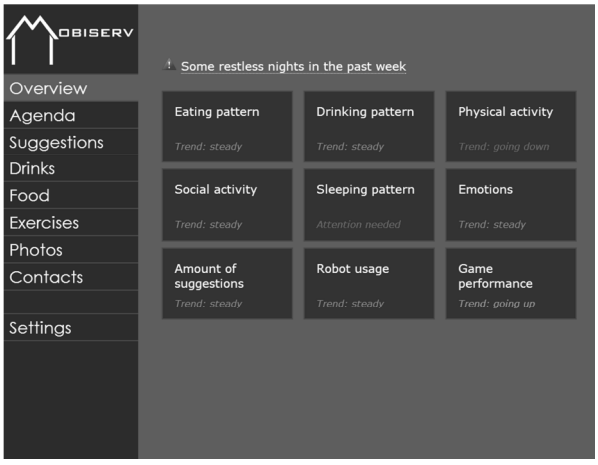
1. Giving an overview of how the person is doing, based on data collected by MOBISERV.
2. Personalizing, adjusting and updating the MOBISERV services.
3. Setting up and/or changing the system's basic settings.

5.1 Access and access control

The access for secondary users to the MOBISERV system and robot configuration and collected data is achieved via an Internet connection that is achieved through wireless LAN. In order to protect the stored data and robot behaviour the access control for the secondary user interface has been implemented by following the Role-Based Access Control (RBAC) paradigm. The access rights for modification of the various robot configuration files and reading different stored data are defined for different roles such as a relative, a friend, or a caretaker. Each secondary user is assigned for their corresponding role and then inherits the rights based on their role. Thus when new caretakers arrive they can be just assigned to their corresponding role rather than defining rights explicitly to all possible resources.

5.2 Getting an overview

Figure 7 shows the design of the main landing page of the secondary user interface, after being logged in through the RBAC login screen. This overview page gives a quick overview of all collected data, and highlights trends (in red or green) and things that need attention (at the top).



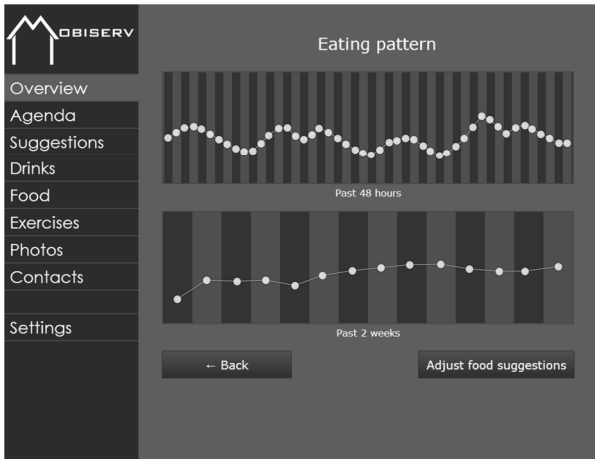


Figure 7: Main menu and overview section. Figure 8: Detailed overview of eating pattern.

When the (informal) carer clicks on the one of the squares, a more detailed visualisation of this specific data appears, as depicted in figure 8. Here the two graphs have appeared showing the user's eating pattern in the last 48 hours (top) and the last 2 weeks (bottom). In this graph, eating reminders will be shown, so the carer knows whether they have had a positive effect or not. At the bottom right, there is a button that leads to the eating suggestions, so the carer can immediately change or add these suggestions for the user.

5.3 Personalizing & Adjusting

In figure 9, the agenda design is shown per month. Per day, the carer can see whether there are appointments or todo-times for which the user will be reminded. When clicking on a day with events, an overview of these events is shown with edit options and with the option to add another event. When clicking on a day without events, the form for a new event will be shown directly.

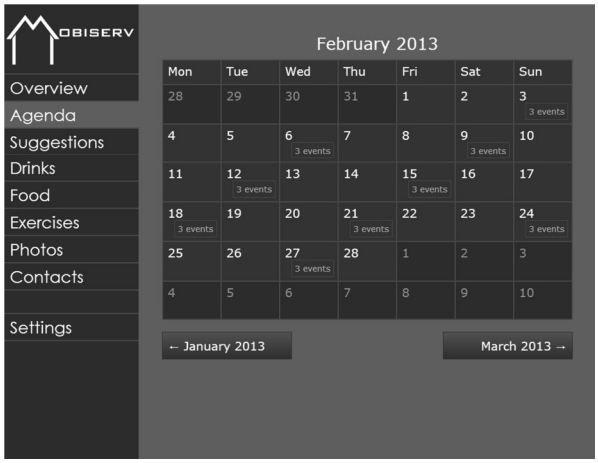


Figure 9: Agenda overview of the month

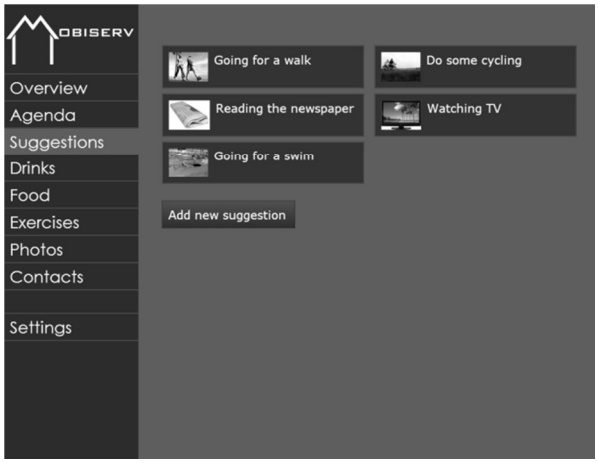


Figure 10: Overview of suggestions

In figure 10, an overview of the current general suggestion is shown. They do have some optional parameters such as 'social suggestion' or 'happy suggestion'. In general, these are suggestions that are not related to eating, drinking or exercising.

Figure 11 shows a specific drinking suggestion. Here the carer can add the description of the drink, the timeslots it may be given to the user, upload a picture, and set the normal and/or extra healthy parameter. Figure 12 shows the same screen, but now for a food suggestion. Difference here is that there are more timeslots available.

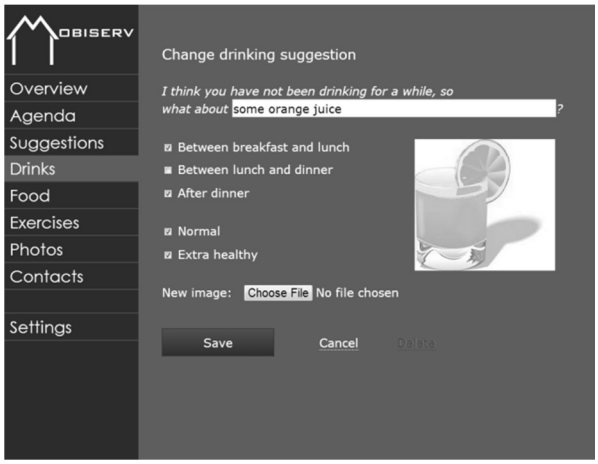


Figure 11: Changing one of the drinking suggestions

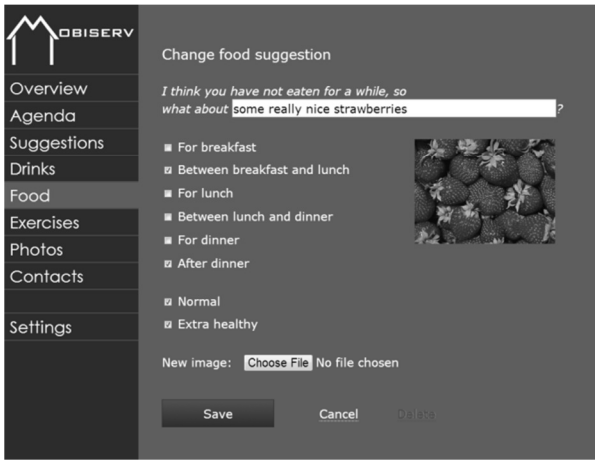


Figure 12: Changing one of the eating suggestions

In figure 13, a specific exercise is shown, which can be edited or deleted. The carer may change the title, the description, the suggested amount of time, and the picture/video.

Figure 14 shows an overview of the photos that are in the MOBISERV system. The carer can add more photos or delete existing ones. When adding a new photo, the carer can upload a photo and add a short title or description to it.

Figure 13: Changing one of the exercises

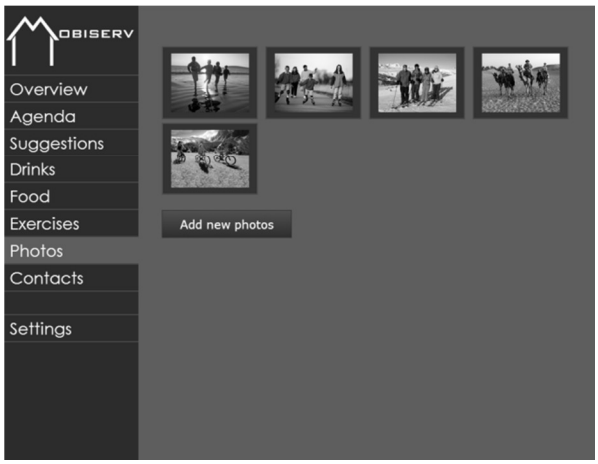


Figure 14: Overview of the photos

In figure 15, the contacts page design is shown. A carer can add or change contacts here. These are contacts that the user can call via Lync, but also carers that will be informed or called in case of emergencies.

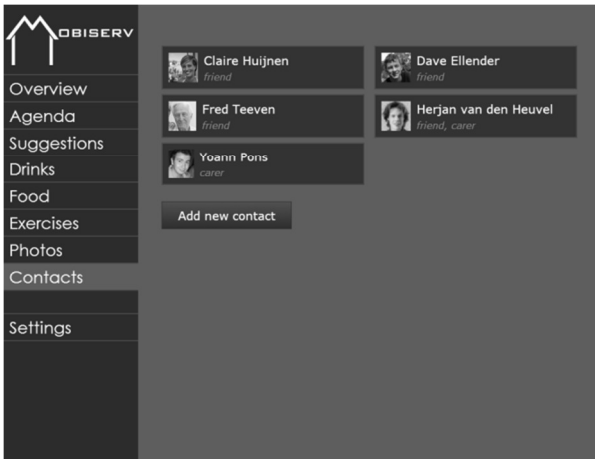


Figure 15: Overview of the user's contacts.

5.4 Changing Settings

Figure 16 shows the design of one of the settings screens, in which the carer should be able to configure the system and its behaviour, such as timing and thresholds before certain behaviour will be triggered. The name of the user and of the robot can be set here. Many other settings per function were foreseen but have not been implemented in the current prototype.

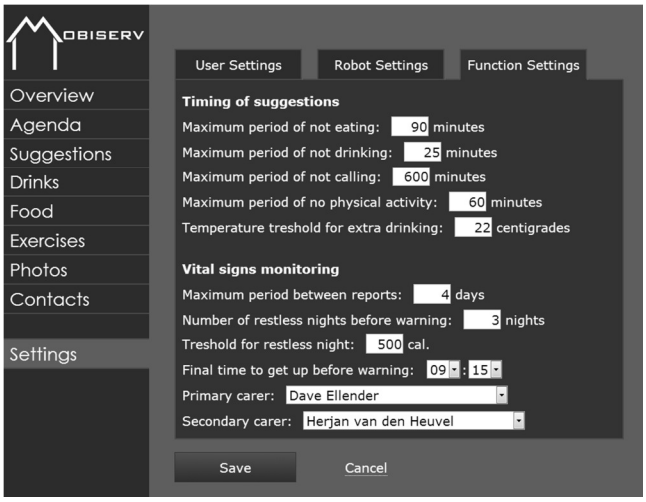


Figure 16: The settings tab.

6 Extended security analysis

This is an extension to the previous security analysis documented in deliverable D6.1. In this extension, the MOBISERV environment device components (in further parts of the document referred as assets) and the communications between them are analysed. As a result, the most risky devices and connections are detected. The goal here is to identify the devices that should be protected carefully, and the connections that should be secured.

The security in MOBISERV can be divided into two parts: physical security of the residence and the security of the user. Additionally, the privacy of the user is considered. The residence security has a major effect on it.

In section 6.1, the classification for risk, threats and effects are described along tasks definitions for the devices. In section 6.2, an overall summary of the threats is presented. The more detailed security analysis can be found in *Appendix 1: Security Analysis*.

6.1 Classifications

In order to create a risk classification for different parts of the system, the classification for different levels of risk must be defined. Here the classification for different risk levels and the criteria that was used to value assets and information are presented. Also the ways to determine likelihood for each threat is described. The connections that are presented here are analysed as going from the asset towards some other source. The abbreviations that are used in the analysis are described in this section.

The following section presents the threats and risks related to each asset (a device in the environment such as the Tablet PC or the Home Automation Control System) and to the connections that the asset makes to other assets. Each threat and connection is given a calculated risk value to show the potential weak spots in the environment regarding security and privacy of the user and the security of the residence.

Also the abstract tasks the assets fulfil are presented. These tasks are the basic operations the assets are executing.

6.1.1 Asset tasks

The different tasks the assets contain and execute, multiple tasks can be combined within one asset:

- Controller: Controls sources by either giving commands to them or maintaining the source
- Source: Provides information from surroundings, events or data stored on disk / permanent memory
- Reader: Reads data from a source
- Storer: Stores the data provided by sources for specified time period (temporary or permanent storage)
- Accesser: Accesses the data stored by Storer, read only access
- Processer: Processes the data stored by Storer, read and possibly write access

6.1.2 Effects on transmissions

The different effects on the data transmissions:

1. Captured: The transferred data is captured by the attacker.
2. Fabricated: Attacker is able to send fabricated data from the device or some other device masquerading as the actual device.
3. Intercepted: The transmission is interrupted by the attacker. It is done either at the device or on the transmission pathway.
4. Manipulated: Attacker is able to manipulate the transferred data on the device or on the transmission pathway.

When data transmission is captured, fabricated, intercepted or manipulated one or more of the following is the result:

5. Confidentiality **(C) - I**nadvertent or unauthorized disclosure of data
6. Integrity **(I) –** Inadvertent or unauthorized modification of data
7. Availability **(A)** – Making assets unavailable for authorized use

6.1.3 Classification for risks

The risk values are calculated for both connections and for each threat against the assets. In following sections these abbreviations are used:

- **LH** = Likelihood, how probable the attack is regarding the state of the environment (e.g. user actions are limited) and how ludicrous and beneficial the target is for the potential attacker.
- **S** = Severity, how severe the results of a successful attack would be towards the system integrity, information security and/or user safety.

6.1.3.1 Assets

The assets are labelled with MAJOR.MINOR type labelling system, where MAJOR is the bigger entity (in roman numerals) and MINOR is the actual device (with alphanumerical capital letter). For instance PRU is a major component where the database is a part of it, if PRU = I and database = B, then database is labelled as I.B.

The assets are valued with the same scale as others, from 1 to 6, where 6 is the highest value. Values are determined by

- how important data the asset contains (private or otherwise relevant to the whole environment)
- how long the asset stores the data
- would the malfunction/malicious usage of this asset endanger the health of the user
- would the malfunction/malicious usage of this asset endanger the security of the residence
- how important the asset is for the functionality of the environment

The likelihood of each threat is determined by the execution method, i.e. what is required that

the attack would succeed. User interaction in this environment is intended to be minimized and, therefore, it is not very likely that user error would make the attack succeed. Also the cost-effectiveness of the attack is taken into account, in other words; are the costs of the attack more than the value of an successful attack.

The severity of the threat is the numeric value on scale from 1 to 6 stating the level of harm the threat would pose towards privacy of the user and towards the security of the user, systems and residence.

6.1.3.2 Connections

All connections, as mentioned, are going from the asset towards some other device and labelling draws basis from the labelling of the assets. Each connection going from a certain asset is labelled as the asset itself with added connection id (as numeric value [1, n]), for example connections from database are labelled as I.B.1, I.B.2, etc.

Like the assets, the connections are also valued with the same scale. Values are determined by:

- How important data is transferred from privacy and security point of view, including the security of the residence.
- Would the manipulation/capture/interception of the data be any use for the attacker, i.e. would it be harmful towards the user.

Likelihood (same scale from 1 to 6) of the attacks on the connection between the two participants is determined by:

- What communication medium is used (wired connections are naturally harder to eavesdrop and intercept than wireless)
- What is the scope of the data (e.g. inside the residence network vs. Internet)
- Can the connection be considered secure by default (e.g. VPN connection)

The severity is determined separately for each effect (capture, fabrication, interception and manipulation) based on the harm each would result in towards the functionality of the systems, privacy of the user or security of the systems or residence.

6.1.3.3 Calculating the risk value

The risk value is calculated with following formula (1):

$$Value * \sum_{n=1}^{A} LH_n * S_n \quad (1)$$

The higher the value, the higher the risk. With connections that have risk rating of 5 or 6 encryption is mandatory. With connections that have risk rating of 3 or 4 encryption is strongly recommended. With assets that have risk rating of 5 or 6 the strong access protection must be implemented and it is necessary to keep the software and operating systems of these assets up to date. With assets that have a risk rating of 3 or 4, strong access protection is recommended and it is necessary to keep the software and operating systems of these assets up to date.

Severity scales are different for threats and connections because of different amount of variables in the connection. The scales are explained in following table 1.

Table 1: Risk value ratings and linking to severity and likelihood

Rating	Threat risk value	Connection risk value	Severity	Likelihood
6	180 - 216	600 - 720	Extreme	The attack is bound to happen.
5	144 - 179	480 - 599	Very High	The attack is very likely to happen.
4	108 - 143	360 - 479	High	There exists high risk of attack.
3	072 - 107	240 - 359	Medium	There exists a risk of an attack.
2	036 - 071	120 - 239	Low	The attack is not very probable.
1	001 - 035	001 - 119	Negligible	The attack will not happen.

6.2 Threat summary against assets and connections

The full analysis is in *Appendix 1: Security Analysis* which goes through every asset and connection in detail. Here a summary of the threats is presented. For assets the average of all of the risks is used.

The most risky assets were the I.B Database, I.D WWW interface and VIII. Lync (mainly for malware potential) and second highest risk values were calculated for II.A ORU, IV.A Control system and VI. Internet Access. The common denominator for all of these is related to the usage of the Internet, either directly or indirectly. Also the use of wireless techniques did affect to the risk value. In order to guarantee user's security and protect the privacy, these devices and access to them must be properly protected. Some initial guidelines are presented in Appendix I per asset.

One of the most risky connection groups are the connections over Internet to and from the devices that are not integral parts of the MOBISERV environment, like the home PC or carer's PC. Also the connections to and from the WWW interface were classified as the most risky ones since it enables access to private information. Every connection that exposes private data over Internet can be rated as high risk connections. In addition the alerts that are sent over Internet are considered as risky ones.

In general every communication that is done over wireless connections was assigned with a risk value that was much higher than the one the wired one was assigned. Wireless connections do bring ease of use with mobility etc., but not without risks. In cases where a wired alternative exists, providing more robust and reliable connectivity, it could be considered as a valuable option with the cost of mobility. However, when wireless techniques are used, proper encryption of the connections usually provides almost the same security as the wired one does. Wireless interference is another thing and must be accounted for. As it is not possible to prevent it, one can only adapt to it.

6.2.1 Assets

The summary of the risks for each asset are shown in table 2. The illustration of the architecture at the same level that was used in analysis is presented in Figure 17.

Table 2: Asset risk classification

Asset	Asset name	Risk value	Risk classification
I.A	Tablet PC	130	High
I.B	Database	198	Extreme
I.C	Web camera	1	Negligible
I.D	WWW interface	202	Extreme
II.A	ORU	144	Very High
II.B	Indoor camera	6	Negligible
II.C	WLAN Access Point	118	High
III.A	Sensors	99	Medium
III.B	Data logger	114	High
IV.A	Control System	150	Very High
IV.B	Media centre (optional)	90	Medium
IV.C	Door lock	6	Negligible
IV.D	Doorbell	5	Negligible
IV.E	Audio input	4	Negligible
IV.F	Audio output	4	Negligible
IV.G	Door camera	48	Low
V.A	Temperature sensor	50	Low
V.B	Motion sensor	5	Negligible
VI	Internet access	153	Very High
VII	User	1	Negligible
VIII	Lync servers & Lync super nodes	180	Extreme
IX	Gmail server	-	-
X	Home PC	108	High
XI	Work PC	108	High
XII	Control PC	132	High
XIII	Guest	1	Negligible

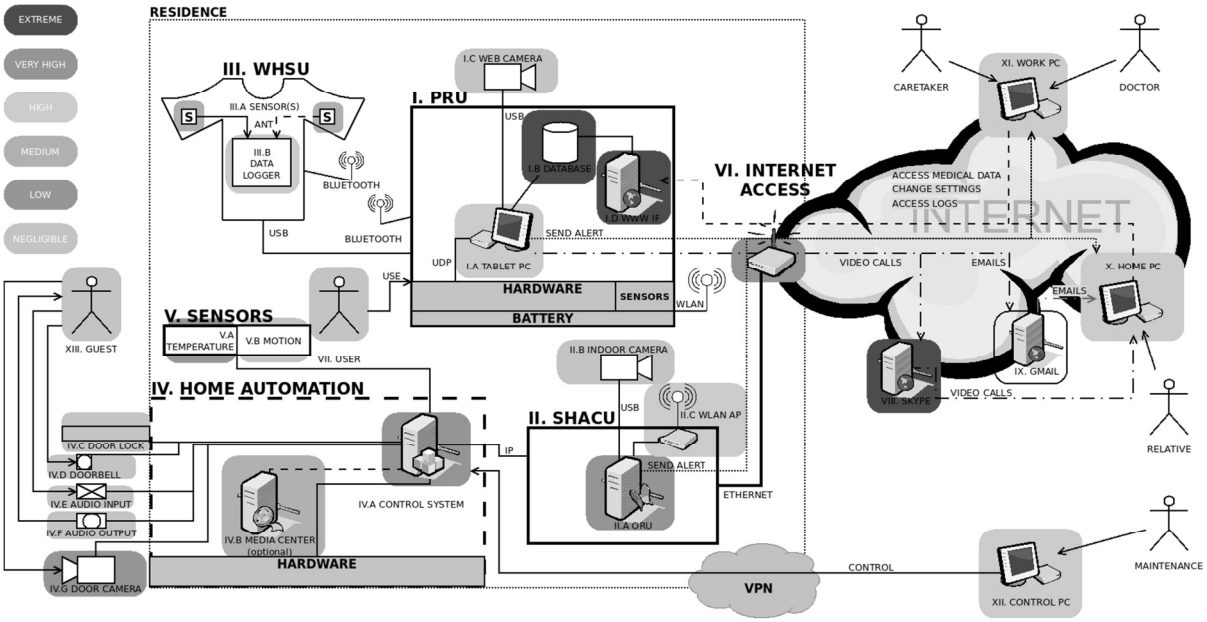


Figure 17: Overview of the architecture with asset risks

6.2.2 Connections

The risks for each and every connection are shown in table 3.

Table 3: Connection risks

Connection	Connection name	Risk value	Risk classification
I.A.1	Lync video	170	Low
I.A.2	Gmail	168	Low
I.A.3	Alerts to caretakers / relatives	510	Very High
I.A.4	Robot controls	102	Negligible
I.A.5	Health data to database	144	Low
I.A.6	Control system controls	306	Medium
I.A.7	Recorded audio to home automation	255	Medium
I.B.1	Health data to Tablet PC	126	Low
I.B.2	Personal data to Tablet PC	90	Negligible
I.B.3	Robot settings to Tablet PC	78	Negligible
I.B.4	Schedule to Tablet PC	80	Negligible
I.B.5	Health data to WWW interface	114	Negligible
I.B.6	Personal data to WWW interface	108	Negligible
I.B.7	Robot settings to WWW interface	84	Negligible
I.B.8	Schedule to WWW interface	84	Negligible
I.B.9	Log file data to WWW interface	108	Negligible

I.C.1	Video and audio feed to Tablet PC	84	Negligible
I.D.1	Robot settings to database	168	Low
I.D.2	Schedules to database	156	Low
I.D.3	Health data over Internet	684	Extreme
I.D.4	Personal data over Internet	684	Extreme
I.D.5	Logs over Internet	684	Extreme
I.D.6	Robot settings over Internet	360	High
I.D.7	Schedule over Internet	480	Very High
II.A.1	Alerts over Internet	720	Extreme
II.A.2	Detected actions to database	504	Very High
II.A.3	Camera control	108	Negligible
II.A.4	Control system controls	114	Negligible
II.B.1	Video and audio feed to ORU	144	Low
III.A.1	Sensor data to data logger	288	Medium
III.B.1	Logged data over USB	144	Low
III.B.2	Logged data over Bluetooth	576	Very High
IV.A.1	Status to SHACU	170	Low
IV.A.2	Status / diagnostic to control PC	255	Medium
IV.A.3	Media centre control	66	Negligible
IV.A.4	Home automation device controls	216	Medium
IV.A.5	Audio output to door	112	Negligible
IV.B.1	Media playback	72	Negligible
IV.B.2	Status information to control system	72	Negligible
IV.C.1	Status to control system	264	Medium
IV.D.1	Status to control system	140	Low
IV.E.1	Recorded audio from door	128	Low
IV.F.1	Recorded audio to door speaker	16	Negligible
IV.G.1	Video to control system	68	Negligible
V.A.1	Temperature readings to control system	65	Negligible
V.B.1	Motion events to control system	75	Negligible
VII.A.1	Speech to Tablet PC	7	Negligible
VII.A.2	Touchscreen actions on Tablet PC	4	Negligible
VIII.A.1	Initiation via super nodes	340	Medium
VIII.A.2	Relayed video / text via super nodes	320	Medium
IX.A.1	E-mails and contact information to Tablet	95	Negligible
X.A.1	Authentication credentials	540	Very High

X.A.2	Settings	570	Very High
X.A.3	Schedules	480	Very High
XI.A.1	Authentication credentials	450	High
XI.A.2	Settings	475	High
XI.A.3	Schedules	400	High
XII.A.1	Authentication credentials	180	Low
XII.A.2	Control commands	180	Low

Appendix 1: Security Analysis

1 PRU

The PRU is the physical robotic unit containing the main user interface to the systems of the residence. It provides assistance for the user as well as notifies about certain triggered events. The connectivity between other devices is happening via WLAN. Because the PRU is the main place for storing user information (personal information, analysed data and schedules) it should be properly protected from unauthorized access, not only because it can be connected directly from the Internet (WWW interface) but it is also very important part of user and residence security.

1.1 Tablet PC

Connection types: WLAN, Internet (WLAN), Message bus, Bluetooth (WHSU), USB

Tasks: Controller, Source, Reader, Storer, Accesser, Processer

Asset overall value: 6

Possible attacks:

Table 4:

Type	How is executed (LH)	Consequences (S)	Ways to prevent	Risk
Malware (Worm / Virus / Trojan)	User is sent an email containing a Trojan: Would require user interaction in order to infect. **(2)** Attacker uses target system vulnerabilities to infect it: would require that the system can be accessed from outside or if another device in the same network is used **(2)**	Data or private information gets stolen. Remote access is opened for malicious party. Traffic could be redirected through some other server. The privacy of the customer is threatened. **(6)** The integrity of the device is compromised (settings are changed, device does not work as it should or backdoor is opened for attacker). **(6)**	Scan emails for Trojans/viruses. Install latest software updates. Use a virus scanner with latest Trojan/virus database.	**144**
Wireless harassment	The frequencies are jammed or interference is created with specialized device. **(4)**	Device cannot communicate with other devices (e.g. cannot send commands to door) . Events sent by other devices (e.g. SHACU) cannot be processed. **(4)**	Interference in the wireless network should be monitored and when a threshold is reached an alarm could be raised. This would require manual inspection of residence surroundings.	**96**

1.1.1 Lync video

Communication medium: Internet (over WLAN)

Target of communication: VIII. Lync (super node / peer), X. Home PC

Data sent: Video, video call initialization, contact information request

Data scope: Internet

Table 5:

	Effect	**C**	**I**	**A**	**S**
Captured	Information about the residence is revealed (layout, contents). Private information of the user is revealed.	x			6
Fabricated	False connection information is provided resulting in connection to malicious user. False video or text is received.	x	x		5
Intercepted (lost)	No video is provided. Connections are not made to contacts. No contact information is received.			x	2
Manipulated	Connection is made to wrong person and the video is forwarded to wrong user.	x			4
Overall value					5
Attack likelihood					2
Risk classification					170

1.1.2 Gmail

Communication medium: Internet (over WLAN)

Target of communication: IX. Gmail server

Data sent: Emails, contact information request

Data scope: Internet

Table 6:

	Effect	**C**	**I**	**A**	**S**
Captured	Email content is revealed leaking possibly private information.	x			6
Fabricated	False emails are received with false content and/or false senders.	x			2
Intercepted (lost)	Emails are not sent to recipients. Contact information or cannot be retrieved. New emails are not retrieved.		x	x	2
Manipulated	Email sent to wrong persons. Email content is changed to possibly insulting.	x	x		4
Overall value					4
Attack likelihood					3
Risk classification					168

1.1.3 Alerts

Communication medium: Internet (over WLAN)

Target of communication: XI. Work PC and/or X. Home PC

Data sent: Health alerts

Data scope: Internet

Table 7:

	Effect	**C**	**I**	**A**	**S**
Captured	Alarm reasons are revealed to malicious parties.	x			4
Fabricated	False alarms are being sent.		x		3
Intercepted (lost)	Alarms are not received by the recipients.		x	x	6
Manipulated	Alarms are sent with false alarm reasons.		x		4
Overall value					6
Attack likelihood					5
Risk classification					510

1.1.4 Robot controls

Communication medium: Message bus

Target of communication: PRU Hardware

Data sent: Robot control commands

Data scope: Inside PRU

Table 8:

	Effect	**C**	**I**	**A**	**S**
Captured	Controls are revealed – no real value.				1
Fabricated	Robot starts or stops the action prematurely or starts running on its own.	x			5
Intercepted (lost)	Robot does not execute the requested actions.	x		x	6
Manipulated	Robot reacts incorrectly to commands or malfunctions.	x	x		5
Overall value					6
Attack likelihood					1
Risk classification					102

1.1.5 Health data

Communication medium: Message bus

Target of communication: I.B Database

Data sent: Health data retrieved from III. WHSU

Data scope: Inside PRU

Table 9:

	Effect	**C**	**I**	**A**	**S**
Captured	Status of the users health is revealed. Personal information is leaked.	x			6
Fabricated	False health data entries are stored to database (e.g. intercept and inject fabricated data) resulting in wrong treatments, medicine or exercises.		x		6
Intercepted (lost)	No health data is stored for the measuring period, potential health status changes go unnoticed.		x	x	6
Manipulated	Invalid health data (e.g. heart rate reading is increased) is stored to database resulting possibly wrong treatments, medicine or exercises.		x		6
Overall value					6
Attack likelihood					1
Risk classification					144

1.1.6 Control system controls

Communication medium: WLAN connection to SHACU that relays commands to AMX Home Automation via IP-based connection

Target of communication: IV.A Control System

Data sent: Control commands: door controls, residence lightning, residence temperature (optional: media centre controls)

Data scope: Inside residences communication environment

Table 10:

	Effect	**C**	**I**	**A**	**S**
Captured	Controls are revealed – no real value.				1
Fabricated	Controls are performed without user noticing them, e.g. door lock opened, lights go out when they should be on. This could compromise residence security.		x		6
Intercepted (lost)	Devices cannot get the request and are not performing actions as requested.			x	4
Manipulated	Controls are not executed as requested, e.g. door is kept open although lock is requested, which compromises residence security.	x	x		6
Overall value					6
Attack likelihood					3
Risk classification					306

1.1.7 Recorded audio

Communication medium: WLAN connection to SHACU that relays commands to AMX Home Automation via IP-based connection

Target of communication: IV.F Audio output

Data sent: Audio data

Data scope: Inside residences communication environment

Table 11:

	Effect	**C**	**I**	**A**	**S**
Captured	Reveals the partial conversation – the parts the user has sent to audio output.	x			3
Fabricated	Impersonation of the user, illogical responses to questions/arguments presented by the quest.	x			4
Intercepted (lost)	No audio is provided to the audio output – guest hears nothing.	x			4
Manipulated	Users response is distorted and might be hard to understand by the guest at the door or it might be modified to sound like the user is in need of medical assistance.	x	x		6
Overall value					5
Attack likelihood					3
Risk classification					255

1.2 Database

The database in PRU is the place for storing all data (personal data, log about user actions, etc.) and is accessed by other assets to gain access to the data. The database is not used directly by any device and the connections are going through some other device or interface. Still it must be carefully protected hence the personal information it stores.

Connection types: Message bus

Tasks: Storer (permanent)

Asset overall value: 6

Possible attacks:

Table 12:

Type	How is executed (LH)	Consequences (S)	Ways to prevent	Risk
Break-in	Attacker is able to exploit weaknesses in the WWW interface or weak login procedure and gains access to other devices in the network which are used to attack against the database. **(6)**	Attacker is able to read and write to database. **(6)**	Penetration testing for WWW interface. Use strong user authentication, prevent usage of weak passwords for login.	**216**
Backdoor access	Attacker uses backdoor on some other device opened by a malware to gain access to devices in the network. **(5)**	Attacker is able to read and write to database if the infected device has rights to access the database. **(6)**	Install latest software updates. Use a virus scanner with latest Trojan/virus database	**180**

1.2.1 Health data to Tablet PC

Communication medium: Message bus

Target of communication: I.A Tablet PC

Data sent: Requested health data

Data scope: Inside PRU

Table 13:

	Effect	**C**	**I**	**A**	**S**
Captured	The data requested for time period is revealed. Personal information is leaked.	x			6
Fabricated	False health data is provided for the Tablet PC resulting in possible false alarms.		x		5
Intercepted (lost)	No health data is provided for Tablet PC resulting in another request.			x	4
Manipulated	Altered health data is provided – it might be possible to hide event that should normally raise an alarm.		x		6
Overall value					6
Attack likelihood					1
Risk classification					126

1.2.2 Personal data to Tablet PC

Communication medium: Message bus

Target of communication: I.A Tablet PC

Data sent: Private personal information about user

Data scope: Inside PRU

Table 14:

	Effect	**C**	**I**	**A**	**S**
Captured	Requested personal information is revealed.	x			6
Fabricated	False information is provided to Tablet PC confusing the user.	x			5
Intercepted (lost)	No personal information is provided to Tablet PC resulting in another request.			x	1
Manipulated	Altered personal information is provided to Tablet PC confusing the user.	x			6
Overall value					5
Attack likelihood					1
Risk classification					90

1.2.3 Robot settings to Tablet PC

Communication medium: Message bus

Target of communication: I.A Tablet PC

Data sent: Robot settings

Data scope: Inside PRU

Table 15:

	Effect	**C**	**I**	**A**	**S**
Captured	Robot settings are revealed – no real value.				1
Fabricated	False robot settings are provided – changes made based on this data could result in robot malfunction or unexpected behavior.		x		5
Intercepted (lost)	No settings is provided for Tablet PC resulting in another request.			x	1
Manipulated	Manipulated settings are provided to Tablet PC – changes made based on this data could result in robot malfunction or unexpected behavior.		x		6
Overall value					6
Attack likelihood					1
Risk classification					78

1.2.4 Schedule to Tablet PC

Communication medium: Message bus

Target of communication: I.A Tablet PC

Data sent: User schedule

Data scope: Inside PRU

Table 16:

	Effect	**C**	**I**	**A**	**S**
Captured	The user schedule is revealed.	x			3
Fabricated	False schedule is provided which could contain arbitrary exercises which are introduced to the user.	x	x		6
Intercepted (lost)	No schedule data is provided to Tablet PC.			x	1
Manipulated	A schedule containing changed schedule times or types is provided to Tablet PC.	x	x		6
Overall value					5
Attack likelihood					1
Risk classification					80

1.2.5 Health data to WWW interface

Communication medium: Message bus

Target of communication: WWW interface

Data sent: Health data of the user

Data scope: Inside PRU

Table 17:

	Effect	**C**	**I**	**A**	**S**
Captured	The data requested for time period is revealed. Personal information is leaked.	x			6
Fabricated	False health data is provided for the WWW interface resulting in possible false diagnosis or medical prescriptions.		x		6
Intercepted (lost)	No health data is provided for WWW interface resulting in another request.			x	1
Manipulated	Altered health data is provided resulting in possible false diagnosis or medicines.		x		6
Overall value					6
Attack likelihood					1
Risk classification					114

1.2.6 Personal data to WWW interface

Communication medium: Message bus

Target of communication: WWW interface

Data sent: Personal information about user

Data scope: Inside PRU

Table 18:

	Effect	**C**	**I**	**A**	**S**
Captured	Requested personal information is revealed.	x			6
Fabricated	False information is provided to WWW interface.	x	x		5
Intercepted (lost)	No personal information is provided to WWW interface.			x	1
Manipulated	Altered personal information is provided to WWW interface.	x			6
Overall value					6
Attack likelihood					1
Risk classification					108

1.2.7 Robot settings to WWW interface

Communication medium: Message bus

Target of communication: WWW interface

Data sent: Robot settings

Data scope: Inside PRU

Table 19:

	Effect	**C**	**I**	**A**	**S**
Captured	Robot settings are revealed.	x			1
Fabricated	False robot settings are provided – changes made based on this data could result in robot malfunction or unexpected behavior.		x		6
Intercepted (lost)	No settings is provided for WWW interface.			x	1
Manipulated	Manipulated settings are provided to WWW interface – changes made based on this data could result in robot malfunction or unexpected behavior.		x		6
Overall value					6
Attack likelihood					1
Risk classification					84

1.2.8 Schedule to WWW interface

Communication medium: Message bus

Target of communication: WWW interface

Data sent: User schedule

Data scope: Inside PRU

Table 20:

	Effect	**C**	**I**	**A**	**S**
Captured	The user schedule is revealed.	x			3
Fabricated	False schedule is provided which could contain arbitrary exercises and changes to these based on this fabricated information might result in potentially harmful exercises.		x		5
Intercepted (lost)	No schedule data is provided to WWW interface.			x	1
Manipulated	A schedule containing changed schedule times or types is provided to WWW interface.	x	x		5
Overall value					6
Attack likelihood					1
Risk classification					84

1.2.9 Log file data to WWW interface

Communication medium: Message bus

Target of communication: WWW interface

Data sent: Log data

Data scope: Inside PRU

Table 21:

	Effect	**C**	**I**	**A**	**S**
Captured	All log data about user actions and health for the requested time period is revealed.	x			5
Fabricated	False log data is provided to WWW interface potentially resulting in unnecessary maintenance calls, wrong diagnosis or wrong medicines.		x		6
Intercepted (lost)	No log data is provided to WWW interface.			x	1
Manipulated	Altered log data is provided which might result in unnecessary maintenance calls, invalid diagnosis or wrong medicines.		x		6
Overall value					6
Attack likelihood					1
Risk classification					108

1.3 Web Camera

The web camera in PRU is a normal web camera device that is used mainly for Lync video calls. Usually triggered on only by the I.A Table PC.

Connection types: USB

Tasks: Source

Asset overall value: 4

Possible attacks:

Table 22:

Type	**How is executed (LH)**	**Consequences (S)**	**Ways to prevent**	**Risk**
-	**(1)**	**(1)**	-	**4**

1.3.1 Video and audio feed

Communication medium: USB

Target of communication: Tablet PC which forwards the data to, e.g. Lync.

Data sent: Video and audio data.

Data scope: Inside PRU & Internet when forwarded

Table 23:

	Effect	**C**	**I**	**A**	**S**
Captured	Video and audio feed is revealed. Would give detailed information about the contents of the residence.	x			6
Fabricated	Wrong video or audio is provided.	x	x		4
Intercepted (lost)	No video and/or audio is provided.			x	1
Manipulated	Distorted audio and/or grainy video is provided.	x			3
Overall value					6
Attack likelihood					1
Risk classification					84

1.4 WWW interface

The value of the WWW interface is extremely high as it is used to change settings of devices in the residence, albeit indirectly. Since it can be contacted directly from the Internet the likelihood of each threat is very high as well as attacks against communications to the database.

Connection types: Message bus, Internet (WLAN)

Tasks: Source, Storer, Accesser

Asset overall value: 6

Possible attacks:

Table 24:

Type	How is executed (LH)	Consequences (S)	Ways to prevent	Risk
DDOS	Multiple requests to WWW interface from multiple different machines. **(6)**	WWW interface becomes unresponsive (service unavailable) or the service crashes because of programming errors. **(4)**	Limit connections per connecting machine via internet and temporarily block ones that try to connect too many times. Use a firewall to limit access to the WWW interface only from known addresses.	**144**
Break-in	Use weaknesses in the server operating system or in the software or in the interface code to gain access to the device. **(6)**	Attacker can access the WWW interface and provide fabricated data to other users. Can be also used to access other devices in the network and, e.g.,. steal or manipulate health data. **(6)**	Penetration testing for the WWW interface. Use a firewall to limit access to WWW interface. Install latest software and operating system updates. Limit access to other parts of the network from the WWW interface with DMZ for instance.	**216**
SQL-injection	Attacker uses weaknesses in the WWW interface to conduct a SQL-injection attack. **(6)**	Attacker gains access to data that should not be available (read only access) – would threaten users privacy. **(6)**	Penetration testing for the WWW interface. Use a firewall to limit access to WWW interface.	**216**
Cross-Site Request Forgery	Attacker exploits potential weaknesses in the software by using a special embedded JavaScript on some website that authoritative user has visited/currently viewing to execute commands on web server when authorized user is logged in to the WWW interface. **(6)**	Remote code execution with root privileges. Leaking of all data that can be accessed via WWW interface **(6)**	Penetration testing for the WWW interface. Do not accept double cookies. Strict session control. Do not allow remote users to have administrative privileges to WWW interface.	**216**
Cross-Site Scripting	Attacker is able to echo specialized code into user's browser instance. **(6)**	Leaking of data that can be accessed via WWW interface. **(6)**	Penetration testing for the WWW interface.	**216**

In addition to the presented the threats related to used environment and languages for creating the functionality on the interface pose their own risks towards security and privacy. These specific threats must be evaluated separately. Some classification about threats towards Web Applications can be found at:

http://projects.webappsec.org/w/page/13246978/Threat%20Classification

1.4.1 Robot settings

Communication medium: Message bus

Target of communication: I.B Database

Data sent: Changed robot settings

Data scope: Inside PRU

Table 25:

	Effect	**C**	**I**	**A**	**S**
Captured	Robot settings are revealed – no real value.				1
Fabricated	False robot settings are stored to database resulting in illogical behavior of the robot.		x		6
Intercepted (lost)	No robot settings are stored to database.			x	1
Manipulated	Altered robot settings are stored to database resulting in illogical behavior of the robot.		x		6
Overall value					6
Attack likelihood					2
Risk classification					168

1.4.2 Schedules

Communication medium: Message bus

Target of communication: I.B Database

Data sent: Changed user schedule

Data scope: Inside PRU

Table 26:

	Effect	**C**	**I**	**A**	**S**
Captured	New schedule is revealed.	x			1
Fabricated	False schedule is stored resulting in potentially unnecessary exercises or no exercises at all.		x		5
Intercepted (lost)	New schedule is not stored.			x	2
Manipulated	Altered schedule is stored resulting in potentially unnecessary exercises.		x		5
Overall value					6
Attack likelihood					2
Risk classification					156

1.4.3 Health data

Communication medium: Internet (WLAN)

Target of communication: XI. Work PC / X. Home PC

Data sent: User health status data

Data scope: Internet

Table 27:

	Effect	**C**	**I**	**A**	**S**
Captured	User health status is revealed.	x			6
Fabricated	False health status is provided resulting in wrong diagnosis or medicines or wrong exercises.	x	x		6
Intercepted (lost)	No health status is provided. A re-request must be made when detected.			x	1
Manipulated	Altered health status is provided resulting in wrong diagnosis or medicines or wrong exercises.	x	x		6
Overall value					6
Attack likelihood					6
Risk classification					684

1.4.4 Personal data

Communication medium: Internet (WLAN)

Target of communication: XI. Work PC / X. Home PC

Data sent: Private personal information about user

Data scope: Internet

Table 28:

	Effect	**C**	**I**	**A**	**S**
Captured	Requested personal information is revealed.	x			6
Fabricated	False information is provided possibly causing a mix-up with some other person resulting in potentially wrong treatments or medicines.	x			6
Intercepted (lost)	No personal information is provided. A re-request must be made when detected.			x	1
Manipulated	Altered personal information is provided possibly causing a mix-up with some other person resulting in potentially wrong treatments or medicines.	x			6
Overall value					6
Attack likelihood					6
Risk classification					684

1.4.5 Logs

Communication medium: Internet (WLAN)

Target of communication: XI. Work PC / X. Home PC

Data sent: Log file data about user health status and activities

Data scope: Internet

Table 29:

	Effect	**C**	**I**	**A**	**S**
Captured	All log data about user actions and health for the requested time period is revealed.	x	x		6
Fabricated	False log data is provided to potentially resulting in unnecessary maintenance calls, wrong diagnosis or wrong medicines.		x		6
Intercepted (lost)	No log data is provided. A re-request must be made when detected.			x	1
Manipulated	Altered log data is provided which might result in unnecessary maintenance calls, invalid diagnosis or wrong medicines.		x		6
Overall value					6
Attack likelihood					6
Risk classification					684

1.4.6 Robot settings

Communication medium: Internet (WLAN)

Target of communication: XI. Work PC / X. Home PC

Data sent: Robot settings

Data scope: Internet

Table 30:

	Effect	**C**	**I**	**A**	**S**
Captured	Robot settings are revealed – no real value.				1
Fabricated	False robot settings are provided – changes made based on this data could result in robot malfunction or unexpected behavior.		x		5
Intercepted (lost)	No settings are provided. A re-request must be made when detected.			x	1
Manipulated	Manipulated settings are provided – changes made based on this data could result in robot malfunction or unexpected behavior.		x		5
Overall value					5
Attack likelihood					6
Risk classification					360

1.4.7 Schedule

Communication medium: Internet (WLAN)

Target of communication: XI. Work PC / X. Home PC

Data sent: User schedule

Data scope: Internet

Table 31:

	Effect	**C**	**I**	**A**	**S**
Captured	The user schedule is revealed.	x			5
Fabricated	False schedule is provided which could contain arbitrary exercises.		x		5
Intercepted (lost)	No schedule data is provided. A re-request must be made when detected.			x	1
Manipulated	A schedule containing changed schedule times or types is provided.		x		5
Overall value					5
Attack likelihood					6
Risk classification					480

2 SHACU

In current implementation SHACU is responsible of sharing the Internet connection over WLAN to other devices, mainly to PRU. SHACU also acts as a gateway for controlling the home automation as it is more permanent element in the residence with fixed power supply and should be on at all times. The nutrition detection is contained in SHACU and is done with the help of a video camera in the residence. The video itself is not stored into SHACU but the analysed and anonymised result of each detected action is. Breach in SHACU would reveal the activity of the user and private information would be leaked.

2.1 ORU

ORU is the computer responsible of pattern recognition duties in the residence, it detects nutrition, hydration, etc. actions from the provided video data and stores the results as anonymised data. The results are used for notifying the user about missed events. Also some alerts can be created based on the analysis results. Therefore, the ORU can be marked as a highly valuable asset for the user.

Connection types: Internet (Ethernet), WLAN, Ethernet

Tasks: Controller, Source, Reader, Storer, Accesser, Processer

Asset overall value: 6

Possible attacks:

Table 32:

Type	How is executed (LH)	Consequences (S)	Ways to prevent	Risk
Man in The Middle (MiTM)	Attacker is able to exploit weaknesses in the software or in the operating system to infect it with a malware of some sort to make changes into routing tables and DNS server configurations. **(4)**	The DNS requests and traffic might be routed through some other machine which either manipulates the traffic or steals important information. **(6)**	Install latest software and operating system updates. Use a virus scanner with latest databases to scan for changes in the system. Monitor / periodically update the routing table and DNS server settings and allow updates to these only from certain device or address.	**144**
Malware (Worm / Virus / Trojan)	User is sent an email containing a Trojan: Would require user interaction in order to infect. **(2)** Attacker uses target system vulnerabilities to infect it: would require that the system can be accessed from outside or if another device in the same network is used **(2)**	Data or private information gets stolen. Remote access is opened for malicious party. Traffic could be redirected through some other server. The privacy of the customer is threatened. **(6)** The integrity of the device is compromised (settings are changed, device does not work as it should or backdoor is opened for attacker). **(6)**	Scan emails for Trojans/viruses. Install latest software updates. Use a virus scanner with latest Trojan/virus database.	**144**

2.1.1 Alerts

Communication medium: Internet (WLAN)

Target of communication: XI. Work PC and/or X. Home PC

Data sent: Health alert regarding the users health status change that needs attention

Data scope: Internet

Table 33:

	Effect	**C**	**I**	**A**	**S**
Captured	The severity of the alert is revealed.	x			6
Fabricated	False alert is sent to recipients resulting in unnecessary house calls.	x			4
Intercepted (lost)	No health alert is delivered causing potentially bigger health issues.	x		x	6
Manipulated	The severity of the alert is changed to more or less severe causing either unnecessary house calls or potentially bigger health issues.		x		4
Overall value					6
Attack likelihood					6
Risk classification					720

2.1.2 Detected actions

Communication medium: WLAN

Target of communication: I.B Database

Data sent: Analysed data of user actions detected via anonymised video

Data scope: Inside residence

Table 34:

	Effect	**C**	**I**	**A**	**S**
Captured	The activity of the user is revealed in form of analyzed data which contains no identifiable information.	x			4
Fabricated	False activities are stored into the database – using this data for schedule changes would result in wrong types of exercises for the user.	x	x		6
Intercepted (lost)	No activity is stored into database.			x	5
Manipulated	Changed activities (types, repetitions, etc.) are stored – using this data for schedule changes would result in wrong types of exercises for the user.	x	x		6
Overall value					6
Attack likelihood					4
Risk classification					504

2.1.3 Camera control

Communication medium: USB

Target of communication: II.B Indoor camera

Data sent: Camera control commands

Data scope: Inside SHACU

Table 35:

	Effect	**C**	**I**	**A**	**S**
Captured	Camera controls are revealed – no real value.				1
Fabricated	Camera is rotating or panning into wrong areas or not focusing on the right target. Camera can also be shut down. Each results in invalid detection of nutrition, hydration, medicine intake and/or activities or no detection at all.	x	x		6
Intercepted (lost)	Camera controls are not sent.		x		5
Manipulated	Camera rotates into wrong way or stops following some actions prematurely which results in invalid detection of nutrition, hydration, medicine intake and/or activities or no detection at all.		x		6
Overall value					6
Attack likelihood					1
Risk classification					108

2.1.4 Control system controls

Communication medium: IP-based connection (Ethernet)

Target of communication: IV.A Control System

Data sent: Control commands: door controls, residence lightning, residence temperature (optional: media centre controls)

Data scope: Inside residence (wired only)

Table 36:

	Effect	**C**	**I**	**A**	**S**
Captured	Controls are revealed – no real value.				1
Fabricated	Controls are performed without user noticing them, e.g. door lock opened, lights go out when they should be on. This could compromise residence security.	x	x		6
Intercepted (lost)	Devices cannot get the request and are not performing actions as requested.	x		x	6
Manipulated	Controls are not executed as requested, e.g. door is kept open although lock is requested, which compromises residence security.	x	x		6
Overall value					6
Attack likelihood					1
Risk classification					114

2.2 Indoor camera

Indoor camera is the camera that is connected to the ORU for recording video about user events. Since it is a vital part in SHACU and ORU the asset value is the same as for ORU as it cannot function without the camera providing the video feed.

Connection types: USB

Tasks: Source

Asset overall value: 6

Possible attacks:

Table 37:

Type	**How is executed (LH)**	**Consequences (S)**	**Ways to prevent**	**Risk**
-	**(1)**	**(1)**	-	**6**

2.2.1 Video and audio feed

Communication medium: USB

Target of communication: II.A ORU

Data sent: Video and audio feed

Data scope: Inside SHACU (wired)

Table 38:

	Effect	**C**	**I**	**A**	**S**
Captured	Video and audio feed is revealed. Would give detailed information about the contents of the residence.	x			6
Fabricated	Wrong video or audio is provided. Results in invalid detection of nutrition, hydration, medicine intake and activity events.	x	x		6
Intercepted (lost)	No video and/or audio is provided. Nutrition, hydration, medicine intake and activity are not detected.		x	x	6
Manipulated	Distorted audio and/or grainy video is provided. Results in invalid detection of nutrition, hydration, medicine intake and activity events.	x	x		6
Overall value					6
Attack likelihood					1
Risk classification					144

2.3 WLAN Access Point

The WLAN Access Point (AP) resides in the SHACU and shares the Internet connection mainly to I. PRU. Being an essential part of the network in the residence the value is set to highest as most user functions (communications to database and outside world) depend on it.

Connection types: WLAN, Ethernet

Tasks:

Asset overall value: 6

Possible attacks:

Table 39:

Type	How is executed (LH)	Consequences (S)	Ways to prevent	Risk
Replace WLAN AP	Attacker is able to insert another WLAN AP into the vicinity of the residence that broadcasts much stronger signal (above legal limits but still within tolerable error rates for transmissions) with the same SSID but without encryption as the secret key for the real WLAN AP is not known by the attacker unless the used encryption is weak (e.g. WPA). **(5)**	PRU might connect to this WLAN network instead of the original one. This could happen after the PRU is restarted, ongoing connection might not be transferred to this bogus AP. The connection to bogus AP is possible only if the software on the PRU handling the WLAN connectivity does not take account whether the connected AP has the same encryption set as the previously connected one. Would result in capturing and possibly modifying of the data sent by PRU. **(6)**	-	**180**

3 WHSU

WHSU is the wearable health detection unit that is recording the user health status. The collected data is stored into the PRU using a wired connection and, therefore, it can be considered as secure. However, option for using Bluetooth exists and when used, proper precautions must be taken. The data the sensors of the WHSU collect is very valuable for the caretakers and doctors, and, of course indirectly to the user, too as health alarms are created based on the measurements. The connections between the logger and the sensors are happening via BAN and are not bound to eavesdropping or data manipulation but harassment (interception or transmissions) is possible.

3.1 Sensors

The sensors in the WHSU measure the heart rate, breathing rate, etc. of the user and provides this data for data logger and, therefore, is a very important asset.

Connection types: ANT Body Area Network

Tasks: Source

Asset overall value: 6

Possible attacks:

Table 40:

Type	How is executed (LH)	Consequences (S)	Ways to prevent	Risk
Interferenc e / DDOS	Attacker might be able to interfere with the connections between sensors and the data logger or with the sensors themselves by applying big amounts of radio wave interference into the vicinity of the WHSU. **(3)**	The sensors might give invalid readings, no readings at all or they cannot transfer the readings to the data logger. This might result in serious health issues if severe health status changes are missed. **(6)**	Monitor and report wireless interference in the residence. Proper reaction would be inspecting the residence manually for potential interference emitters.	**108**
Battery depletion	Attacker could use a frequency jammer device to interfere with the connections between sensors and data logger or the sensors themselves by transmitting arbitrary data on the same frequency as the devices are operating but with increased transmit power. **(3)**	Premature depletion of the sensor battery because of retransmissions and/or repeated measurements. **(5)**	Monitor and report wireless interference in the residence. Proper reaction would be inspecting the residence manually for potential interference emitters.	**90**

3.1.1 Sensor data

Communication medium: ANT Body Area Network

Target of communication: IV. B Data logger

Data sent: Measured sensor data (heart rate, breathing rate, etc.)

Data scope: In WHSU

Table 41:

	Effect	**C**	**I**	**A**	**S**
Captured	The status of users health is revealed.	x			6
Fabricated	False health data is sent to data logger causing risks towards users health.		x		6
Intercepted (lost)	No health data is sent – data from this period is completely lost. Might hide an oncoming serious health risk.		x	x	6
Manipulated	Altered health data is sent to the data logger. Some event might be made less or more severe which could be used to hide an event or to raise an false event.		x		6
Overall value					6
Attack likelihood					2
Risk classification					288

3.2 Data logger

Data logger is the initial storing place for sensor data in WHSU and has a limited amount of memory for the sensor data. As specification states, the memory is 2GB in size and lasts approximately for 9 days. It has the most recent data about users health that is purged into the database residing in PRU when plugged in by the user. Due to the sensitivity and importance of this information the value of this asset is extremely high.

Connection types: USB, Bluetooth

Tasks: Source, Reader, Storer, Accesser, Processer

Asset overall value: 6

Possible attacks:

Table 42:

Type	How is executed (LH)	Consequences (S)	Ways to prevent	Risk
Injection	The attacker might be able to use weaknesses in the protocol to inject fabricated data into the transmissions. **(3)**	Fabricated data stored in data logger might render all stored sensor data unusable or cause risks towards the users health if diagnosis is based on this fabricated data. By doing this it would be also possible to fill the database of data logger prematurely which might cause some events not to be stored hence the memory is full. **(6)**	Pairing of communicating devices, although devices with duplicate ids are hard to detect, therefore verification of authenticity is required. The transferred data must be always verified (the source and the data).	**108**
Battery depletion (Bluetooth only)	Attacker could use a frequency jammer device to interfere with the connections between sensors and data logger or the sensors themselves by transmitting arbitrary data on the same frequency as the devices are operating but with increased transmit power. **(4)**	Premature depletion of the data logger battery because of required retransmissions for data transfer. **(5)**	Monitor and report wireless interference in the residence. Proper reaction would be inspecting the residence manually for potential interference emitters.	**120**

3.2.1 Logged data over USB

Communication medium: USB

Target of communication: I PRU / I.A Tablet PC (forwards to I.B Database)

Data sent: Logged sensor data about users health status

Data scope: In WHSU

Table 43:

	Effect	**C**	**I**	**A**	**S**
Captured	The health status of the user is revealed.	x			6
Fabricated	False health status data is stored resulting in potentially false alarms, diagnosis and/or medicines.		x		6
Intercepted (lost)	No health data is sent. Serious health status changes are probably missed resulting in potential risks towards users health.		x	x	6
Manipulated	Manipulated data is saved which would result in false alarms, diagnosis, medicines and/or missed health status changes.		x		6
Overall value					6
Attack likelihood					1
Risk classification					144

3.2.2 Logged data over Bluetooth

Communication medium: Bluetooth

Target of communication: I PRU / I.A Tablet PC

Data sent: Logged sensor data about users health status

Data scope: In WHSU

Table 44:

	Effect	**C**	**I**	**A**	**S**
Captured	The health status of the user is revealed.	x			6
Fabricated	False health status data is stored resulting in potentially false alarms, diagnosis and/or medicines.		x		6
Intercepted (lost)	No health data is sent. Serious health status changes are probably missed resulting in potential risks towards users health.		x	x	6
Manipulated	Manipulated data is saved which would result in false alarms, diagnosis, medicines and/or missed health status changes.		x		6
Overall value					6
Attack likelihood					4
Risk classification					576

4 Home Automation

The home automation system in the residence is responsible of the controlling of the generic house devices (locks, lights, temperature, etc.) and is controlled by other devices in the residence. The connection is going via SHACU and the home automation is mainly used from the PRU by the user.

4.1 Control System

The most crucial part of the home automation is the control system which provides information about the status of the devices as well as functions as the interface for controlling the devices. The connection between control system and home automation devices is done over proprietary wired connections and controlling interface is accessed via WLAN provided by SHACU. Additionally a remote connection is provided for the maintenance of the home automation over VPN connection.

Connection types: IP/Ethernet, Ethernet → WLAN (via SHACU), IP via KNX-GW

Tasks: Controller, Source, Reader, Accesser, Processer

Asset overall value: 5

Possible attacks:

Table 45:

Type	How is executed (LH)	Consequences (S)	Ways to prevent	Risk
Malware (Worm / Virus / Trojan)	The attacker is able to use the Control PCs vulnerabilities to infect the Control System with a malware to allow unauthorized remote access to home automation. **(5)**	The door locks, lighting and residence temperature are in the hands of a malicious party. It is also possible to attack other devices in the network or to eavesdrop transferred data. **(6)**	The connections from Control System to outside should be restricted (allow only LAN and VPN/Extranet). Additionally the Control System should be periodically checked for changes in the software. The Control PC should be restricted from other use (and other networks) in order to prevent it from getting a virus / Trojan infection.	**150**

4.1.1 Status

Communication medium: Ethernet, Ethernet → WLAN via SHACU to PRU

Target of communication: II. SHACU (I. PRU)

Data sent: Home automation status data and event changes

Data scope: Inside residence

Table 46:

	Effect	**C**	**I**	**A**	**S**
Captured	The status of the home automation and sent events are revealed.	x			3
Fabricated	False status of the home automation is provided resulting in wrong reaction to requested commands or fabricated events are sent to recipients	x	x		6
Intercepted (lost)	No status data or event changes are delivered.		x	x	2
Manipulated	Invalid status of the home automation is provided resulting in wrong reaction to requested commands (e.g. report that door is unlocked although it is locked).	x	x		6
Overall value					5
Attack likelihood					2
Risk classification					170

4.1.2 Status / diagnostic

Communication medium: Extranet/VPN (via II. SHACU and VI. Internet access)

Target of communication: XII. Control PC

Data sent: Home automation status data and diagnostic information

Data scope: Internet / Extranet / VPN

Table 47:

	Effect	**C**	**I**	**A**	**S**
Captured	The status of home automation and diagnostic information is revealed.	x			3
Fabricated	False status or diagnostic information is provided resulting in wrong kind of adjustments or unnecessary maintenance calls.	x	x		6
Intercepted (lost)	No status or diagnostic information is provided.		x	x	2
Manipulated	Altered status or diagnostic information is provided resulting in wrong kind of adjustments or unnecessary maintenance calls.	x	x		6
Overall value					5
Attack likelihood					3
Risk classification					255

4.1.3 Media centre control

Communication medium: IP/Ethernet

Target of communication: IV.B Media centre

Data sent: Media centre control commands

Data scope: Inside home automation network

Table 48:

	Effect	**C**	**I**	**A**	**S**
Captured	Media center controls are revealed – no real value.				1
Fabricated	False control commands are sent resulting in playing of wrong media or increasing the playback volume to the max for instance.	x			4
Intercepted (lost)	The control commands are not sent to media center.			x	2
Manipulated	The media center plays wrong media or restarts playback instead of, e.g., pausing confusing the user as the controls seem to be malfunctioning.	x			4
Overall value					3
Attack likelihood					2
Risk classification					66

4.1.4 Home automation device controls

Communication medium: IP via KNX-GW

Target of communication: IV.C Door lock, IV.E Audio input, IV.G Door camera

Data sent: Control commands for various home automation devices (lock/unlock door, pan camera, record audio from door)

Data scope:

Table 49:

	Effect	**C**	**I**	**A**	**S**
Captured	Control actions are revealed.				1
Fabricated	The home automation devices get false commands without user interaction and the devices work in abnormal fashion (constant playback of audio from door, constant lock-unlock cycle of the door for instance).	x	x		6
Intercepted (lost)	The devices do not get the control commands and the controls seem to be unresponsive from the users point of view.			x	5
Manipulated	The reaction of home automation devices do not correspond to the control user has pressed hence the manipulation of data.	x			6
Overall value					6
Attack likelihood					2
Risk classification					216

4.1.5 Audio output to door

Communication medium: IP via KNX-GW

Target of communication: IV.F Audio output

Data sent: Playback audio recorded with I. PRU to door speaker

Data scope: Inside home automation

Table 50:

	Effect	**C**	**I**	**A**	**S**
Captured	The conversation from users part is revealed.	x			3
Fabricated	The recorded audio is swapped to fabricated audio which might confuse or irritate the guest at the door.	x	x		5
Intercepted (lost)	No audio is sent to door speaker.			x	1
Manipulated	The sent audio might sound distorted, delayed, etc.	x	x		5
Overall value					4
Attack likelihood					2
Risk classification					112

4.2 Media centre (optional)

The optional media centre is meant only for playback of media by users request. It also functions as media storage (videos, music, photos). As it is an optional feature it is not rated very high in asset value.

Connection types: Ethernet, Ethernet → WLAN via II. SHACU

Tasks: Source, Storage (permanent)

Asset overall value: 3

Possible attacks:

Table 51:

Type	How is executed (LH)	Consequences (S)	Ways to prevent	Risk
Malware (Worm / Virus / Trojan)	The attacker infects the media center by using a vulnerability in its software when playing videos or audio via Internet based services whose streams are infected with a malware. **(5)**	A backdoor might be opened for the attacker which can be utilized to attack other devices in the network. Alternatively the attacker can manipulate the operations of the media center. **(6)**	Install latest software updates for media center. Check periodically for changes in the software. Do not use streaming software that is not secure.	**90**

4.2.1 Media playback

Communication medium: Ethernet, Ethernet → WLAN via II. SHACU

Target of communication: II. SHACU / I. PRU

Data sent: Requested media (video, audio, picture)

Data scope: Inside residence

Table 52:

	Effect	C	I	A	S
Captured	Reveals what the user is watching or in long term has watched if large amounts of data is captured.	x			3
Fabricated	Arbitrary media is provided to user that might be insulting, disturbing or otherwise inappropriate.	x			4
Intercepted (lost)	No media is provided to user.			x	2
Manipulated	Wrong media is played or the played media contains audio distortion, video is grainy or pictures are manipulated.		x		3
Overall value					3
Attack likelihood					2
Risk classification					72

4.2.2 Status information

Communication medium: Ethernet

Target of communication: IV.A Control System

Data sent: Current status of the media centre

Data scope: Inside home automation

Table 53:

	Effect	**C**	**I**	**A**	**S**
Captured	Reveals the status of the media center.	x			2
Fabricated	False status is provided to Control system possibly resulting in invalid responses to requests made by the user.	x	x		4
Intercepted (lost)	No status information is provided to Control system and the status provided to user might not be updated resulting in wrong responses to some actions.	x		x	3
Manipulated	Manipulated status information is provided possibly resulting in invalid responses to requests made by the user.	x	x		3
Overall value					3
Attack likelihood					2
Risk classification					72

4.3 Door lock

The electronic lock at the front door is one of the highly valuated devices in the residence as most of the residences physical security relies on it. The controlling of the lock is in the hands of the user and done using the Tablet PC (via control system), however, there usually is also a manual override for the lock.

Connection types: IP via KNX-GW

Tasks: Source

Asset overall value: 6

Possible attacks:

Table 54:

Type	**How is executed (LH)**	**Consequences (S)**	**Ways to prevent**	**Risk**
-	**(1)**	**(1)**	-	**6**

4.3.1 Status

Communication medium: IP via KNX-GW

Target of communication: IV.A Control system

Data sent: Door lock status (locked / unlocked)

Data scope: Inside home automation

Table 55:

	Effect	**C**	**I**	**A**	**S**
Captured	Reveals whether the door is open or closed.	x			4
Fabricated	Wrong status reported to Control system resulting in wrong reaction to next lock / unlock request.		x		6
Intercepted (lost)	No status information is provided, the state on control system is not updated possibly resulting in wrong reaction to next lock / unlock request.		x	x	6
Manipulated	Wrong status reported to Control system resulting in wrong reaction to next lock / unlock request.	x	x		6
Overall value					6
Attack likelihood					2
Risk classification					264

4.4 Doorbell

The bell at the front door is an important indicator of the guest presence. All notifications are delivered to the control system which can provide this information to other devices, mainly to PRU.

Connection types: IP via KNX-GW

Tasks: Source

Asset overall value: 5

Possible attacks:

Table 56:

Type	**How is executed (LH)**	**Consequences (S)**	**Ways to prevent**	**Risk**
-	**(1)**	**(1)**	-	**6**

4.4.1 Status

Communication medium: IP via KNX-GW

Target of communication: IV.A Control system

Data sent: Doorbell event

Data scope: Inside home automation

Table 57:

	Effect	**C**	**I**	**A**	**S**
Captured	Reveals when the doorbell is ringing.	x			3
Fabricated	False event is provided which might unnecessary alert the user.	x			5
Intercepted (lost)	No doorbell event is provided resulting in missing visitor.		x		5
Manipulated	No real effect if devices can handle “empty” event.				1
Overall value					5
Attack likelihood					2
Risk classification					140

4.5 Audio input

Audio input is the microphone at the front door that is used for recording audio response from the person at the door. This response is delivered to the control system which forwards it to the PRU for the user to hear. It is not as important as the doorbell as notification from the door can be received without the microphone response and the video feed from the door will tell more about the person at the door than plain recorded voice.

Connection types: IP via KNX-GW

Tasks: Source

Asset overall value: 4

Possible attacks:

Table 58:

Type	**How is executed (LH)**	**Consequences (S)**	**Ways to prevent**	**Risk**
-	**(1)**	**(1)**	-	**4**

4.5.1 Recorded audio from door

Communication medium: IP via KNX-GW

Target of communication: IV.A Control system

Data sent: Audio recorded from door microphone

Data scope: Inside home automation

Table 59:

	Effect	**C**	**I**	**A**	**S**
Captured	The conversation from guests part is revealed.	x			3
Fabricated	The recorded audio is swapped to fabricated audio which might confuse or irritate the user.	x			5
Intercepted (lost)	No audio is sent.			x	3
Manipulated	The sent audio might sound distorted, delayed, etc.	x	x		5
Overall value					4
Attack likelihood					2
Risk classification					128

4.6 Audio output

Audio output is the speaker at the door that plays the response the user has recorded with the Tablet PC. The device itself is of medium/high value towards user privacy or residence security as it can just play the recording it is given. However, the value of this device is higher for the user.

Connection types: Analogue (audio)

Tasks: Accesser

Asset overall value: 4

Possible attacks:

Table 60:

Type	**How is executed (LH)**	**Consequences (S)**	**Ways to prevent**	**Risk**
-	**(1)**	**(1)**	-	**4**

4.6.1 Recorded audio to door speaker

Communication medium: Analogue (audio)

Target of communication: XIII. Guest

Data sent: The response user has recorded in waveform via speaker at the door

Data scope: Door area of the residence

Table 61:

	Effect	**C**	**I**	**A**	**S**
Captured	-				1
Fabricated	-				1
Intercepted (lost)	-				1
Manipulated	-				1
Overall value					4
Attack likelihood					1
Risk classification					16

4.7 Door camera

The camera at the front door is an important asset for the user but for his/her privacy and security of the residence the importance is not that high. This is because it is used as input only and is fairly hard/cumbersome to wiretap in order to provide false feed for the user.

Connection types: IP via KNX-GW

Tasks: Source

Asset overall value: 4

Possible attacks:

Table 62:

Type	**How is executed (LH)**	**Consequences (S)**	**Ways to prevent**	**Risk**
Wiretap	Attacker is able to physically wiretap the connection from door camera. **(2)**	The video feed from door can be changed to other, e.g. record a relative at the door and replace a video of some other person with the previously recorded one. As a result of this the user might open the door for unknown person. **(6)**	Put all wires inside wall so they cannot be physically accessed by any other than maintenance from inside the residence.	**48**

4.7.1 Video to control system

Communication medium: IP over KNX-GW

Target of communication: IV.A Control system

Data sent: Recorded video from door

Data scope: Inside home automation

Table 63:

	Effect	**C**	**I**	**A**	**S**
Captured	Reveals the person at the door.	x			1
Fabricated	False video feed is provided from the door and the user might open the door for unknown person if a video of a known person (e.g. relative) is provided.	x			6
Intercepted (lost)	No video is provided from the door. User cannot be sure who is at the door and might open the door based on audio response only.	x		x	5
Manipulated	Grainy or otherwise poor quality video is provided to user and it might be impossible to identify the person at the door.	x	x		5
Overall value					4
Attack likelihood					1
Risk classification					68

5 Sensors

The sensors in the residence are connected to home automation system and they provide state information about the residence, e.g. temperature and motion detected in certain parts of the residence.

5.1 Temperature sensor

The temperature sensor provides temperature readings from the residence and provides this data for thermostats in the home automation so the temperature of the residence can be regulated. The value for privacy and security is very low but the convenience of the user and potentially for the user health it has much larger effect, therefore, the asset value is very high.
Connection types: IP via KNX-GW
Tasks: Source
Asset overall value: 5
Possible attacks:

Table 64:

Type	How is executed (LH)	Consequences (S)	Ways to prevent	Risk
Harassment	Attacker is able to trick the sensor to get a reading that is bigger than the actual temperature. Requires physical access and can be done from within the residence only. **(2)**	The thermostats adjust themselves with false data resulting in too high or low temperatures in the residence. **(5)**	-	**50**

5.1.1 Temperature readings

Communication medium: IP via KNX-GW

Target of communication: IV.A Control system

Data sent: Temperature readings

Data scope: Within home automation, can be accessed only via IV.A Control system

Table 65:

	Effect	**C**	**I**	**A**	**S**
Captured	Reveals the residence temperature. No real value.				1
Fabricated	Thermostats are adjusted with false temperature readings.		x		4
Intercepted (lost)	No temperature measurements are provided. Thermostats are not adjusted.			x	4
Manipulated	Thermostats are adjusted with false temperature readings.		x		4
Overall value					5
Attack likelihood					1
Risk classification					65

5.2 Motion detection sensor

Motion detection sensors provide movement event detections for the home automation so the lighting in the residence can be controlled. Its value for the user safety is very high.

Connection types: IP via KNX-GW

Tasks: Source

Asset overall value: 5

Possible attacks:

Table 66:

Type	**How is executed (LH)**	**Consequences (S)**	**Ways to prevent**	**Risk**
-	**(1)**	**(1)**	-	**5**

5.2.1 Motion events

Communication medium: IP via KNX-GW

Target of communication: IV.A Control system

Data sent: Motion event

Data scope: Within home automation, no external access.

Table 67:

	Effect	**C**	**I**	**A**	**S**
Captured	Event is revealed – might give away the location of the user in the residence.	x			2
Fabricated	False event is provided and devices are triggered in wrong places.		x		4
Intercepted (lost)	No event is sent (e.g. lights stay off in certain places)			x	5
Manipulated	Event is altered and devices are triggered in wrong places.		x		4
Overall value					5
Attack likelihood					1
Risk classification					75

6 Internet access

The Internet access point handles all communication between the residence and outer world. The basic protection can be gained by using Network Address Translation (NAT) to hide the devices in the residence from outer world and to use port forwarding to the devices and their respective services which are required to be contacted by external sources (caretakers and relatives for instance).

The access to the device itself should be strictly restricted and all access from outside must be rejected, only maintenance access within residence (LAN) can be allowed. The access control mechanism that allows access to other devices in the residence is not required to handle the access to this device, it is necessary that the access is protected with a strong password known only by the maintenance. External maintenance should be accepted only via VPN.
Connection types: Ethernet, WAN (xDSL, 3G etc.)

Tasks:

Asset overall value: 6

Possible attacks:

Table 68:

Type	How is executed (LH)	Consequences (S)	Ways to prevent	Risk
MiTM	By using a vulnerability in the software of the router attacker could change the DNS server used by the router. **(5)**	All requests are redirected to malicious DNS server which could then forward the requesting computers to phishing sites for instance. **(6)**	Use only routers that have been verified to be secure against regular attacks.	**180**
DDoS	Attacker attempts to use the open access from outside to make the router crash; would require that access is open from Internet and the software has programming errors. **(3)** Attacker sends data from multiple computers to router in order to make it unresponsive **(5)**	The router reboots itself disconnecting all active connections. **(2)** The router is unable to send any data to Internet nor is it able to deliver any data sent by other devices in the Internet to devices in the residence. **(3)**	Do not allow direct access to router from Internet. Set connection limits into router or restrict connections to certain domains.	**126**

7 User

The end-user in the residence.
Connection types: Voice, Touchscreen
Tasks: Source
Asset overall value: 1
Possible attacks:

Table 69:

Type	How is executed (LH)	Consequences (SEV)	Ways to prevent	Risk
-	**(1)**	**(1)**	-	**1**

7.1 Speech

Communication medium: microphone

Target of communication: I.A Tablet PC

Data sent: Audio commands

Data scope: In the vicinity of the I. PRU

Table 70:

	Effect	C	I	A	S
Captured	Audio commands are revealed – no real value.				1
Fabricated	Impersonator imitates the user or recorded audio is provided resulting in execution of commands as if the user has said them.				4
Intercepted (lost)	-				1
Manipulated	-				1
Overall value					1
Attack likelihood					1
Risk classification					7

7.2 Touchscreen

Communication medium: Touchscreen

Target of communication: I.A Tablet PC

Data sent: User actions

Data scope: I. PRU

Table 71:

	Effect	**C**	**I**	**A**	**S**
Captured	User actions are revealed – no real value.				1
Fabricated	-				1
Intercepted (lost)	-				1
Manipulated	-				1
Overall value					1
Attack likelihood					1
Risk classification					4

8 Lync servers & Lync super nodes

Microsoft Lync system is used for audio / video calls to relatives. Could reveal lots of private information about the residence and the user health (video) and for this reason is rated as very highly valued asset.

Connection types: Internet

Tasks: Storer (account details), Accesser

Asset overall value: 5

Possible attacks:

Table 72:

Type	How is executed (LH)	Consequences (S)	Ways to prevent	Risk
Malware	User is provided a link in Lync conversation to a installable application that contains a malware (e.g. Trojan). **(6)**	Attacker can gain control of the devices in the residence via backdoor opened by the malware. **(6)**	Limit user permissions on the Tablet PC and disable the possibility to install new software. Hide/disable sending of files (or links) via Lync client.	**180**

8.1 Initiation via super nodes

Communication medium: Internet (UDP & TCP)

Target of communication: I.A Tablet PC / X. Home PC

Data sent: Lync signalling data (UDP) containing data for the key creation

Data scope: Internet (within Lync clients and super node)

Table 73:

	Effect	C	I	A	S
Captured	The data for connection key is revealed.		x		5
Fabricated	False data for key creation is sent resulting in incorrect connection establishment.	x			4
Intercepted (lost)	No signaling data is sent.			x	4
Manipulated	Wrong data for key creation is sent resulting in incorrect connection establishment.	x			4
Overall value					5
Attack likelihood					4
Risk classification					340

8.2 Relayed video / text via super nodes

Communication medium: Internet (UDP & TCP)

Target of communication: I.A Tablet PC / X. Home PC

Data sent: Relayed video and/or text if both targets are behind NAT/firewall

Data scope: Internet (within Lync clients and super node)

Table 74:

	Effect	**C**	**I**	**A**	**S**
Captured	Recorded video and/or text messages are revealed giving away information about the residence.	x			6
Fabricated	False video and/or text is provided to recipient(s) resulting in potentially invalid interpretations.	x			4
Intercepted (lost)	No video and/or text is provided.			x	2
Manipulated	Altered video (e.g. grainy, twisted or distorted audio) is provided to recipient(s) resulting in potentially invalid interpretations.	x	x		4
Overall value					5
Attack likelihood					4
Risk classification					320

9 Gmail server

The email server the user uses via Tablet PC. Contains private emails and contact information of other users (relatives, friends, etc.) and is very high in value for the user.

Connection types: Internet

Tasks: Source, Storage (permanent)

Asset overall value: 5

Possible attacks:

Table 75:

Type	How is executed (LH)	Consequences (S)	Ways to prevent	Risk
Regular attacks against Internet services	Beyond the scope of this analysis.	Beyond the scope of this analysis.	Beyond the scope of this analysis.	**0**

9.1 Emails and contact information

Communication medium: Internet

Target of communication: I.A Tablet PC

Data sent: Emails and contact information

Data scope: Internet

Table 76:

	Effect	C	I	A	S
Captured	Emails sent to the user are revealed along their contents. The contacts the user has are revealed.	x			5
Fabricated	False emails or contact information are provided.		x		5
Intercepted (lost)	No emails or contact information is sent resulting in another request.			x	4
Manipulated	The content of the email is changed or addresses of contacts are changed.	x	x		5
Overall value					5
Attack likelihood					1
Risk classification					95

10 Home PC

The home computer is the device residing at the residence of the relatives that is used to change schedules and for contacting the user. The value is medium as it is not an integral part of the environment and cannot be controlled in any way by the user or the maintenance staff. Home computer is used mainly for accessing the WWW interface in the PRU and has no other direct access to the devices.

Connection types: Internet

Tasks: Controller, Source, Reader, Accesser

Asset overall value: 3

Possible attacks:

Table 77:

Type	How is executed (LH)	Consequences (S)	Ways to prevent	Risk
Malware (Worm / Virus / Trojan)	A malware is used to infect the home computer via system vulnerability. The home computer is infected because of the actions of the computer user(s), e.g. opening an email containing virus/Trojan, using an old operating system etc. **(6)**	Attacker is able to gain access to the home computer and also is able to access the data sent to I.D WWW interface and also manipulate the data that is received. **(6)**	Scan emails for Trojans/viruses. Install latest software updates. Use a virus scanner with latest Trojan/virus database.	**108**
MiTM	Attacker is able to use vulnerabilities in the home computer or in the home computer network to forward the computers to malicious DNS server. **(6)**	The computer is redirected to some phishing site which steals user credentials to system. **(6)**		**108**

10.1 Login credentials

Communication medium: Internet

Target of communication: I.D WWW interface

Data sent: Relative login credentials

Data scope: Internet (Home PC and WWW interface)

Table 78:

	Effect	**C**	**I**	**A**	**S**
Captured	Login credentials are revealed making it possible for the attacker to use them to access the system and attempt to exploit weaknesses in the server which require authenticated access.	x	x		6
Fabricated	Authentication fails.			x	3
Intercepted (lost)	Authentication fails.			x	3
Manipulated	Authentication fails.			x	3
Overall value					6
Attack likelihood					6
Risk classification					540

10.2 Settings

Communication medium: Internet

Target of communication: I.D WWW interface

Data sent: Changed robot settings that the WWW interface provides

Data scope: Internet (Home PC and WWW interface)

Table 79:

	Effect	**C**	**I**	**A**	**S**
Captured	The settings are revealed.	x			3
Fabricated	False settings are provided to WWW interface resulting in saving of wrong settings for PRU.		x		6
Intercepted (lost)	No settings data is provided to WWW interface – the settings are not changed.			x	4
Manipulated	Altered settings data is provided to WWW interface resulting in saving of potentially harmful setup for PRU.	x	x		6
Overall value					5
Attack likelihood					6
Risk classification					570

10.3 Schedules

Communication medium: Internet

Target of communication: I.D WWW interface

Data sent: Changed schedule for the user that was provided by the WWW interface

Data scope: Internet (Home PC and WWW interface)

Table 80:

	Effect	**C**	**I**	**A**	**S**
Captured	Schedule set for the user is revealed.	x			3
Fabricated	False schedule is set for the user resulting in unnecessary exercises for instance.	x			5
Intercepted (lost)	No schedule is set for the user or old one is not changed.			x	3
Manipulated	Schedule containing invalid or removed events is saved for the user which might be unnecessary or necessary events are removed.		x		5
Overall value					5
Attack likelihood					6
Risk classification					480

11 Work PC / Tablet

The work computer or tablet is used by the caretakers and the doctors for checking the health status of the user and also for changing the settings of the PRU and maintaining the schedule. The work computer connects mainly to the WWW interface but can also receive alert messages from within the residence and, therefore, the value is higher than the one of the home computer. Also because the work computer can be controlled and monitored more closely. The access from this computer with the higher authority credentials can also open more data and control for the caretaker/doctor.

Connection types:

Tasks:

Asset overall value: 4

Possible attacks:

Table 81:

Type	How is executed (LH)	Consequences (S)	Ways to prevent	Risk
Malware (Worm / Virus / Trojan)	A malware is used to infect the work computer via system vulnerability. Or the work computer is infected because of the actions of the computer user(s), e.g. opening an email containing virus/Trojan etc. **(5)**	Attacker is able to gain access to the home computer and also is able to access the data sent to I.D WWW interface and also manipulate the data that is received. **(6)**	Scan emails for Trojans/viruses. Install latest software updates. Use a virus scanner with latest Trojan/virus database.	**120**
MiTM	Attacker is able to use vulnerabilities in the work computer or in the workplace network to forward the computers to malicious DNS server. **(4)**	The computer is redirected to some phishing site which steals user credentials to system. **(6)**		**96**

11.1 Login credentials

Communication medium: Internet

Target of communication: I.D WWW Interface

Data sent: Caretaker / doctor login credentials

Data scope: Internet (between work PC and WWW interface)

Table 82:

	Effect	**C**	**I**	**A**	**S**
Captured	Login credentials are revealed making it possible for the attacker to use them to access the system and attempt to exploit weaknesses in the server which require authenticated access.		x		6
Fabricated	Authentication fails.			x	3
Intercepted (lost)	Authentication fails.			x	3
Manipulated	Authentication fails.			x	3
Overall value					6
Attack likelihood					5
Risk classification					450

11.2 Settings

Communication medium: Internet

Target of communication: I.D WWW Interface

Data sent: Changed robot settings that the WWW interface provides

Data scope: Internet (between work PC and WWW interface)

Table 83:

	Effect	**C**	**I**	**A**	**S**
Captured	The settings are revealed.	x			3
Fabricated	False settings are provided to WWW interface resulting in saving of wrong settings for PRU.		x		6
Intercepted (lost)	No settings data is provided to WWW interface – the settings are not changed.			x	4
Manipulated	Altered settings data is provided to WWW interface resulting in saving of potentially harmful setup for PRU.		x		6
Overall value					5
Attack likelihood					5
Risk classification					475

11.3 Schedules

Communication medium: Internet

Target of communication: I.D WWW Interface

Data sent: New or changed user schedule data

Data scope: Internet (between work PC and WWW interface)

Table 84:

	Effect	**C**	**I**	**A**	**S**
Captured	Schedule set for the user is revealed.	x			3
Fabricated	False schedule is set for the user resulting in unnecessary exercises for instance.	x			5
Intercepted (lost)	No schedule is set for the user or old one is not changed.			x	3
Manipulated	Schedule containing invalid or removed events is saved for the user which might be unnecessary or necessary events are removed.		x		5
Overall value					5
Attack likelihood					5
Risk classification					400

12 Control PC

The control computer of the home automation is the device used by maintenance personnel for doing remote maintenance on the home automation system. It has a high value as it has access to the controls of the residence security.

Connection types: VPN/Extranet over Internet

Tasks: Controller, Reader, Accesser

Asset overall value: 4

Possible attacks:

Table 85:

Type	How is executed (LH)	Consequences (S)	Ways to prevent	Risk
Malware	The control PC is infected with a malware as a result of user carelessness or a system vulnerability. **(5)**	The malware either provides the attacker an access to the system, steals data from the system or allows the attacker to manipulate sent and received data. As a result the residence security can be compromised. **(6)**	Apply latest software updates to control PC and use a virus scanner with latest databases (if applicable).	**120**
Phishing	The maintenance personnel is lured to a phishing site either in an email or the systems DNS settings are altered by some malware. **(6)**	The authentication credentials used to access the home automation are revealed. **(6)**	Restrict the access to home automation from authorized computers only, e.g. from IP addresses of a certain company. Make the control software to detect connections to fraudulent sites. Instruct personnel about potential phishing attacks and report when the activity is high.	**144**

12.1 Authentication credentials

Communication medium: VPN/Extranet over Internet

Target of communication: IV.A Control system

Data sent: Control system authentication credentials

Data scope: In secure channel over Internet

Table 86:

	Effect	**C**	**I**	**A**	**S**
Captured	Authentication credentials are revealed and the attacker can control the home automation.	x	x		6
Fabricated	Authentication fails.			x	3
Intercepted (lost)	Authentication fails.			x	3
Manipulated	Authentication fails.			x	3
Overall value					6
Attack likelihood					2
Risk classification					180

12.2 Control commands

Communication medium: VPN/Extranet over Internet

Target of communication: IV.A Control system

Data sent: Control and diagnostic commands

Data scope: In secure channel over Internet

Table 87:

	Effect	**C**	**I**	**A**	**S**
Captured	Controls are revealed – no real use.				1
Fabricated	False device controls are sent resulting in arbitrary device reactions that could compromise the residence security (door lock).	x	x		6
Intercepted (lost)	No controls are delivered and e.g. the door can remain unlocked if locking was requested.		x		5
Manipulated	The controlled devices do not respond as they should resulting in compromising the residence security or invalid diagnostic of the home automation.	x	x		6
Overall value					5
Attack likelihood					2
Risk classification					180

13 Guest

The guest at the door. Can only give information about him/herself (video, audio, presence).

Connection types:

Tasks: Source

Asset overall value: 1

Possible attacks:

Table 88:

Type	How is executed (LH)	Consequences (S)	Ways to prevent	Risk
-	**(1)**	**(1)**	-	**1**

13.1 Connection

Communication medium:

Target of communication:

Data sent:

Data scope:

Table 89:

	Effect	C	I	A	S
Captured					1
Fabricated					1
Intercepted (lost)					1
Manipulated					1
Overall value					1
Attack likelihood					1
Risk classification					4