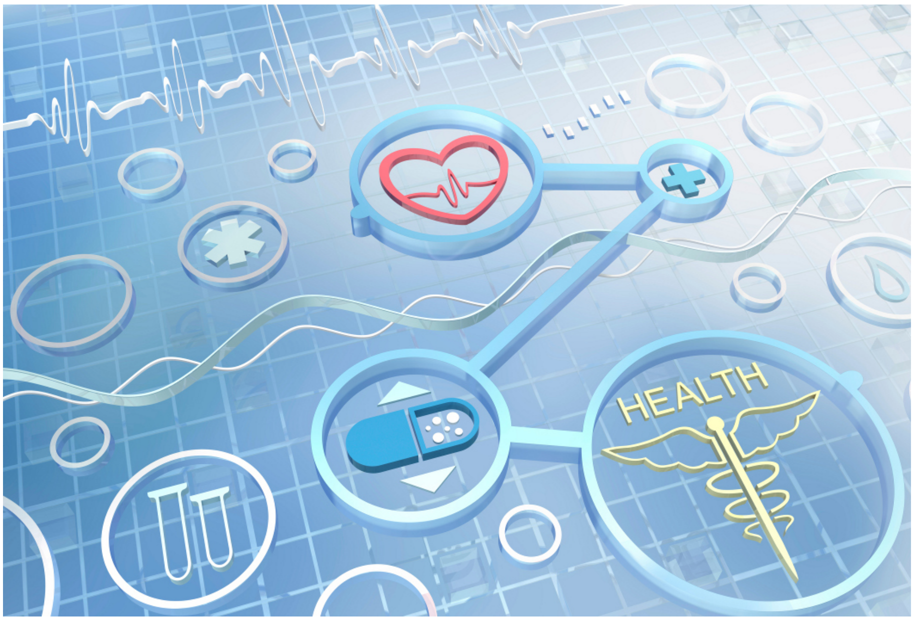
Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Note

Defining the ASSET Scenarios

ASSET D6.1 Technical Note: Case study scenarios definition Version 1



Note no	DART/17/12
Authors	Wolfgang Leister Habtamu Abie Stefan Poslad
Date	December 2012

The authors

Wolfgang Leister, assisting research director at Norsk Regnesentral, received the Dr. rer. nat. degree in 1991 from the Universität Karlsruhe, Germany. His research interests cover smart information systems, multimedia, computer graphics, computer and sensor networks, health care applications, mobile systems, and free software.

Habtamu Abie is currently a Senior Research Scientist at NR. He received his B.Sc., M.Sc. and Ph.D. from the University of Oslo, and has many years of experience in computing, both as practitioner and researcher. He has a solid and extensive background in the design and development of real-time systems, and the design, modeling and development of security for distributed object computing systems.

Stefan Poslad, PhD, is an academic member of SEECS Interactive Media & Communication (IMC) Research Group at Queen Mary University of London. He received his B.Sc. in physics from the University of Southhampton, the M.Sc. in medical physics and IT from the University of Aberdeen, and a PhD from the University of Newcastle upon Tyne. His research focus is on ubiquitous computing, also referred to as Pervasive Computing. Ambient intelligence and more recently as the Internet of Things.

Frontpage image: © Alexandr Mitiuc, image 108682181 at photos.com.

Norwegian Computing Center

Norsk Regnesentral (Norwegian Computing Center, NR) is a private, independent, nonprofit foundation established in 1952. NR carries out contract research and development projects in the areas of information and communication technology and applied statistical modeling. The clients are a broad range of industrial, commercial and public service organizations in the national as well as the international market. Our scientific and technical capabilities are further developed in co-operation with The Research Council of Norway and key customers. The results of our projects may take the form of reports, software, prototypes, and short courses. A proof of the confidence and appreciation our clients have for us is given by the fact that most of our new contracts are signed with previous customers.

Norsk Regnesentral
Norwegian Computing Center
Postboks 114, Blindern
NO-0314 Oslo, Norway

Besøksadresse
Office address
Gaustadalléen 23
NO-0373 Oslo, Norway

Telefon · telephone
(+47) 22 85 25 00
Telefaks · telefax
(+47) 22 69 76 60

Internett · internet
www.nr.no
E-post · e-mail
nr@nr.no

Title	**Defining the ASSET Scenarios** **ASSET D6.1 Technical Note:** **Case study scenarios definition – Version 1**
Authors	**Wolfgang Leister, Habtamu Abie, Stefan Poslad**
Quality assurance	Trenton Schulz
Date	December 2012
Publication number	DART/17/12

Abstract

This research note defines the scenarios for the research on adaptive security to be used for the Internet of Things in healthcare systems. We start by extending previously defined generic models. Based on these, we develop a home scenario for patients with chronic diseases using biomedical sensors, and a hospital scenario including examination, surgery, pre- and post-operative procedures. These elements are then used to create two storylines: (*a*) a chronic patient living at home; and (*b*) a hospital patient undergoing surgery and recovery.

Keywords	ASSET, scenarios, home scenario, hospital scenario, Internet of Things, healthcare
Target group	Participants
Availability	Open
Project	ASSET
Project number	320485 (NFR 213131/070)
Research field	Internet of Things, Security
Number of pages	17
© Copyright	Norwegian Computing Center

Contents

1 Introduction

The ASSET project will research and develop risk-based adaptive security methods and mechanisms for Internet of Things (IoT) that will estimate and predict risk and future benefits using game theory and context awareness. The security methods and mechanisms will adapt their security decisions based upon those estimates and predictions.

The main application area of ASSET is health and welfare. Health organisations may deploy IoT-based services to enhance traditional medical services and reduce delay for treatment of critical patients. ASSET's case study will lead to a simulation experiment in the following manner at the test-bed that belongs to the Oslo University Hospital: Blood pressure, electrocardiogram (ECG) and heart rate values will be gathered from patients, where the patient ID will be removed and the sensor data made anonymous. The sensor data will be stored in different biomedical sensor nodes that are capable of communicating with any of the following connectivity options available: ZigBee, Wi-Fi, 3G, GPRS, Bluetooth, and 802.15.4. A smartphone, for instance, with a ZigBee-transceiver will act as an access point that communicates with both ZigBee sensor nodes and a Medical Centre.

We will study two different scenarios, one in a home environment and the other in a hospital environment, where different Quality of Service (QoS) metrics and adaptive security methods and mechanisms will be analysed using game theory and context awareness.

The selection of the scenarios for ASSET will be motivated from previous experiences in projects like *Credo* (Balasingham et al., 2007) and *SAMPOS* (Leister et al., 2011). This document is also based on the work by Savola et al. (2012) and Abie and Balasingham (2012). In Section 2, we will extend the previously developed Generic System Model (Leister et al., 2011). Section 3 defines the structure of the scenarios. In Section 4, we present two story-lines for the home and hospital scenario.

2 Generic System Models for the eHealth Scenarios

Patient monitoring systems are a major data source in healthcare environments. In welfare technology monitoring systems for citizens, e.g., in a training environment, are increasingly used. It is important that these monitoring systems maintain a certain level of availability, QoS, and that they are secure and protect the privacy of the patient.

Previously, we have analysed the security and privacy for patient monitoring systems with an emphasis on wireless sensor networks (Leister et al., 2009) and suggested a framework for providing privacy, security, adaptation and QoS in patient monitoring systems (Leister et al., 2011). In this work, patient monitoring systems are divided into four generic levels (GLs): (0) the patient; (I) the personal sensor network; (II) devices in the closer environment following several scenarios; and (III) the healthcare information system. In Section 2.3, we will extend this model by one more generic level for inter-healthcare enterprise communication.

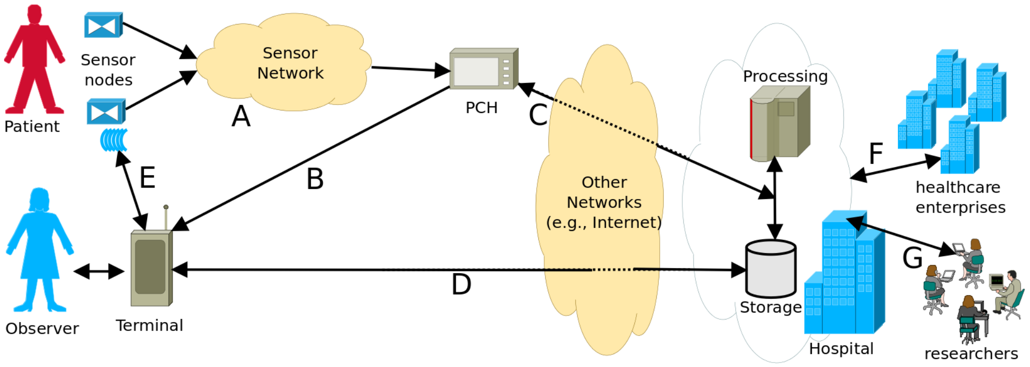


Figure 1. Generic System Model.

2.1 The Generic System Model

In a more concrete model, entities and communication channels in a patient monitoring system are characterised. We show the communication Channel A for the personal sensor network, Channels B, C, and D for information channels in the other levels in Figure 1. We extended this model with Channel E for communication with NFC technology, Channel F for inter-hospital communication, and Channel G for communication to (medical) researchers. In a practical deployment, biomedical sensors in Channel A are (possibly wirelessly) connected to a bedside patient cluster head (PCH) acting as a patient data collector, which in turn is connected to the hospital infrastructure or directly to a terminal enabled to access medical digital items allowing medical personnel or the patient to access the patient data. When actuators are used, and for the purpose of configuring sensor nodes, the communication channel can be two-ways.

The model in Figure 1 is designed to be applied to a variety of scenarios, for which the characteristics of the channels and devices, as well as the concrete technologies and implementations need to be defined.

2.2 Biomedical Sensor Networks

Channel A, which implements a (wireless) BSN in the Generic System Model, is of particular interest. The other channels and entities define the environment settings. In many cases, a wireless sensor network (WSN) is used to implement Channel A. A WSN consists of spatially distributed autonomous devices using sensors to cooperatively monitor physical, environmental or biomedical conditions, such as temperature, sound, vibration, pressure, motion, pollutants or biomedical signals at different locations. Biomedical sensors are used to monitor parameters such as blood gas, blood pressure, pulse rate, temperature, ECG, and electroencephalogram (EEG). For more information about biomedical sensor networks in patient monitoring systems, we refer to the work by Leister et al. (2011) and Abie and Balasingham (2012).

2.3 Extending the Generic Levels

We extend the generic level-model presented by Leister et al. (2011) by the levels (IIf), (IVa) and (IVb). The work by Savola et al. (2012) requires such an extension of the generic

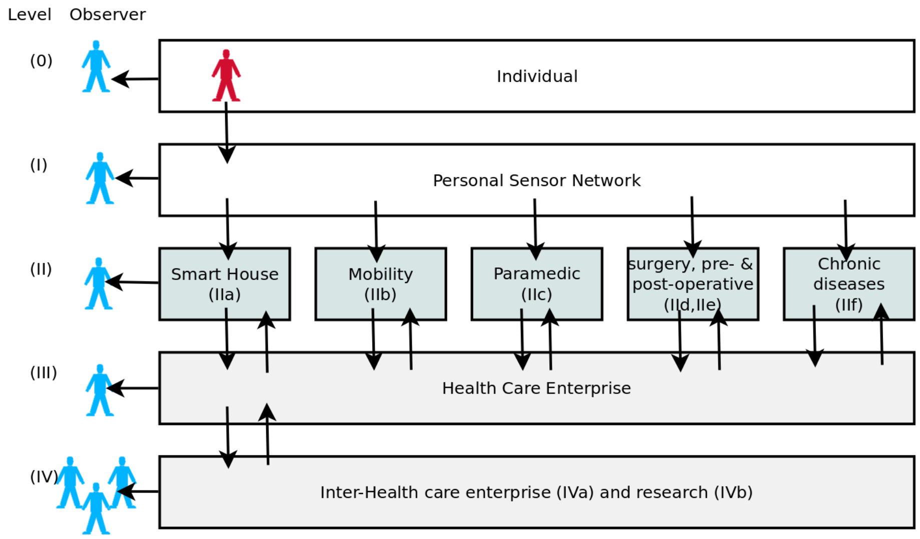


Figure 2. Generic eHealth framework indicating the use cases in five levels.

level model. Thus, this model is now divided into five levels – (0), (I), (II), (III), and (IV) – depending on the logical distance to the patient with Level (0) being the patient. For Level (II), usually only one type applies at a time. However, it must be possible to switch between the types in Level (II) as easily as the patient moves between them.

(0) Patient. This is the actual patient.

(I) Personal sensor network. The personal sensor network denotes the patient and the sensors measuring the medical data. These sensors are connected to each other in a biomedical sensor network (BSN). While this sensor network can be connected randomly, in most cases one special BSN node is appointed to be a personal cluster head (PCH), where all data for one patient are collected.

(IIa) Paramedic. In the paramedic scenario, the BSN is connected to the medical devices of an ambulance (car, plane, helicopter) via the PCH. The devices of the ambulance can work autonomously, showing the patient status locally. Alternatively, the devices of the ambulance can communicate with an external healthcare infrastructure, e.g., at a hospital.

(IIb) Smart home. The smart home scenario envisages that the patient is in a smart-home environment, where the personal sensor network is connected to the infrastructure of the smart-home. The smart home infrastructure might be connected to a healthcare enterprise infrastructure using long-distance data communication.

(IIc) Mobility. The mobility scenario envisages that the patient is mobile, e.g., using public or personal transportation facilities. The personal sensor network of the patient is connected to the infrastructure of a healthcare enterprise via a mobile device, e.g., a mobile Internet connection.

(IId) Intensive care/surgery. During an operation the sensor data are transferred to the PCH or directly to the hospital infrastructure over a relatively short distance. The

Table 1. Generic levels (GLs) for IoT E-Health

GL	Description
(0)	Patient
(I)	Personal sensor network, e.g., BSN.
(IIa)	Paramedic scenarios
(IIb)	The patient is in a smart home environment.
(IIc)	Mobility scenarios. The patient is mobile, using available cellular networks or WLAN zones
(IId)	Intensive care or surgery.
(IIe)	Pre- or postoperative sensor data management
(IIf)	Use of BSN for chronic patients (similarities to (IIb).)
(III)	Healthcare information system comprising the hospital network, computing facilities, databases and access terminals in the hospital.
(IVa)	Communication between healthcare providers
(IVb)	Communication between healthcare provider and research

sensors are in a very controlled environment, but some sensors might be very resource limited due to their size, so extra transport nodes close to the sensors might be needed.

(IIe) Pre- and postoperative. During pre- and postoperative phases of a treatment, and for use in hospital bedrooms, the sensor data are transferred from the sensor network to the PCH, and from there to the healthcare information system.

(IIf) Chronic disease treatment. The BSN data are used by healthcare personnel in non-emergency treatment of individual patients with a chronic disease.

(III) Healthcare information system. The healthcare information system is considered a trusted environment. It consists of the hospital network, the computing facilities, databases, and access terminals in the hospital. Note that that the communication between Levels (II) and (III) is two-way.

(IVa) inter-healthcare provider. Information is shared between different healthcare providers concerning medical information of an individual patient.

(IVb) healthcare provider and research. Information is shared between healthcare providers and medical research organisations for the purposes of research, new solutions development, etc.

3 The Structure of the ASSET Scenarios

The scenarios in healthcare using biomedical sensor networks are quite complex. Therefore, we need to structure the scenarios (hereafter denoted as *overall scenarios*) into sub-scenarios (hereafter denoted as *core scenarios*) and the transitions in between them. In this section, we describe *a*) *overall scenarios*, showing the overall use case in healthcare and

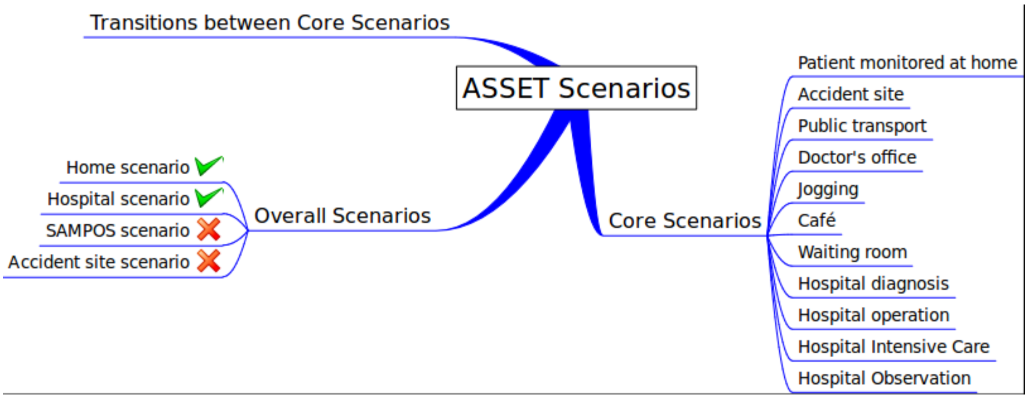


Figure 3. Overview of the structure of the ASSET scenarios.

welfare, e.g., a home situation or a hospital situation (overall scenarios are described in Section 3.1); *b*) *core scenarios*, showing situations with well-defined requirements (core scenarios are described in Section 3.2); and *c*) *transitions* between the core scenarios (transitions are described in Section 3.3). Figure 3 shows the structure of the ASSET scenarios.

3.1 Overall Scenarios

The overall scenarios are derived from scenarios that were used in the projects *Credo* and *SAMPOS* (Balasingham et al., 2007; Leister et al., 2011). For ASSET, the overall scenarios are:

a) Overall Scenario A, a home scenario; and

b) Overall Scenario B, a hospital scenario.

Each of these overall scenarios will contain a set of core scenarios and the transitions in between these as outlined below.

3.1.1 The ASSET Home Scenario (A)

Overall Scenario A envisages a home scenario where a monitored patient lives a normal life at home (i.e., *not* in a hospital). The patient can be in several situations:

- The patient is at home or in a nursing home using monitoring equipment (Core Scenario I).
- The patient will visit the doctors office (Core Scenario V) regularly and use public transport to get there (Core Scenario IV); the doctor's office will include the waiting room (Core Scenario VIII).
- The patient will regularly take walking or jogging tours (Core Scenario VI).
- The patient will regularly visit a café with friends (Core Scenario VII); this includes walking or commuting with public transport (Core Scenario VI and Core Scenario IV).
- In case of an emergency or planned surgery, the patient may be sent to a hospital with an ambulance (Core Scenario III).

3.1.2 The ASSET Hospital Scenario (B)

Overall Scenario B envisages a hospital scenario where a patient enters a hospital for a planned surgery (*not* an emergency). The patient will first be in a waiting room (Core Scenario VIII) before undergoing a diagnosis phase (Core Scenario IX). Eventually, surgery will be performed on the patient (Core Scenario X), followed by intensive care (Core Scenario XI). During convalescence, the patient will be in a room under observation and monitoring (Core Scenario XII). We will also consider the case when the patient is delivered to the hospital by an ambulance (Core Scenario III).

3.2 Core Scenarios

The core scenarios describe a specific part of an overall scenario; e.g., a situation a patient experiences. Each core scenarios can be part of several overall scenarios. We define 12 core scenarios for the ASSET project that are outlined below[1].

3.2.1 Patient Monitored at Home Scenario (I)

In Core Scenario I, where biomedical sensors are employed in an environment in which the patient is at home or in a nursing home. The patients are monitored by biomedical sensor networks, and the sensor data and alarms can be transmitted to medical centres and emergency dispatch units.

In this scenario, the sensors might not be monitoring or transmitting the physiological patient data continuously in order to reduce battery power consumption. Depending on a predefined algorithm, abnormal sensor data from certain sensors may be used to activate other sensors autonomously before an alarm is triggered, and sent to a central monitoring unit. In this scenario, the following characteristics are given:

1. Ease of use and non-intrusiveness are important issues.
2. Very low power consumption, enabling a long life span of the batteries, is required.
3. A network infrastructure is available, such as access to the Internet via LAN, WLAN, or mobile networks.
4. Limited mobility, handoff is possible, but infrequent.

Core Scenario I could be split up into several sub-scenarios, if necessary, depending on the patient's activities, time of the day, etc. These sub-scenarios may include sleeping, watching TV, kitchen work, or other household activities.

3.2.2 Accident Site Scenario (II)

Core Scenario II, is a disaster and accident response application scenario, for example a response to a fire, terrorist attack, or a traffic accident.[2] In this scenario, biomedical sensors are deployed, to measure values like blood pressure, temperature, pulse and ECG in

[1] The Core Scenarios XI, I, and II (*Post operative monitoring of patients with artificial heart*, *early warning of heart attack and/or stroke*, and *deployment of biomedical sensors networks at the site of an accident*) have been selected from the projects *Credo* and *SAMPOS*.

[2] Note that Core Scenario II, which has been developed for the *SAMPOS* project, is *not* included in the ASSET overall scenarios. We include the accident-scenario in this document for completness.

an ad-hoc network at the site of an accident. Here, the normal wired or wireless communications infrastructures may be damaged or unavailable, and a large number of severely injured people might overwhelm the emergency field personnel and hospital staff. This could prevent them from providing efficient and effective emergency rescue. Biomedical sensor networks can be quickly deployed to monitor vital signs. A large number of injured can be monitored simultaneously.

In this scenario, the following characteristics are given:

1. The sensor network must operate autonomously, and needs a high degree of self-organisation. The network topology is highly dynamic. Therefore, the sensor nodes should be able to discover each other and setup a sensor network autonomously.
2. A fixed network infrastructures is not available; data transfered from Level (II) to Level (III) must use a mobile network or other specific wireless network, such as microwave, or digital trunk communication.
3. The radio link might be unstable and the radio link quality might vary. Additionally, the communication environment is rather complex, since many sensor nodes may be deployed in a small area, possibly causing severe channel competition.
4. High degree of mobility. Handoffs are possible and might be frequent.
5. Blue-light functionality. That is, being able to re-use sensors on short notice with high flexibility (short-cutting some of the usual procedures).

3.2.3 Ambulance Scenario (III)

In Core Scenario III, the patient is in an ambulance. The sensors on the patient are connected to the ambulance's information system, which is connected to a hospital infrastructure via a mobile network connection. The communication between the patient's sensors is either directly to the ambulance infrastructure, or via the mobile phone. The ambulance and the patient's mobile phone might use different carriers.

Note that once the patient is inside the ambulance, sensors should communicate with devices in the ambulance without involving the mobile carrier.

3.2.4 Public Transport Scenario (IV)

Core Scenario IV presents a scenario where a patient commutes to a doctor's office or to a café using public transport. Here, the patient needs to use a smartphone as a device that collects sensor data, using the mobile networks to transmit the data. Blind spots without connectivity to a mobile network, roaming, varying data transmission quality, etc. are parts of this scenario.

3.2.5 Doctor's Office Scenario (V)

In Core Scenario V, the patient is in the doctor's office, usually after some time in a waiting room (Core Scenario VIII). Here, the patient can have attached extra sensors. These extra sensors, as well as the existing sensors, can communicate with the doctor's infrastructure either through the smartphone of the patient, or directly, depending on the needs. The doctor can change characteristics of the sensors, which requires the possibility to re-program the sensor devices.

3.2.6 Walking and Jogging Scenario (VI)

In Core Scenario VI, the patient does daily training of jogging in the nearby park or in the woods, does shorter walks, e.g., from the home to the public transport, to the café, shop, or doctor's office. Common in these situations is that the patient needs to use a smartphone as a device that collects sensor data, using the mobile networks to transmit the data. When walking or jogging in the park many other people and their devices might interfer with the communication of the smartphone.

When walking in the woods, there might be several spots which are not covered by a mobile network. In this case, the signal is so weak that only an emergency calls from another provider can be done. While data traffic is not possible, SMS messages can be used to send data with very low bandwidth, possibly after several retries. For an average walking trip, this outage may last for some minutes.

3.2.7 Café Scenario (VII)

In Core Scenario VII, the patient is in a cafe. Here, the patient needs to use a smartphone as a device that collects sensor data, using mobile networks or café's WLAN zone for data transfer. Here, switching between the WLAN and mobile networks may occur, the WLAN might be of varying quality, many other café visitors may interfere, or the WLAN might not actually be connected to the Internet.

3.2.8 Waiting Room Scenario (VIII)

The Core Scenario VIII describes a patient in a waiting room at a doctor's office or in a hospital. Patients that are known to the healthcare system can be connected from their smartphone to the healthcare network; here, specific actions for collecting data from the device or other preparations can be performed. For patients without a specific need for extra sensors, the waiting room will serve as a connection through the WLAN zone of the waiting-room with the same functionality as in Core Scenario VII (café scenario).

Note that once the patient is in the range of the hospital area, the use of smartphones to transfer patient data to the system can be direct to devices in the hospital infrastructure via short-range communication, instead of using long-range mobile communication.

3.2.9 Hospital Diagnosis Scenario (IX)

In Core Scenario IX, the patient is examined; extra sensors are attached, and existing sensors on the patient might be accessed both directly and via the patient's smartphone. In addition, NFC tags are used to identify objects. The medical personnel can re-configure and re-program the sensors during diagnosis.

3.2.10 Hospital Operation Scenario (X)

In Core Scenario X, the patient is under surgery; extra sensors are attached, and existing sensors on the patient are accessed directly by the hospital system rather than through the smartphone of the patient. In this scenario, the QoS is set very high, while security-wise the sensors are in a protected zone. The medical personnel can re-program the sensors during the operation.

Note that this scenario is different from Core Scenario V (doctor's office) since the hospital is connected to a different kind of network infrastructure. Usually, the primary healthcare points (doctor's office) and hospitals have different security requirements and regimes.

3.2.11 Hospital Intensive Care Scenario (XI)

In Core Scenario XI, the patient is in intensive care after an operation. Extra sensors are attached, and existing sensors on the patient might be accessed both through the patient's smartphone, and directly through the hospital infrastructure. In addition, NFC tags are used to identify objects. In most cases, the smartphone will be used as PCH. The medical personnel can re-program the sensors during intensive care.

In this scenario, biomedical sensors are used in a hospital environment. Here, the patient is located in an operating room (OR) or intensive care unit (ICU) while undergoing intensive monitoring of vital physiological parameters. Additional sensors might be required during this procedure to monitor other physiological parameters. The patient may be moved between different rooms during the treatment, e.g., from the OR to the ICU, but monitoring must continue uninfluenced by this. The sensor data may need to be transferred over different wireless networks. The system should be able to cope with breakdown in sensor nodes, new software updates, wireless network traffic congestion, and interferences with other wireless networks and biomedical devices.

In this scenario, the following characteristics are given:

1. A fixed network infrastructure is available between Levels (II) and (III) which can be accessed by the sink nodes of the BSN.
2. The scenario includes a complex communication environment. Interference from coexisting wireless networks, mobile networks, and various medical facilities is possible; this may reduce the performance of the transmission.
3. The network topology in this scenario is fixed. However, changes to the network topology may happen while patients are moving or being moved from one place to another, possibly causing handoffs to other gateways. Roaming to other networks is not part of this scenario in order to stay within the hospital domain.

3.2.12 Hospital Observation Scenario (XII)

In Core Scenario XII, the patient is in a room under "normal" observation; in contrast to the home scenario, the patient's smartphone has direct access to the hospital systems and will deliver data directly with higher QoS through the secured hospital systems.

3.3 Transitions between Core Scenarios

We select the important transitions between the core scenarios. The transitions that are foreseen to be used in ASSET are shown in Table 2. Figures 4 and 5 show the the home

Table 2. Overview of core scenarios. A bullet (•) means that this core scenario is included in the overall scenario. Transitions in paranthesis can be considered, but are unlikely or covered otherwise.

core	core scenario	ov. sc.		transition to
scenario	name	A	B	core scenario
I	home monitoring	•		VI, III
II	accident			III
III	ambulance	•	•	IX, (V)
IV	public transport	•		VI
V	doctor's office	•		VI, III
VI	jogging, walking	•		IV, I, VIII, (III)
VII	café	•		VI, (III)
VIII	waiting room	•	•	V, IX, VI
IX	hospital diagnosis		•	X, XI, XII, VI, (VIII)
X	hospital operation		•	XI, (IX)
XI	hospital intensive		•	XII, X
XII	hospital observation		•	VI, XI, IX

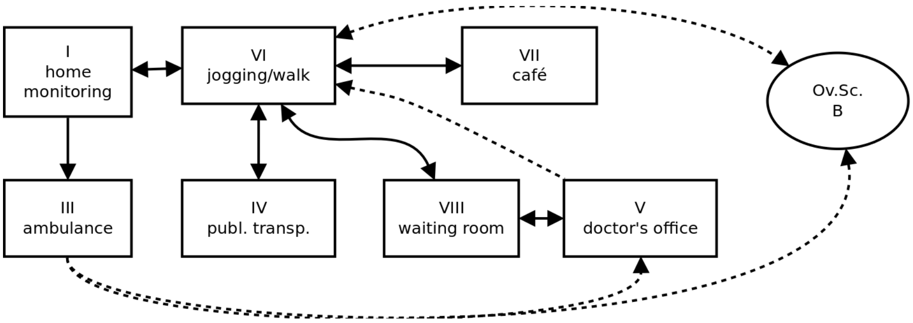


Figure 4. Overall Scenario A and its transitions.

and hospital scenarios, respectively, including the transitions between the core scenarios in a graphical notation.

4 Creating Storylines

The set of overall scenarios, core scenarios, and transitions can be used to create *storylines* that can be used as case studies in ASSET. We show some examples to illustrate such storylines. Several (technical) details in these storylines need to be defined at a later stage when the technical and security requirements become ready. We present storylines for both Overall Scenario A (home scenario) in Section 4.1 and Overall Scenario B (hospital scenario) in Section 4.2.

4.1 Storyline for Home Scenario

Petra has both a heart condition and diabetes. In a hospital, she had two sensors placed in her body: one heart sensor and one diabetes sensor. In addition, she uses external sensors

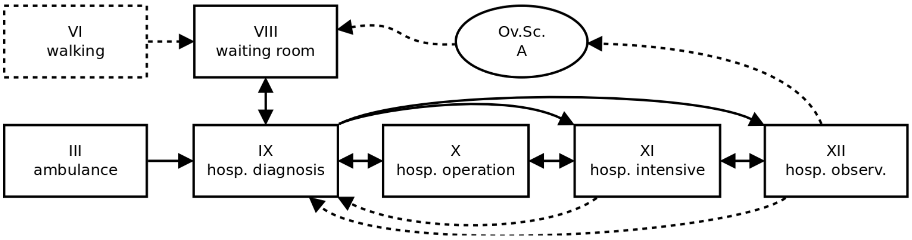


Figure 5. Overall Scenario B and its transitions.

to measure blood pressure, heart beat, inertial sensors, etc., as well as a camera. Petra is living in her home that has been prepared for the monitoring system and is commissioned with the necessary data connections so that her vital signs can be periodically reported to the healthcare personnel in levels (II) (nurse or doctor) or (III) (patient records) as introduced in Figure 2; several technologies will be discussed.

The patient monitoring system is set up so that the sensor data are transmitted wirelessly (several transmission technologies are possible) to a smartphone that acts as PCH. The PCH communicates with the hospital infrastructure (Level (III)).

1. Petra is now being monitored at home but data is acquired remotely (Core Scenario I); the following requirements are important:
   a. Petra wants her data to remain confidential from neighbours, i.e., people close-by, but outside her home;
   b. Petra wants her data to remain confidential from visitors, i.e., people inside her home.
2. Petra takes a bath in her home (planned sensor acquisition disruption; Core Scenario I);
   a. the sensors are water-proof; the PCH is close enough to receive signals;
   b. the sensors must be removed;
      i. a change in the values implicitly indicates the sensor removal; or
      ii. patient must notify the PCH about the sensors going off-line;
3. Petra is sleeping and sensors fall off (unplanned sensor acquisition disruption; Core Scenario I);
4. Petra leaves her home for training outdoors or a stroll in the park nearby (Core Scenario VI).
5. Petra leaves her home to visit her friends in a café (Core Scenarios VI, VII, IV).
6. Petra visits her regular doctor for a check-up; the doctor's office is in walking distance from her home; Core Scenarios VI, VIII, and V.
7. Petra becomes ill and is transported by an emergency ambulance to the hospital; Core Scenario III and transition to Overall Scenario B.

4.2 Storyline for Hospital Scenario

Petra has both a heart condition and diabetes. One year ago, she had two sensors placed in her body: one heart sensor and one blood sugar sensor that both communicate wirelessly. In addition, she uses external sensors to measure blood pressure, heart beat, inertial sensors, etc., as well as a camera. Petra suddenly gets ill while being at home that is caught by the patient monitoring system installed at her home.

1. Petra is taken in an ambulance to the hospital (Core Scenario III). In addition to the sensors she is using, the paramedics use EEG and ECG sensors. The information from all sensors is being available in the ambulance from three possible sources:

   a. information received directly from the sensors, available on the displays in the ambulance;

   b. information received from the PCH that Petra is using;

   c. information received from the healthcare records.

2. After the ambulance arrives at the hospital, Petra is moved to a room where diagnosis of her condition is performed (Core Scenario IX). Different sensors are used to find out her condition. These sensors are removed after diagnosis.

3. It becomes clear that Petra needs to undergo surgery (Core Scenario X). During surgery sensors are used to measure certain biomedical values. However, the medical procedure also creates electromagnetic noise in the same band as the data transmission between sensors is ongoing.

4. After the surgery, Petra is moved to intensive care (Core Scenario XI) where a variety of sensors are used to observe her biomedical values.

5. After two days, Petra is moved to a recovery room with three other patients to allow time for her surgery wound to heal and for observation (Core Scenario XII). In addition to the heart and blood sugar sensors, two additional sensors are now used, but these will be removed after the observation phase is over. The two other patients in the same room are using the same kind of sensors.

   a. The sensors Petra is using transmit their readings to her PCH.

   b. The additional sensors Petra is using transmit their readings to a base station in the patients' room, while her ordinary sensors are reporting to her PCH.

6. Petra is discharged from hospital; transition to Overall Scenario A.

5 Conclusion

In this note, we presented

- an extension of the generic system models presented by Leister et al. (2011) by adding Level (IV) for inter-enterprise communication, as well as as sub-level (IIf) for patients with chronic diseases;

- the scenarios to be used in the ASSET project consisting of two overall scenarios (a home scenario and a hospital scenario). These overall scenarios use a variety of core scenarios that address specific situations. From these elements we created two storylines: one for a home patient with chronic diseases. and one for a hospital patient undergoing surgery and recovery.

These overall and core scenarios, as well as the storylines will be used in the ASSET project to evaluate the work within adaptive security, addressing the objectives presented by Savola et al. (2012).

References

Abie, H. and Balasingham, I. (2012). Risk-based adaptive security for smart IoT in eHealth. In *BODYNETS 2012 – 7th International Conference on Body Area Networks*. Association for Computing Machinery (ACM). 5, 6

Balasingham, I., Kyas, M., Leister, W., Liang, X., Østvold, B. M., Rossum, A. v., Salden, A., Steffen, M., and Valk, J. M. (2007). Deliverable D6.1 – user driven requirements. Deliverable, CREDO, Project number 33826, funded by the European Commission. 5, 9

Leister, W., Fretland, T., and Balasingham, I. (2009). Security and authentication architecture using MPEG-21 for wireless patient monitoring systems. *International Journal on Advances in Security*, 2(1):16–29. Available from: http://www.iariajournals.org/security/. 5

Leister, W., Schulz, T., Lie, A., Grythe, K. H., and Balasingham, I. (2011). *Biomedical Engineering Trends in electronics, communications and software*, chapter Quality of Service, Adaptation, and Security Provisioning in Wireless Patient Monitoring Systems, pages 711–736. INTECH. 5, 6, 9, 16

Savola, R., Abie, H., and Sihvonen, M. (2012). Towards metrics-driven adaptive security management in e-health iot applications. In *BODYNETS 2012 – 7th International Conference on Body Area Networks*. Association for Computing Machinery (ACM). 5, 6, 17