SINTEF

SINTEF A23344- Unrestricted

Report

Report on ESUMS Risk Analysis

Author(s)
Aida Omerovic
Anders Kofod-Petersen
Bjørnar Solhaug
Ingrid Svagård
Le Minh Sang Tran (University of Trento)

SINTEF ICT
Networked Systems and Services
2012-09-06

SINTEF

SINTEF IKT
SINTEF ICT

Address:
Postboks 124 Blindern
NO-0314 Oslo
NORWAY

Telephone:+47 73593000
Telefax:+47 22067350

postmottak.IKT@sintef.no
www.sintef.no
Enterprise /VAT No:
NO 948 007 029 MVA

Report

Report on ESUMS Risk Analysis

KEYWORDS:
Risk analysis, information security, welfare technology, patient monitoring, ESUMS, CORAS

VERSION
1.1

DATE
2012-09-06

AUTHOR(S)
Aida Omerovic
Anders Kofod-Petersen
Bjørnar Solhaug
Ingrid Svagård
Le Minh Sang Tran (University of Trento)

CLIENT(S)
SINTEF ICT

CLIENT'S REF.
N/A

PROJECT NO.
90B300

NUMBER OF PAGES/APPENDICES:
49 + Appendices

ABSTRACT

This report documents the results of the first case study in the FRISK project, namely a risk analysis. The target of analysis is the ESUMS (Enhanced Sustained Use Monitoring System) prototype system and services for remote patient monitoring. The risk analysis was conducted using the CORAS framework for model-driven risk analysis over a timespan of 10 weeks, and included six workshops. The analysis team consisted of five people, including one analysis leader and two experts in the ESUMS domain. The risk analysis focused on security needs of stakeholders, addressing properties such as confidentiality, integrity and availability of critical information, as well as privacy and data protection. In addition to this, the analysis considered compliance with data protection laws and regulations, as well as service provisioning, i.e. the ability of the system and the service provider to maintain the expected level of service.

PREPARED BY
Bjørnar Solhaug

SIGNATURE

CHECKED BY
Atle Refsdal

SIGNATURE
Atle Refsdal

APPROVED BY
Ketil Stølen

SIGNATURE
Ketil Stølen

REPORT NO.
SINTEF A23344

ISBN
978-82-05303-6

CLASSIFICATION
Unrestricted

CLASSIFICATION THIS PAGE
Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
0.1	2012-04-10	First draft of Section 1 and Section 2
0.2	2012-05-31	First draft of Section 3 through Section 6
0.3	2012-06-12	Second draft of Section 1 through Section 6
0.4	2012-06-21	Semi-final version of Section 1 through Section 6
0.5	2012-08-17	Full semi-final version of the whole report
1.0	2012-08-17	Finalized for quality check
1.1	2012-09-06	Finalized

Table of contents

Terms and definitions

A **party** is an organisation, company, person, group or other body on whose behalf a risk analysis is conducted

An **asset** is something to which a party assigns value and hence for which the party requires protection

An **indirect asset** is an asset that, with respect to the target and scope of the analysis, is harmed only via harm to other assets

A **direct asset** is an asset that is not indirect

Electronic Health Record (EHR) is a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. Included in this information are patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports. The EHR automates and streamlines the clinician's workflow. The EHR has the ability to generate a complete record of a clinical patient encounter – as well as supporting other care-related activities directly or indirectly via interface – including evidence-based decision support, quality management, and outcomes reporting [3].

Information security: Preservation of confidentiality, integrity and availability of information [6]

- **Confidentiality**: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes
- **Integrity**: Property of protecting the accuracy and completeness of (information) assets
- **Availability** : Property of being accessible and usable upon demand by an authorized entity

Data protection: Protection of personal data from misuse (as regulated by governmental laws and regulations)

Personal data: Any information relating to an identified or identifiable person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more specific factors (such as physical, physiological, mental, economic, cultural and social) [7]. Note: Health information is a subset that is restricted by further laws and regulations.

A **threat** is a potential cause of an unwanted incident

A **threat scenario** is a chain or series of events that is initiated by a threat and that may lead to an unwanted incident

An **unwanted incident** is an event that harms or reduces the value of an asset

A **vulnerability** is a weakness, flaw or deficiency that opens for, or may be exploited by, a threat to cause harm to or reduce the value of an asset

Executive Summary

This report documents the results of the first FRISK case study. The case study involved conducting a risk analysis, and the target of analysis was the ESUMS (Enhanced Sustained Use Monitoring System) prototype system and services for remote patient monitoring. The risk analysis was conducted using the CORAS framework for model-driven risk analysis over a timespan of 10 weeks, and included six workshops. The analysis team consisted of five people, including one analysis leader, two analysis secretaries and two experts in the ESUMS domain.

The selected party for the risk analysis was the service provider, i.e. an organization providing the services based on the ESUMS system. The customer of this service provider is a public health organization. The service provider is a 3rd party with respect to the health organization, and is a tenderer of the health care services that are supported by the ESUMS system.

The ESUMS system is currently a prototype under development, but the risk analysis was conducted under the assumption that the system is in use in a real-life setting. Further assumptions include the following: The monitored patients have a chronic condition, but not acute; the patients are monitored at home; the system is used every day by the patient for many hours each day; the nurse will use the system once a day as part of a daily follow-up routine for each patient. The components of the ESUMS system include the following: A patient sensor device; the ESUMS server providing database and web services; desktop application for remote monitoring of patient data; and handheld application owned by the patient to capture and display monitored data, and transmitting monitored data to the server.

The risk analysis focused on security needs of stakeholders, addressing properties such as confidentiality, integrity and availability of critical information, as well as privacy and data protection. In addition to this, the analysis considered compliance with data protection laws and regulations, as well as service provisioning, i.e. the ability of the system and the service provider to maintain the expected level of service.

The risk identification and assessment was structured according to four different parts or aspects of the ESUMS system, namely risks related to patients at home, risks related to the ESUMS server, risks related to the nurse workstation, and risks related to the infrastructure. The risk analysis resulted in 153 identified and documented risks. In addition, 12 more high-level risks were identified by accumulating those of the 153 risks that can be considered as special instances of the same more general risks. Hence, a total of 165 risks were identified. Out of these 165 risks, 27 risks were evaluated as unacceptable and therefore considered for possible treatment and mitigation.

The identified risks differ a lot with respect to which parts of the target system they arise from, and which assets that are harmed. However, one aspect that often was held as a potential source of risk is the deliberate or accidental misuse of the ESUMS system by its users. First, patients may be a threat in case they use the system erroneously, in case they are sloppy, or in case they do not bother to follow-up their responsibilities in an adequate manner. Second, nurses may be a threat in case they bypass any security routines or policies, or in case the ESUMS security mechanisms are insufficient.

As a conclusion, many of the identified risk treatments to improve the risk picture are concerned with improving competence and with preventing accidents or misuse by implementing security mechanisms. For the patients that are being monitored at home, improved training in the use of ESUMS is recommended. Additionally, contracts on conditions of use should be considered to make clear what the responsibilities and liabilities of the users of ESUMS are. To further prevent accidental or deliberate system misuse by patients, improved mechanisms for identification and authentication should be considered. Also for the nurses,

improved training is recommended, both with respect to the ESUMS technology and with respect to security. Routines or mechanisms for data verification and quality checking are also recommended.

1 Introduction

This report documents the results of the first FRISK risk assessment case study. The FRISK project aims for the development of a framework for risk assessment of welfare services that are based on welfare technologies, in particular focusing on security needs of stakeholders with respect to properties such as confidentiality, integrity and availability of sensitive or critical information, as well as privacy and data protection which are highly relevant in the eHealth domain.

The target of analysis for the reported risk analysis was the ESUMS prototype system (Enhanced Sustained Use Monitoring System) [2] and the services that are provided by the system, whereas the CORAS framework for model-driven risk analysis [1] was the selected risk analysis method for the case study. The rationale for choosing ESUMS is that it serves as an instance of the kind of systems that is addressed by the FRISK project, thereby providing a basis for evaluating the FRISK artefacts with respect to their requirements as defined in the FRISK problem analysis. The CORAS approach serves as the FRISK straw-man risk analysis framework. CORAS will be evaluated so as to identify which aspects, techniques, features, etc. that need to be further developed and customized to fulfil the requirements to the FRISK framework. The experiences from the risk analysis of ESUMS as an instance of the kind of systems addressed by FRISK will be an important basis for understanding general aspects of welfare technologies and services that need to be handled by the FRISK framework.

The CORAS risk analysis involved six workshops conducted over a timespan of 10 weeks. The method comprises eight steps, briefly summarised as follows.

1. **Preparations for the analysis**
   The customer briefly informs the analysis team about the target it wishes to have analysed, and the analysis team prepares for the analysis.
2. **Customer presentation of target**
   The customer presents the system or organisation it wished to have analysed; the focus and scope of the analysis is identified and an analysis plan is set up.
3. **Refining the target description using asset diagrams**
   The analysis team presents its understanding of the target of analysis; the assets are identified, as well as the most important related threats and vulnerabilities.
4. **Approval of the target description**
   The analysis team presents the documentation of the target of analysis for finalisation and approval by the customer; values are assigned to the identified assets, and the risk evaluation criteria are established.
5. **Risk identification using threat diagrams**
   Risks are identified through a structured brainstorming.
6. **Risk estimation using threat diagrams**
   The likelihoods and consequences for the identified risks are estimated.
7. **Risk evaluation using risk diagrams**
   The risks are evaluated against the risk evaluation criteria.
8. **Risk treatment using treatment diagrams**
   Treatments for the mitigation of unacceptable risks are identified and evaluated.

All steps of the CORAS method were conducted in this ESUMS risk analysis. An overview of the meetings with meeting dates, purpose of the meetings and the steps of the CORAS process covered by the meetings is given in Table 1. Note that Step 1 was conducted off-line. Also note that some of the steps needed more than one iteration, which is why the steps are not ordered sequentially over the meetings.

When	What	Step
March 2 2012	Target, focus, scope and assets	2-3
March 13 2012	Target, high-level analysis, scales and criteria	3-4
March 23 2012	Risk identification	5
April 13 2012	Scales, criteria and risk identification	3-4-5
May 4 2012	Risk estimation and risk evaluation	6-7
May 16 2012	Risk treatment	8

Table 1 - Overview of meetings

The results of the ESUMS risk analysis are documented in the subsequent sections. Section 2 documents the context of the analysis and covers Step 1 through Step 4 of the CORAS method. Section 3 documents the results of the risk identification, Section 4 documents the results of the risk estimation, Section 5 documents the results of the risk evaluation, and Section 6 documents the results of the treatment identification. Finally, we conclude in Section 7.

The analysis team is represented by the analysis leader, the analysis secretary, and the target team. The analysis leader and the analysis secretary are responsible for facilitating the analysis process, modelling the target, developing the risk models and reporting the findings. The target team includes the domain experts with thorough knowledge of the target of the analysis. The target team provides the input necessary for developing the target models and the risk models, and also approves the models that are developed. The entire analysis team actively participates at all workshops (steps of the analysis). The analysis team of the ESUMS case study consisted of five persons – two of them were domain experts in the ESUMS technology.

2 Context Establishment

Establishing the context of the analysis involves determining the goals and objectives of the analysis, as well as describing and documenting the target of analysis, including the focus, scope and assets to be protected. The context establishment also includes determining and documenting who is the party of the analysis, i.e. the stakeholder on whose behalf the risk analysis is conducted. This is important as it is only by determining the party that also relevant assets can be identified. A high-level risk analysis is moreover conducted in order to better understand the target of analysis and the main concerns. Finally, the likelihood and consequence scales for risk estimation are defined and documented, as well as the risk evaluation criteria for each asset.

2.1 Background

The selected party for the case study is the service provider, i.e. an organization (in our chosen case a private service provider) providing the services based on the ESUMS system. The services that are provided are those that are supported by ESUMS as specified in details in several documents [2][4][5]. In this report we give a more high-level description of the target of analysis, and also document the assumptions made for the risk analysis.

The customer of the service provider is a public health organization. The service provider is a 3rd party with respect to the health organization, and is a tenderer of the health care services that are supported by the ESUMS system. The service provider provides both the technology and the trained personnel (including nurses), and is responsible for the ESUMS system operation, management and maintenance. Note that the service provider is not system developer.

Assumptions include:

- The patients have a chronic condition (such as cardiovascular disease), but not acute
- The patients are monitored at home
- The system is used every day by the patient for many hours each day.
- The nurse will use the system once a day as part of a daily follow-up routine for each patient.

The ESUMS system is currently a prototype under development, but for the case study we assume that the system is in use in a real-life setting. This means that we identify assets and risks for a situation in which the services are being provided.

2.2 Target Description

This section describes the target of the analysis, i.e. the ESUMS system, its structure, usage, functionalities and stakeholders. Figure 1 (from [2]) provides an overview of the ESUMS system. The main components include the following.

- Patient sensor device, i.e. a chest unit with sensors measuring heart rate, skin temperature, activity level and posture.
- ESUMS server which provides database and web services. The server is hosted by the service provider.
- Desktop application for remote monitoring of patient data. The desktop application is used by a monitoring nurse.
- Handheld application installed on a smart phone or similar. The handheld is owned by the patient who wears the chest unit. The handheld application displays live data (acquired by the chest belt) for the patient.
- Additional component-off-the-shelf (COTS) devices which can be connected to the handheld. (Only SpO2 (oxygen saturation) interface is available from the handheld application to these servers.)
- A desktop application that connects to the patient sensor device and shows the sensor device data (same as on handheld) as well as the full ECG waveform. (Not shown in Figure 1 but also part of the ESUMS system.)

The patient sensor device and the additional COTS devices use Bluetooth for communication with the handheld. The handheld communicates with the ESUMS server over the internet (through 3G/WiFi). The desktop application is connected to the ESUMS server over the internet. There is at the moment no web-based access for next-of-kin and there are no web-applications. Moreover, for the current prototype, fewer things are monitored by the sensor than what is described in the requirements part of the ESUMS documentation [2]. Note that the interface to the scales data, depicted at the bottom right of Figure 1, is not implemented in the prototype.

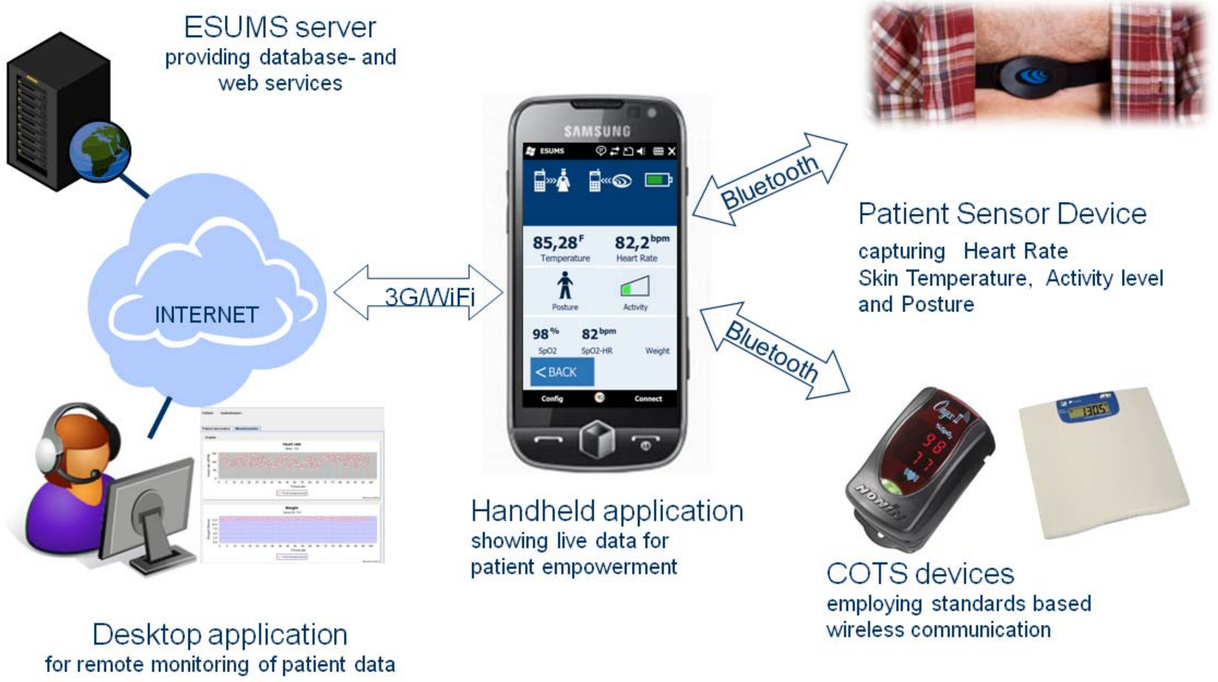


Figure 1- ESUMS overview.

Thus, ESUMS software consists of:

- A windows-based dedicated application for handheld (runs on Windows 6.5 ME)
- A nurse desktop application developed in java. The desktop application has support for setting thresholds by the nurse, documenting interactions with patient, as well as documenting remarks, explanations and comments regarding the data acquired
- Server services and database (i.e. server image software) that runs on a VMWare software platform.

By ESUMS data and in the context of this risk analysis we mean the following.

- The sensor data measured by the sensor device i.e. heart rate, posture, activity and skin temperature
- Sensor data measured by the external COTS sensor (SpO2 (oxygen saturation))
- The data in the configuration text files (on the handheld and the nurse desktop)
- User administrative information in the server database (user names, passwords, addresses, telephone numbers)

Figure 2 (from [2]) provides an overview of the use cases and actors relating to the ESUMS system. Note that the US Food and Drug Administration (FDA) is not relevant for this case study as this agency is responsible for public health regulations in the US. Moreover, next of kin is not part of the current ESUMS system, but will be considered in the analysis. EHR is relevant for the cases study, but there is no separate interface to it from the ESUMS system. Currently in ESUMS the monitored data is stored on the server, the chest unit and handheld.

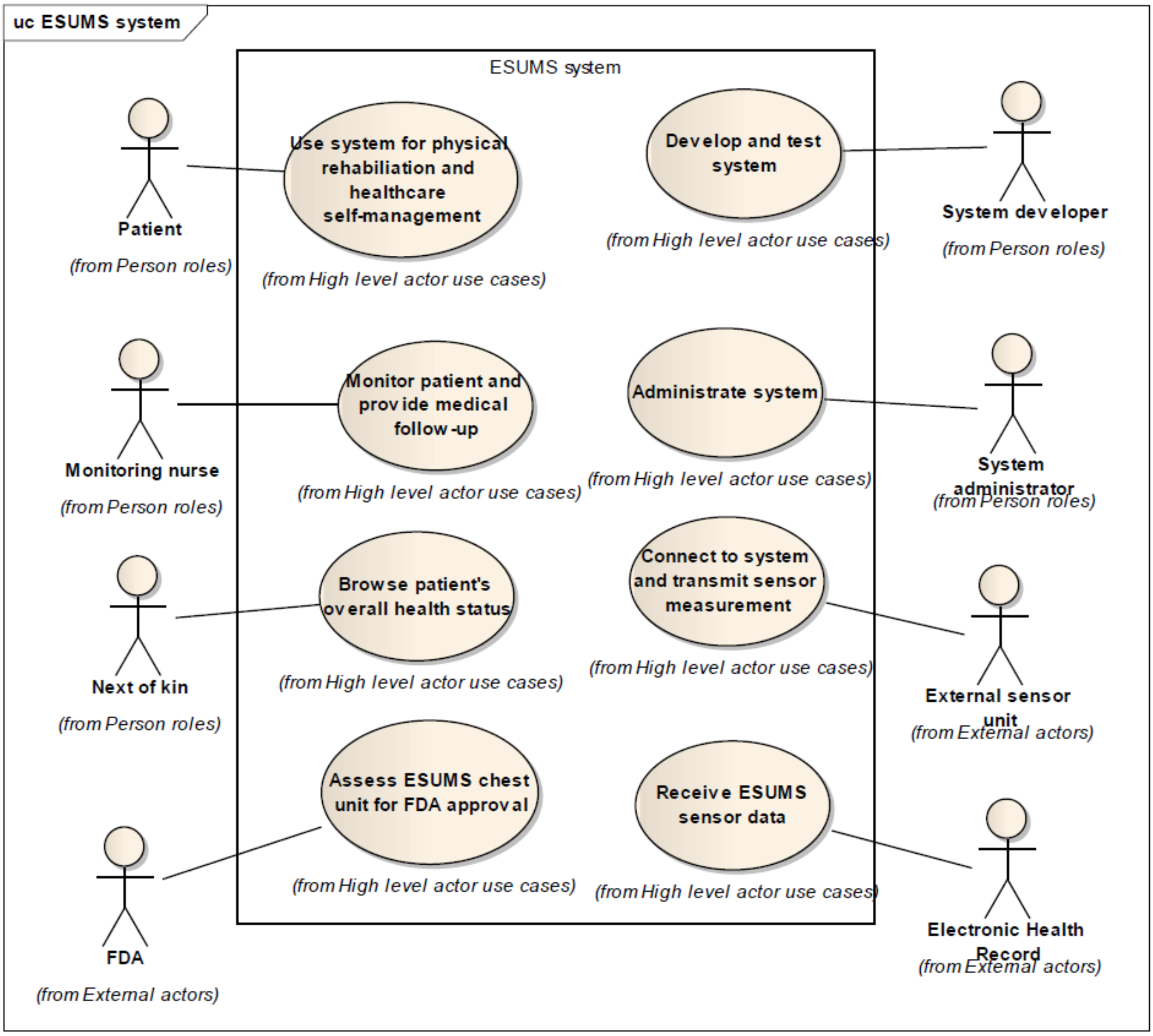

uc ESUMS system
ESUMS system
Patient
(from Person roles)
Use system for physical rehabiliation and healthcare self-management
(from High level actor use cases)
Develop and test system
(from High level actor use cases)
System developer
(from Person roles)
Monitoring nurse
(from Person roles)
Monitor patient and provide medical follow-up
(from High level actor use cases)
Administrate system
(from High level actor use cases)
System administrator
(from Person roles)
Next of kin
(from Person roles)
Browse patient's overall health status
(from High level actor use cases)
Connect to system and transmit sensor measurement
(from High level actor use cases)
External sensor unit
(from External actors)
FDA
(from External actors)
Assess ESUMS chest unit for FDA approval
(from High level actor use cases)
Receive ESUMS sensor data
(from High level actor use cases)
Electronic Health Record
(from External actors)

Figure 2 - Use cases and actors

Figure 3 specifies the ESUMS stakeholders and their responsibilities. The party of this analysis is the service provider which can be a health institution or a third party. The service provider is responsible for operating the ESUMS system, providing training to patients and nurses, signing contracts (development and maintenance) with technology provider, and (in case the service provider is third party) signing contracts with the health care institution.

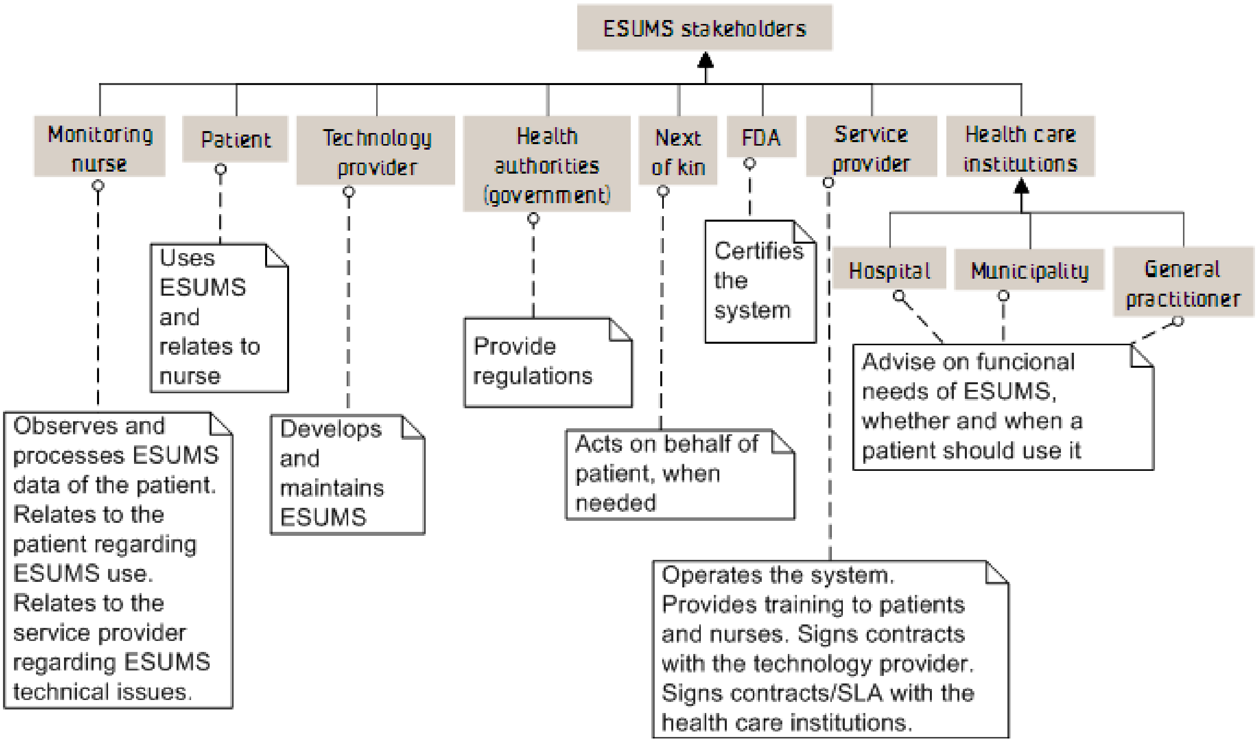

ESUMS stakeholders
Monitoring nurse
Patient
Technology provider
Health authorities (government)
Next of kin
FDA
Service provider
Health care institutions
Hospital
Municipality
General practitioner
Uses ESUMS and relates to nurse
Certifies the system
Provide regulations
Observes and processes ESUMS data of the patient. Relates to the patient regarding ESUMS use. Relates to the service provider regarding ESUMS technical issues.
Develops and maintains ESUMS
Acts on behalf of patient, when needed
Advise on funcional needs of ESUMS, whether and when a patient should use it
Operates the system. Provides training to patients and nurses. Signs contracts with the technology provider. Signs contracts/SLA with the health care institutions.

Figure 3 - ESUMS stakeholders

Figure 4 provides a conceptual diagram which specifies the scope of the analysis. From top to bottom, the elements represent person roles, system components, communication protocols/means, and external entities. (The use of colours is only to highlight the mapping to these categories as specified to the left.)

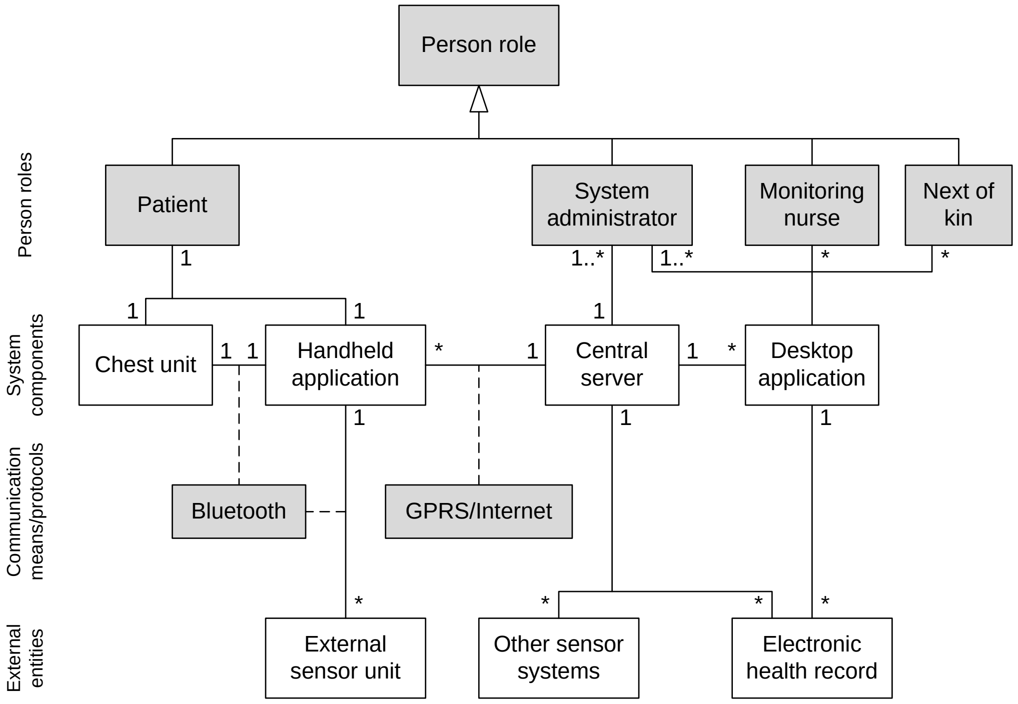


Figure 4 - conceptual view of the target

Summary of the main features of the ESUMS system

Chest unit is an easy-to-use sensor belt that continuously measures a set of physiological data. The chest unit communicates the data over Bluetooth to the handheld application. If no communication link is established, the data is stored locally on the belt and forwarded at a later stage. The handheld application 1) forwards the received data to the server, 2) shows the data to the user, and 3) enables the user to report overall health status. The server provides services for storing data on the server database, and for accessing/retrieving the data in the database. Main non-functional features include usability and reliability (e.g. ensure no loss of data), but some security features are missing in the current prototype. The following ESUMS security services are available for use in server platform: authentication, token management and user management. There is currently no N2N encryption and there is no encryption of data on the server. For further details regarding target description, see Appendix A. The reader is moreover referred to further ESUMS reports for additional documentation [2][4][5].

2.3 Asset Identification

An asset is something to which a party assigns value and hence for which the party requires protection. Asset identification is a core part of the context establishment since the assets are the focus of the analysis, and since a CORAS risk analysis is driven by the assets; all risks that are identified, as well as the threats and vulnerabilities, are with respect to the identified assets

The identified assets are documented by CORAS asset diagrams. An asset diagram specifies the party of the assets, which assets are direct and which are indirect, as well as the relations between the assets. An indirect asset is an asset that, with respect to the target and scope of the analysis, is harmed only via harm to other assets. A relation from one asset to another means that harm to the former may lead to harm to the latter. Because an indirect asset is harmed only via harm to other assets, the risk identification is conducted only with respect to the direct assets. Once the risk identification for the direct assets is completed, the indirect assets are taken into account. In a CORAS asset diagram, direct assets are coloured and with a solid outline, whereas indirect assets are white and with a dashed outline.

The assets identified from the point of view of the service provider as the party of the analysis are shown in Figure 5. The direct assets are *ESUMS data security*, *Compliance* and *Service provisioning*. As specified above, by ESUMS data we refer to patient health information (and other patient data that is relevant for the provided services) that is stored, gathered and processed by the ESUMS system, including the monitored data and other data that is stored on the ESUMS server, on the handheld and on the belt. The data can be accessed and viewed on the nurse workstation. We focus on the protection of the security of this information asset, hence the asset name *ESUMS data security*. By *Compliance* we mean compliance with and obedience to data protection laws and regulations, (i.e. for privacy regulations). By *Service provisioning* we mean the ability to maintain the expected service level.

The indirect assets are *Cost effectiveness*, *Customer trust*, *Patient trust* and *Patient quality of life*. By *Cost effectiveness* we mean the ability to maintain a justifiable level of cost of running the service by comparing gain and cost. The costs should be justifiable when comparing with the alternative of providing traditional health care services without use of monitoring. *Customer trust* refers to the trust of the tenderer in the services provider, whereas *Patient trust* refers to the trust of the monitored patient in the service provider. Finally, by *Patient quality of life* we mean health and general comfort of the monitored patient.

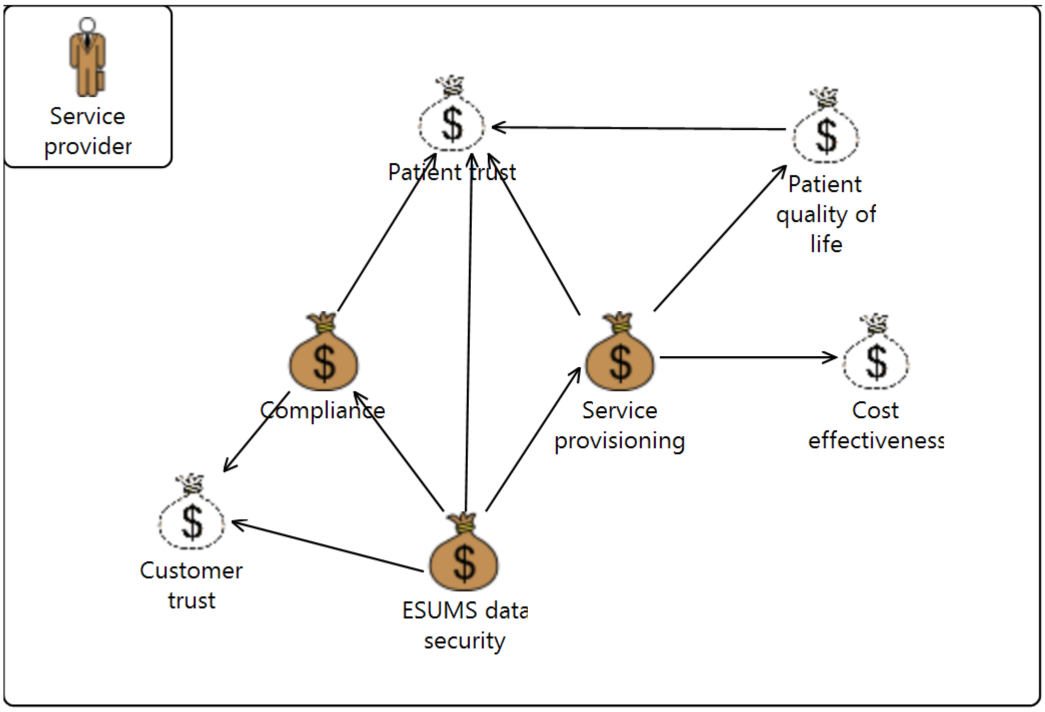


Figure 5 - Assets

2.4 High-level Analysis

The high-level risk analysis is conducted to establish an initial, high-level overview of risks at an enterprise level. It is conducted with respect to the identified assets and the documented target of analysis, and contributes to better understand the desired scope and focus of the risk analysis. In this risk analysis, the high-level risk analysis was conducted as a structured brainstorming where the results were documented on-the-fly in a table. The main terms that were used to structure the discussions and document the results are defined in Table 2.

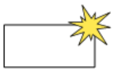
Symbol	Term	Definition
	Asset	Something to which a party assigns value and hence for which the party requires protection
	Vulnerability	A weakness, flaw or deficiency that opens for, or may be exploited by, a threat to cause harm to or reduce the value of an asset
	Threat	A potential cause of an unwanted incident
	Threat scenario	A chain or series of events that is initiated by a threat and that may lead to an unwanted incident
	Unwanted incident	An event that harms or reduces the value of an asset

Table 2 - Symbols for the main terms

After the brainstorming workshop, the results were structured according to various parts of the target of analysis, namely Home (Table 3), ESUMS server (Table 4), Nurse desktop (Table 5), and Environment /external factors (Table 6).

⚠ ⚠ ⚠	⚠ $	🔓
Who/what causes it?	**How? What is the scenario or incident? What is harmed?**	**What makes it possible?**
Patient	Data transmission from chest unit to handheld is interrupted/not happening, affecting availability of ESUMS data. (E.g. patient moves out of range, fails to charge the chest unit, forgets to connect the chest unit to the hand held, not wearing belt properly, etc.)	Lack of user/patient training. Lack of understanding of system interface.
Patient/ External person (friend/next of kin) / Nurse	Data transmission from hand held to server is faulty due to accidental misconfiguration of configuration file.	Lack of protection of configuration file
Chest unit component	Hardware failure/ bugs of chest unit, affecting availability of ESUMS data	Immature technology
Handheld component	Hardware failure of handheld, affecting availability of ESUMS data.	Unreliable handheld
Handheld component	Software failure leads to handheld or patient application not responding. Loss of availability of ESUMS data and services.	Immature technology
Nurse	Erroneous user information inserted in configuration file on handheld denying handheld communication access to server.	Manual, error-prone configuration; lack of verification.
Nurse	Information from wrong user inserted in configuration file leading to merging of data from different patients or disabling correct data acquisition; loss of integrity of ESUMS data. Double measurement can result if the same data is inserted in configuration file on two handhelds.	Manual, error-prone configuration; lack of verification.
Patient	Users themselves change the configuration file, harming the integrity of configuration file.	Lack of protection of configuration file.

Table 3 - High-level risk identification w.r.t. home

⚠ ⚠ ⚠	⚠ $	🔓
Who/what causes it?	**How? What is the scenario or incident? What is harmed?**	**What makes it possible?**
System failure	ESUMS server goes down / becomes unavailable	Immature technology; insufficient maintenance
System administrator	System administrator accidently inserts wrong user information, health information, management information, etc. on the server. Leads to loss of data integrity.	Insufficient training. Manual and error-prone routines. Lack of verification.
System administrator	System administrator stores or transmits ESUMS data on irregular media (e.g. local backup or transmitting data by email). Confidential data leaks to 3rd party due to accidental disclosure.	Work process not aligned with policy. Lack of competence.
System administrator / Nurse / Adversary	Malware introduced by adversary via email. Malware infects server and causes leakage of ESUMS data.	Insufficient malware protection. Work process not aligned with policy.
System administrator	Nurse gets wrong (missing / unnecessary) access to patient accounts.	Error-prone routines; lack of verification

Table 4 - High-level risk identification w.r.t. ESUMS server

⚠ ⚠ ⚠	⚠ $	🔓
Who/what causes it?	**How? What is the scenario or incident? What is harmed?**	**What makes it possible?**
Nurse	Nurse stores or transmits ESUMS data on irregular media (e.g. local backup, transmitting data by email ...). Confidential data leaks to 3rd party due to accidental disclosure.	Work process not aligned with policy. Lack of competence.

Network failure;
hardware failure;
software failure
	Failure on nurse workstation (network, hardware, software) leading to loss of availability to ESUMS system.	Immature technology; unstable connection

Table 5 - High-level risk identification w.r.t. nurse workstation

Who/what causes it?	**How? What is the scenario or incident? What is harmed?**	**What makes it possible?**
Network provider	Loss of internet connection/mobile network, affecting the availability of ESUM data	Dependence on 3rd party network provider. Unreliable network connection.
Network provider	Data transmission from server to workstation is interrupted, affecting the Service Provisioning due to lack of availability of ESUMS data	Dependence on 3rd party network provider. Unreliable network connection.
Hacker	Hacker breaks in to system, leading to leakage of ESUMS data or loss of integrity.	Insufficient network security.
Virus / malware	Virus or other malware infects ESUMS system via surrounding systems and networks.	Insufficient malware protection.
Telephone company; acts of nature	Phone lines for user support goes down (service provider, nurse, patient)	Dependence on 3rd party telecom provider; lack of redundant communication systems

Table 6 - High-level risk identification w.r.t. environment/external factors

2.5 Scales and Evaluation Criteria

A risk is the likelihood of an unwanted incident and its consequence for a specific asset, where an unwanted incident is an event that harms or reduces the value of an asset. The risk level is the level or value of a risk as derived from its likelihood and consequence. In order to estimate and evaluate risks, we therefore need scales of applicable likelihood and consequence values, we need a function to map combinations of likelihood and consequence to risk level, and we need criteria for determining which risk levels are acceptable and which are not. The scales and risk evaluation criteria for the ESUMS risk analysis are documented in this section.

2.5.1 Consequence Scales

For each asset we use a qualitative consequence scale of five values ranging from *insignificant* to *catastrophic*. Because consequences are of a different kind for the different assets we define one scale for each asset. However, at a general level the different consequences – such as *minor*, *moderate* and *catastrophic* – should denote the same degree of harm of severity independent of the asset in question. Therefore, before defining the consequence scale for each asset we indicate how to understand each value in general, as shown in Table 7. The purpose of these descriptions of consequences is to give a general interpretation, independent of the specific assets. The consequence scales for each of the specific assets should harmonize with this general interpretation.

Consequence	Generic interpretation
Catastrophic	Can potentially put the service provider out of business
Major	Failure to recover can potentially put the service provider out of business
Moderate	Several occurrences over time can potentially put the service provider out of business
Minor	Tolerable if easy to recover from or if not very frequent
Insignificant	Generally tolerable and easy to manage or recover from

Table 7 - Consequence scales: General interpretation from the (chosen) viewpoint of the service provider

The consequence scale for the direct asset *ESUMS data security* is shown in Table 8. Note that impact on ESUMS data in this case study means impact on confidentiality, integrity or availability of ESUMS data.

Consequence	Description
Catastrophic	Severe security breach affecting ESUMS data of most patients (E.g. loss of confidentiality of personal data for most patients)
Major	Significant security breach affecting ESUMS data of most patients
Moderate	Significant security breach affecting ESUMS data if some patients
Minor	Limited security breach
Insignificant	Little or no impact on ESUMS data

Table 8 - Consequence scale: ESUMS data security

Note that the above descriptions (Table 8) have been given with little detail as the consequence depends to some extent on what is needed to recover and on the degree of which the security breach has been exploited. From a service provider's perspective it would be catastrophic if just one patient's data was, for example, accidentally compromised, as it may make the new headlines and hence attracted the (negative) attention of a whole society. However, from an engineering perspective, the resources required to find the error might be small. Parameters that affect consequence hence include both number of patients and volumes of data affected, and degree of exploitation of the security breach, by general press or a person with malicious intent.

The consequence scale for the direct asset *Service Provisioning* is shown in Table 9.

Consequence	Description
Catastrophic	Severe impact on services to most users E.g. no users can access ESUMS for two days or more and/or ESUMS data are completely corrupted for two days or more
Major	Significant impact on services to many users E.g. users cannot access system for up to two days
Moderate	Significant impact on services to some users E.g. users cannot access system for up to two days
Minor	Limited impact on services to some users E.g. users experience weekly problems
Insignificant	Little or no impact on services to a few users E.g. users experience smaller problems / annoyances twice a month

Table 9 - Consequence scale: Service provisioning

The consequence scale for the direct asset *Compliance* is shown in Table 10. Note that each consequence will typically include the lower consequences. In ESUMS it would be the national health authorities and the data protection inspectorate that enforce the regulations.

Consequence	**Description**
Catastrophic	Processing of personal data ordered to cease
Major	Criminal liability and fine
Moderate	Enforcement notice
Minor	Information notice
Insignificant	Minor compliance breach discovered and corrected

Table 10 - Consequence scale: Compliance

The consequence scale for the indirect asset *Patient quality of life* is shown in Table 11. Note that consequences should be as compared with traditional health or welfare services, i.e. consequences that could be prevented with traditional health of welfare services.

Consequence	**Description**
Catastrophic	Severe impact on quality of life for more than half of patients E.g. acute hospitalization and/or continuous high stress and frustration level
Major	Significant impact on quality of life for most patients E.g. patients feel unsafe only being monitored at home
Moderate	Many patients worry frequently about own health and the quality of care provided
Minor	Some patients experience minor worries and stress levels
Insignificant	Little or no impact on quality of life for most patients

Table 11 - Consequence scale: Patient quality of life

The consequence scale for the indirect asset *Patient trust* is shown in Table 12.

Consequence	**Description**
Catastrophic	Complete distrust by most patients
Major	Many patients refuse to continue using the services
Moderate	Some patients refuse to continue using the services
Minor	Some patients get reluctant to continue using the services
Insignificant	No impact on trust of most patients

Table 12 - Consequence scale: Patient trust

The consequence scale for the indirect asset *Customer trust* is shown in Table 13.

Consequence	**Description**
Catastrophic	Severe loss of customer trust E.g. most of patients are removed from services and future tenders are lost
Major	Significant loss of customer trust E.g. half of patients are removed from services; future tenders may be lost
Moderate	Some loss of customer trust E.g. renewal of tender may be jeopardised
Minor	Minor loss of customer trust E.g. swift and visible improvement will recover the customer trust
Insignificant	Little or no impact on customer trust

Table 13 - Consequence scale: Customer trust

The consequence scale for the indirect asset *Cost effectiveness* is shown in Table 14. Examples of costs include:

- hospitalization
- need for more training of patients and/or nurses due to usability issues
- faulty components/technology; extra expenses
- maintenance costs

The cost effectiveness of the ESUMS system is in particular compared with the alternative of offering traditional health care services instead of using monitoring. The costs of offering the ESUMS services should be justifiable as compared to traditional services.

Consequence	Description
Catastrophic	Services are terminated due to unjustifiable costs
Major	Costs justifiable only after indefinite period of time
Moderate	Some excess in cost w.r.t several patients
Minor	Minor excess in cost w.r.t. some patients
Insignificant	Little or no impact on expected cost effectiveness

Table 14 - Consequence scale: Cost effectiveness

2.5.2 Likelihood Scale

Likelihoods are assigned to unwanted incidents as part of the risk estimation, but also to threat scenarios to understand the most important sources of risk. One likelihood scale is defined for all scenarios and incidents as shown in Table 15. The likelihood scale for the ESUMS case study is qualitative and based on frequencies.

Likelihood value	Description
Certain	A very high number of similar incidents already on record; has been experienced a very high number of times by the same actor
Likely	A significant number of similar incidents already on record; has been experienced a significant number of times by the same actor
Possible	Several similar incidents on record; has been experienced more than once by the same actor
Rare	Only very few similar incidents on record; has been experienced by few actors
Unlikely	Never experienced by most actors throughout the total lifetime of the system

Table 15 - Likelihood scale

2.5.3 Risk Evaluation Criteria

The risk evaluation criteria are a specification of the levels of risk that the party of the analysis is willing to accept. For the identified risks, the risk evaluation involves comparing the risks and their risk levels with the risk evaluation criteria in order to determine which risks need to be considered for treatment and mitigation.

Before the risk evaluation criteria can be specified, the risk function needs to be defined. A risk function is a mapping from a combination of a likelihood and consequence to a risk level. Given our likelihood and consequence scale of five levels, a convenient way of defining the risk function is by using a matrix. The risk function for the ESUMS analysis is given in Table 16 and gives a mapping to one of the risk levels *acceptable* and *unacceptable* (shaded area).

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Unlikely					▨
	Rare				▨	▨
	Possible			▨	▨	▨
	Likely			▨	▨	▨
	Certain		▨	▨	▨	▨

Table 16 - Risk function

The risk evaluation criteria are the following:

- Acceptable: The risk level is tolerable
- Unacceptable: The risks of this level need to be evaluated further for possible treatment

Note that for any risk, independent of the risk level, the question of treatment is a question of cost and benefit; if the cost of mitigating it is higher than the gain of risk reduction, the treatment option in question cannot be justified. Hence, even risks that in the first place are unacceptable must be evaluated with respect to the treatment options that are identified.

3 Risk Identification

The objective of this step is to identify the risks that must be managed as well as to determine where, when, why and how they may occur. It was conducted as a brainstorming session involving two members of the target team. The assets and the results from the high-level analysis were used as a starting point. The risks were gradually identified by identifying the unwanted incidents, threats, threat scenarios and vulnerabilities. The risk identification was conducted with respect to the target description, and the results were documented on-the-fly by drawing CORAS threat diagrams as the information was gathered.

Figure 6 through Figure 20 show the threat diagrams developed as a part of risk identification. First, risks related to patients at home are presented in Section 3.1. Then, risks related to ESUMS server are presented in Section 3.2. The risks related to nurse workstation are presented in Section 3.3. Finally, the risks related to the infrastructure are presented in Section 3.4.

3.1 Risks Related to Patients at Home

This section presents the threat diagrams addressing the risks at the home of a patient. Most of the identified risks are related to the use of the belt or the handheld, as well as software and hardware failures.

A threat diagram addressing the risks related to the use of belt at home is shown in Figure 6. The patient initiates the threat scenarios due to, for example, lack of training or lack of routines. The resulting unwanted incidents, which harm all of the direct assets, are shown on the right hand side of Figure 6.

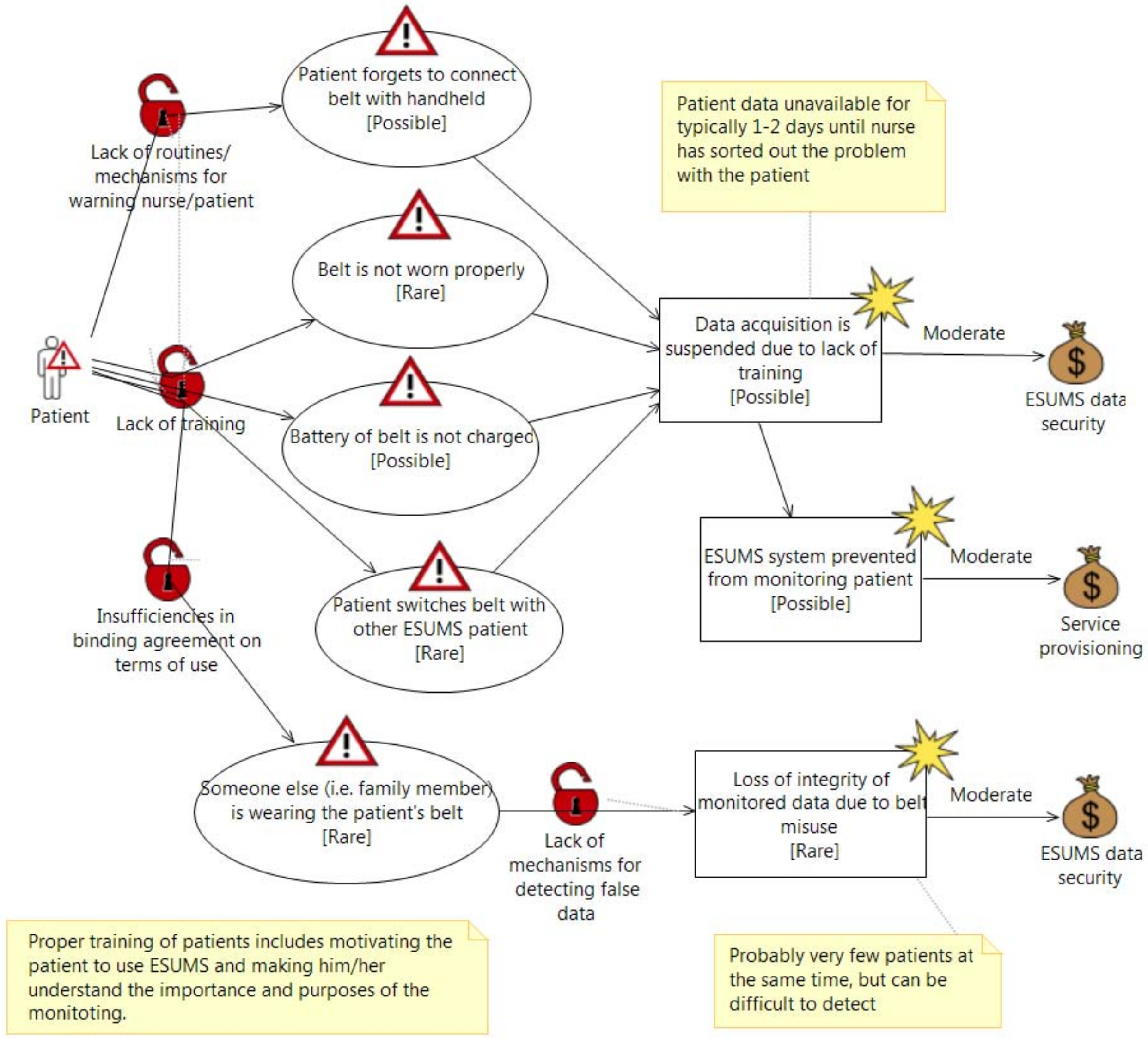

Patient forgets to connect belt with handheld [Possible]
Lack of routines/ mechanisms for warning nurse/patient
Belt is not worn properly [Rare]
Patient
Lack of training
Battery of belt is not charged [Possible]
Patient switches belt with other ESUMS patient [Rare]
Insufficiencies in binding agreement on terms of use
Someone else (i.e. family member) is wearing the patient's belt [Rare]
Lack of mechanisms for detecting false data
Patient data unavailable for typically 1-2 days until nurse has sorted out the problem with the patient
Data acquisition is suspended due to lack of training [Possible]
Moderate
ESUMS data security
ESUMS system prevented from monitoring patient [Possible]
Moderate
Service provisioning
Loss of integrity of monitored data due to belt misuse [Rare]
Moderate
ESUMS data security
Proper training of patients includes motivating the patient to use ESUMS and making him/her understand the importance and purposes of the monitoting.
Probably very few patients at the same time, but can be difficult to detect

Figure 6 - Threat diagram addressing risks related to use of belt at home

A threat diagram addressing the risks related to the handheld is shown in Figure 7. The patient initiates the threat scenarios due to lack of training or lack of alerts. The resulting unwanted incidents, which harm data security or service provisioning, are shown on the right hand side.

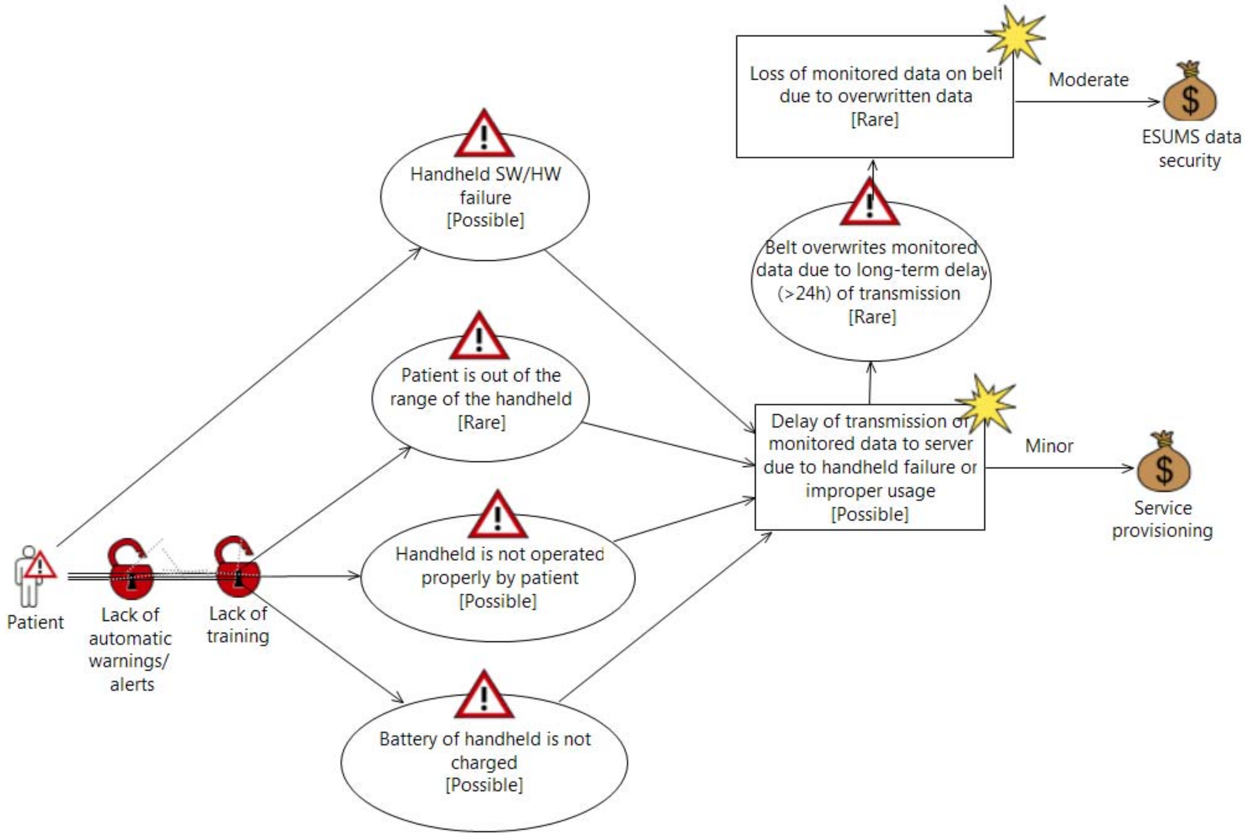

Loss of monitored data on belt due to overwritten data [Rare]
Moderate
ESUMS data security
Handheld SW/HW failure [Possible]
Belt overwrites monitored data due to long-term delay (>24h) of transmission [Rare]
Patient is out of the range of the handheld [Rare]
Delay of transmission of monitored data to server due to handheld failure or improper usage [Possible]
Minor
Service provisioning
Handheld is not operated properly by patient [Possible]
Patient
Lack of automatic warnings/ alerts
Lack of training
Battery of handheld is not charged [Possible]

Figure 7- Threat diagram addressing risks related to handheld

A threat diagram addressing the risks related to the software application installed on the handheld is shown in Figure 8. The patient initiates the threat scenarios shown due to lack of training. The resulting unwanted incident, harming ESUMS data security, is shown on the right hand side.

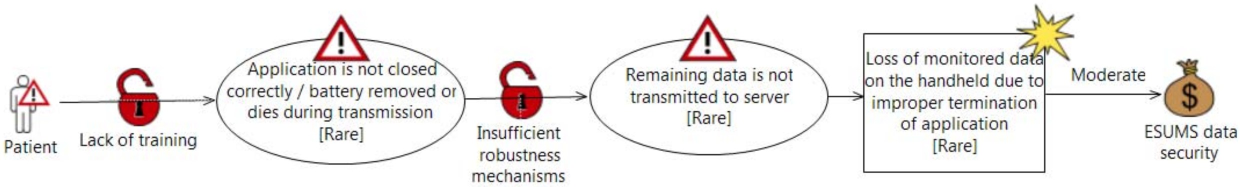

Patient
Lack of training
Application is not closed correctly / battery removed or dies during transmission [Rare]
Insufficient robustness mechanisms
Remaining data is not transmitted to server [Rare]
Loss of monitored data on the handheld due to improper termination of application [Rare]
Moderate
ESUMS data security

Figure 8 - Threat diagram addressing a risk related to SW application on the handheld

A threat diagram addressing the risks related to software and hardware failures at home is shown in Figure 9. Failure of network, handheld or belt initiates the shown threat scenarios. The resulting unwanted incident, harming service provisioning and data security, is shown on the right hand side.

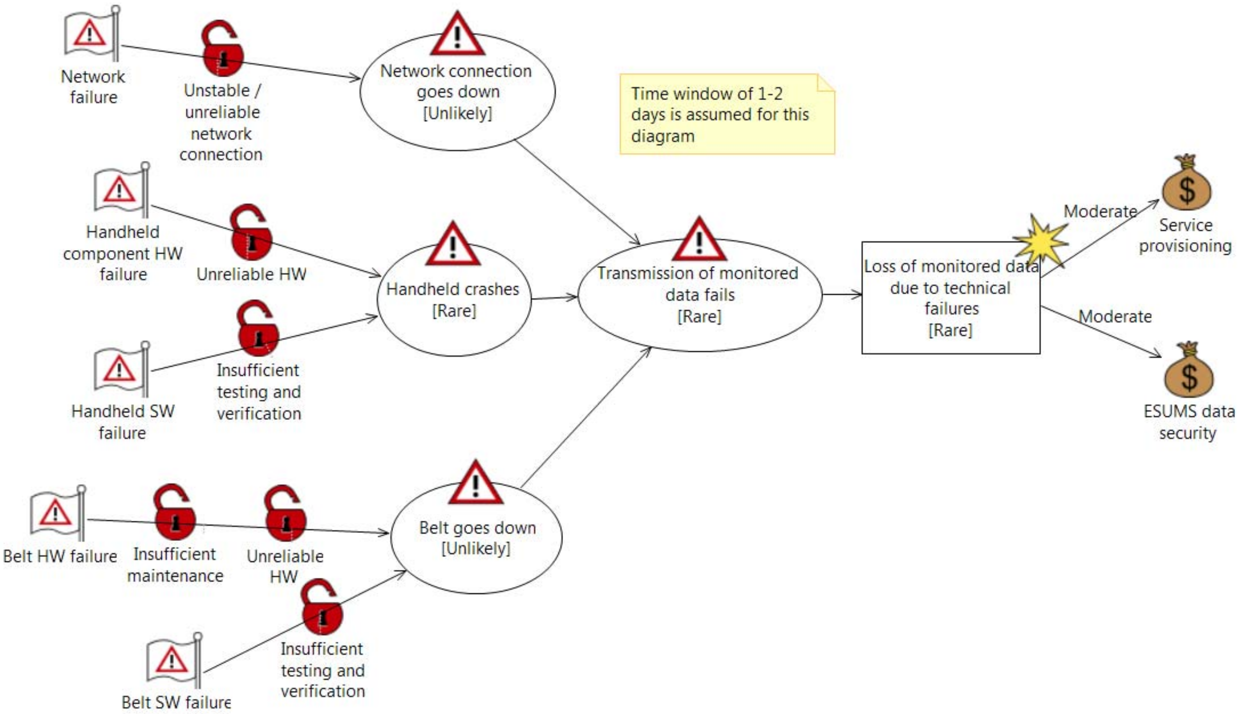

Network failure
Unstable / unreliable network connection
Network connection goes down [Unlikely]
Time window of 1-2 days is assumed for this diagram
Handheld component HW failure
Unreliable HW
Handheld crashes [Rare]
Handheld SW failure
Insufficient testing and verification
Transmission of monitored data fails [Rare]
Loss of monitored data due to technical failures [Rare]
Moderate
Service provisioning
Moderate
ESUMS data security
Belt HW failure
Insufficient maintenance
Unreliable HW
Belt goes down [Unlikely]
Belt SW failure
Insufficient testing and verification

Figure 9 - Threat diagram addressing risks related to SW and HW failures at home

A threat diagram addressing the risks related to misuse of belt or tampering with configuration file is shown in Figure 10. Insufficiencies in configuration file or the agreement on terms of use initiate the shown threat scenarios. The resulting unwanted incidents, which harm ESUMS data security, are shown on the right hand side of Figure 10.

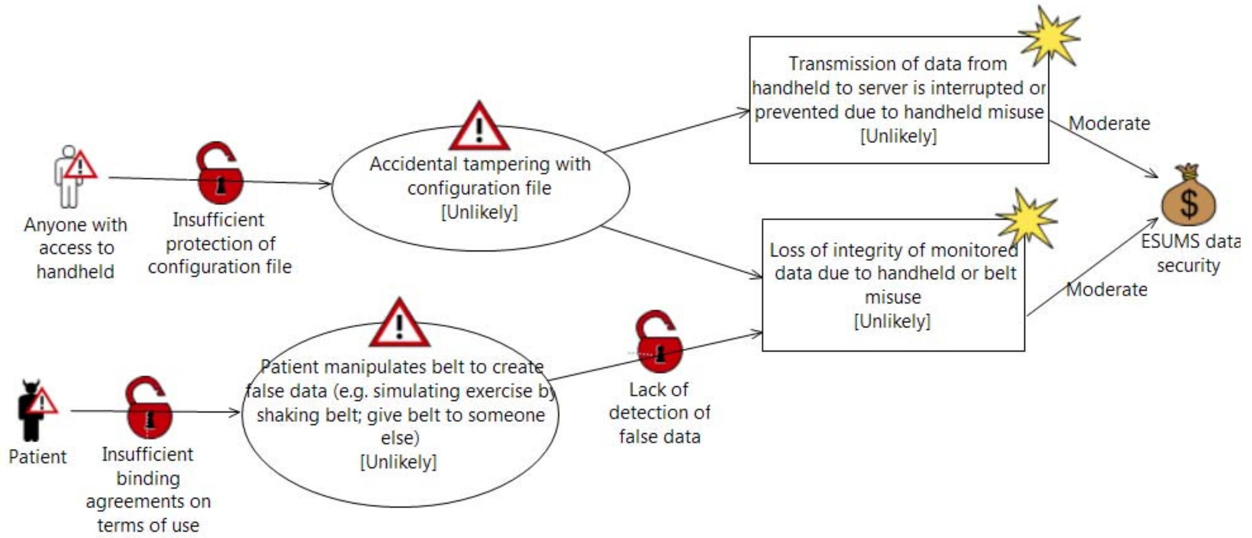

Transmission of data from handheld to server is interrupted or prevented due to handheld misuse [Unlikely]
Anyone with access to handheld
Insufficient protection of configuration file
Accidental tampering with configuration file [Unlikely]
Moderate
ESUMS data security
Loss of integrity of monitored data due to handheld or belt misuse [Unlikely]
Moderate
Patient
Insufficient binding agreements on terms of use
Patient manipulates belt to create false data (e.g. simulating exercise by shaking belt; give belt to someone else) [Unlikely]
Lack of detection of false data

Figure 10 - Threat diagram addressing risks related to misuse of belt or tampering with config file

A threat diagram addressing the risks related to configuration file on the handheld is shown in Figure 11. Insufficiencies in protection of configuration file or quality assurance may be exploited to initiate the shown threat scenarios. The resulting unwanted incidents, harming ESUMS data security, are shown on the right hand side of the figure.

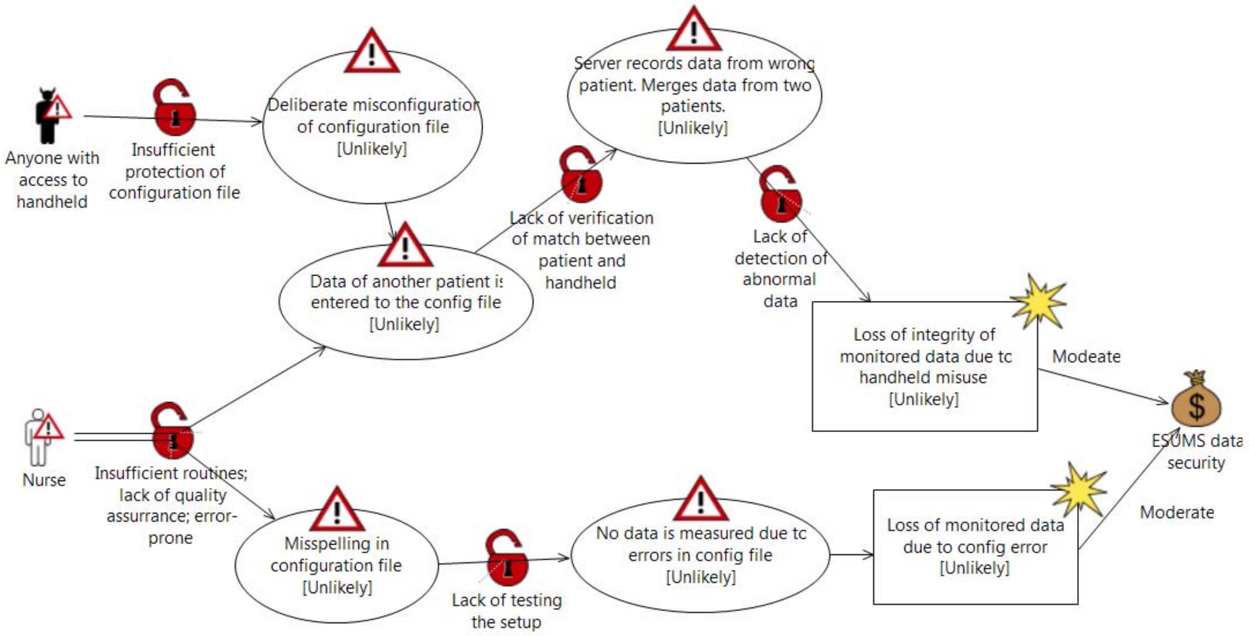

Anyone with access to handheld
Insufficient protection of configuration file
Deliberate misconfiguratior of configuration file [Unlikely]
Server records data from wrong patient. Merges data from two patients. [Unlikely]
Lack of verification of match between patient and handheld
Lack of detection of abnormal data
Data of another patient is entered to the config file [Unlikely]
Loss of integrity of monitored data due tc handheld misuse [Unlikely]
Modeate
ESUMS data security
Nurse
Insufficient routines; lack of quality assurrance; error-prone
Misspelling in configuration file [Unlikely]
Lack of testing the setup
No data is measured due tc errors in config file [Unlikely]
Loss of monitored data due to config error [Unlikely]
Moderate

Figure 11- Threat diagram addressing risks related to config file on the handheld

A threat diagram addressing the risks related to the questionnaire answering (in SW application installed on the handheld) is shown in Figure 12. Insufficiencies in agreement on terms of use or lack of training may open for the shown threat scenarios. The resulting unwanted incidents, which harm ESUMS data security, are shown on the right hand side.

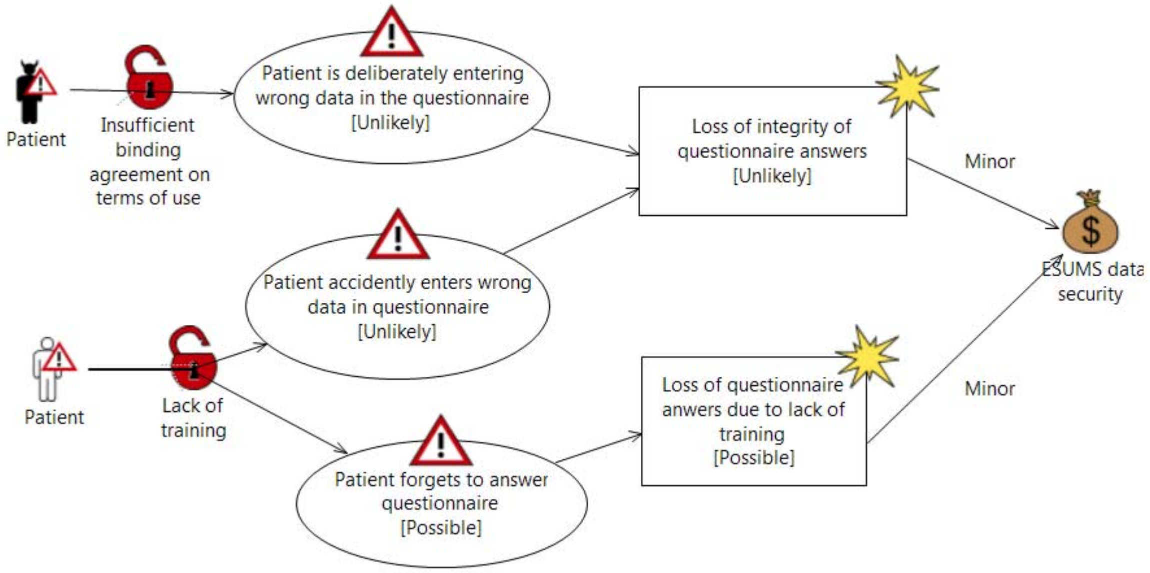

Patient
Insufficient binding agreement on terms of use
Patient is deliberately entering wrong data in the questionnaire [Unlikely]
Loss of integrity of questionnaire answers [Unlikely]
Minor
ESUMS data security
Patient accidently enters wrong data in questionnaire [Unlikely]
Patient
Lack of training
Loss of questionnaire anwers due to lack of training [Possible]
Minor
Patient forgets to answer questionnaire [Possible]

Figure 12- Threat diagram addressing risks related to the questionnaire answering (in SW application installed on the handheld)

3.2 Risks Related to the ESUMS Server

This section presents the threat diagrams addressing the risks related to the ESUMS server. The risks may be related to break-in or malware on the ESUMS server, misconfiguration, change of data, or lack of scalability of the server.

A threat diagram addressing the risks related to misconfiguration, user data change or change of monitored data, on the ESUMS server, is shown in Figure 13. Insufficiencies in security monitoring, policy or security training of system administrator initiate the shown threat scenarios. The resulting unwanted incidents may harm all of the direct assets as shown on the right hand side of the diagram.

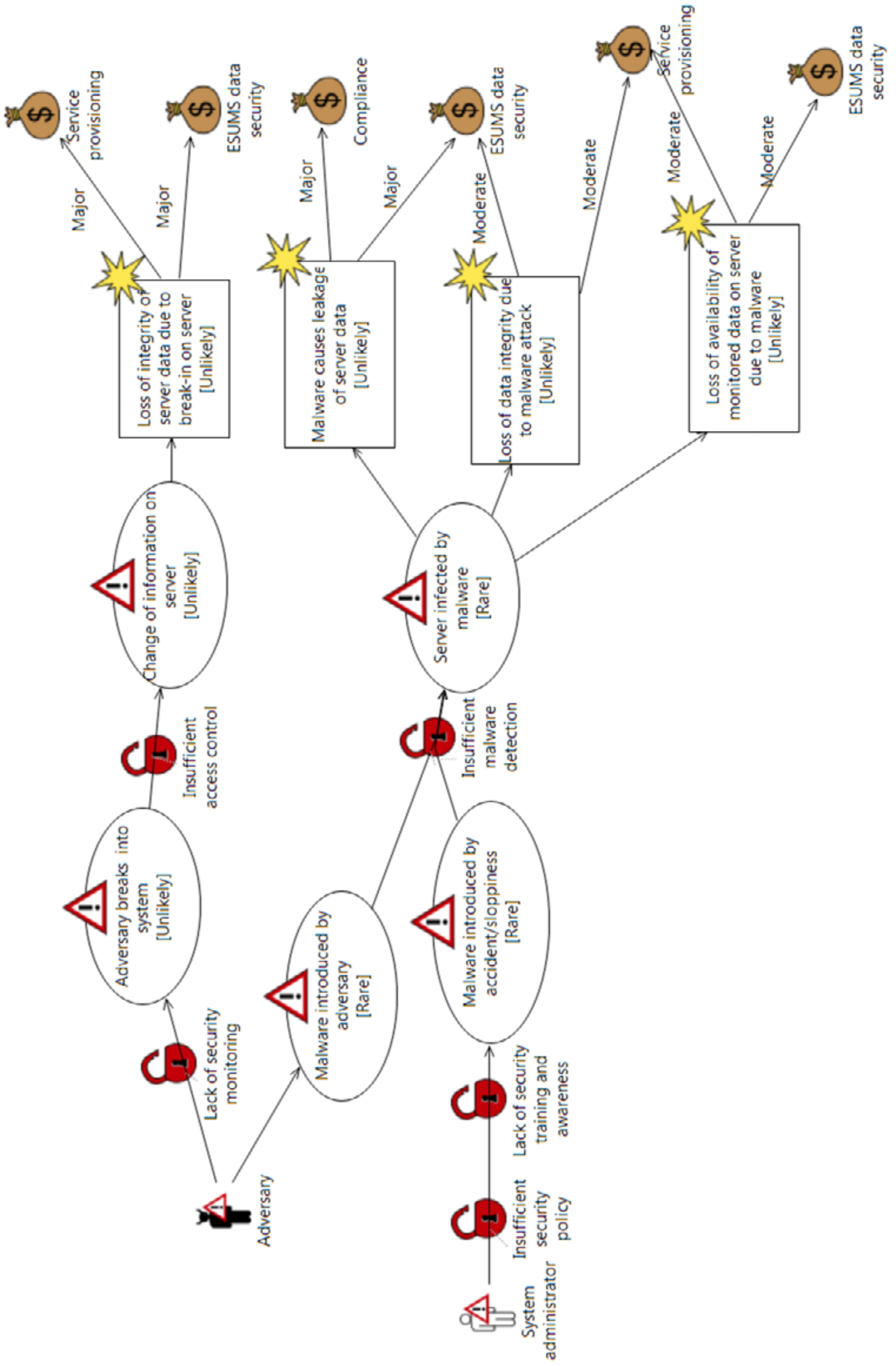

Adversary
System administrator
Lack of security monitoring
Insufficient security policy
Lack of security training and awareness
Adversary breaks into system [Unlikely]
Malware introduced by adversary [Rare]
Malware introduced by accident/sloppiness [Rare]
Insufficient access control
Insufficient malware detection
Change of information on server [Unlikely]
Server infected by malware [Rare]
Loss of integrity of server data due to break-in on server [Unlikely]
Malware causes leakage of server data [Unlikely]
Loss of data integrity due to malware attack [Unlikely]
Loss of availability of monitored data on server due to malware [Unlikely]
Major
Major
Major
Major
Moderate
Moderate
Moderate
Moderate
Service provisioning
ESUMS data security
Compliance
ESUMS data security
Service provisioning
ESUMS data security

Figure 13 - Threat diagram addressing risks related to the break-in or malware on the ESUMS server

A threat diagram addressing the risks related to misconfiguration, user data change or change of monitored data on the ESUMS server is shown in Figure 14. Insufficiencies in logging and authentication and lack of data verification, initiate the shown threat scenarios. The resulting unwanted incidents may harm all of the direct assets.

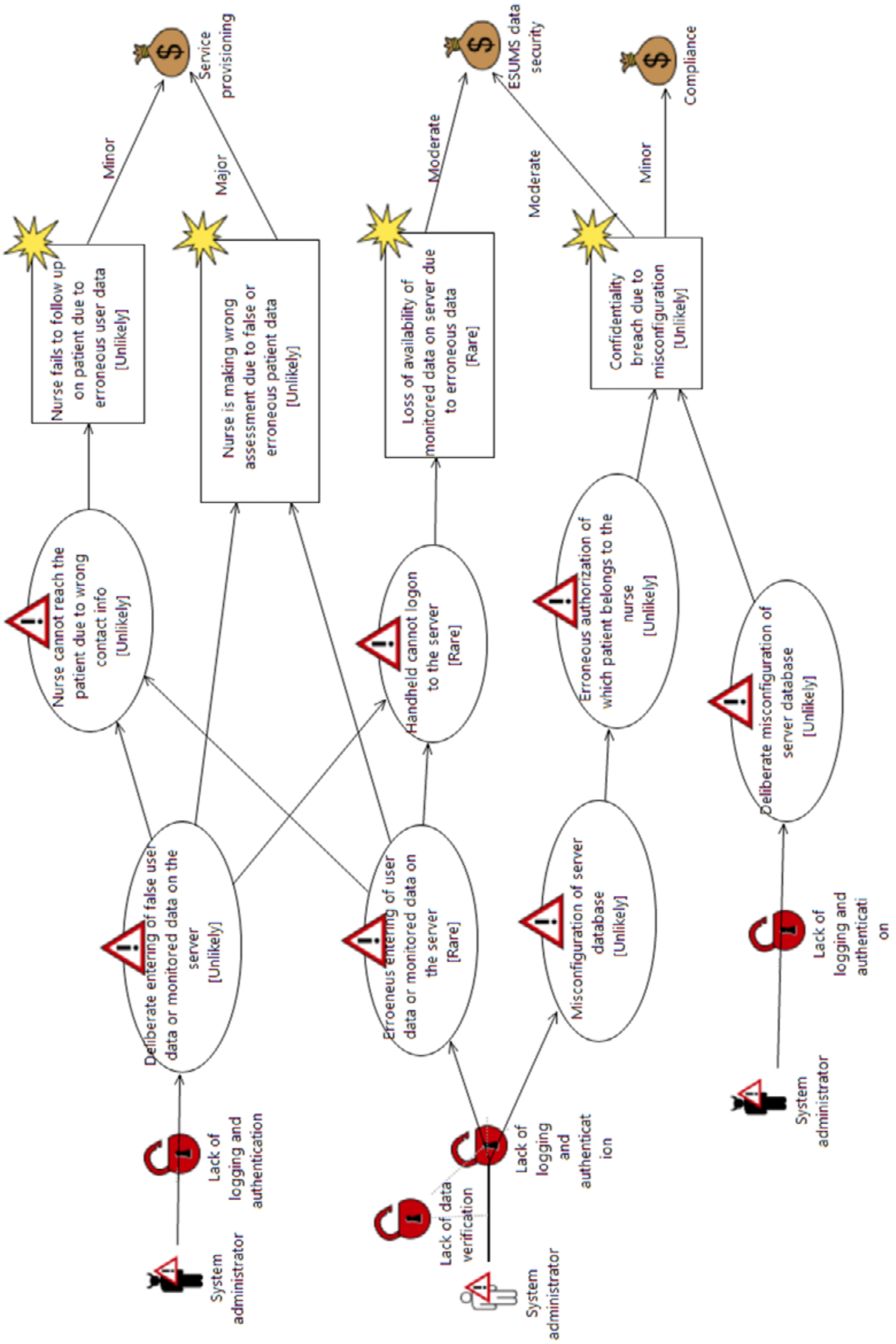

System administrator
Lack of logging and authentication
Deliberate entering of false user data or monitored data on the server [Unlikely]
Lack of data verification
System administrator
Lack of logging and authentication
Erroneus entering of user data or monitored data on the server [Rare]
Misconfiguration of server database [Unlikely]
System administrator
Lack of logging and authentication
Deliberate misconfiguration of server database [Unlikely]
Nurse cannot reach the patient due to wrong contact info [Unlikely]
Handheld cannot logon to the server [Rare]
Erroneous authorization of which patient belongs to the nurse [Unlikely]
Nurse fails to follow up on patient due to erroneous user data [Unlikely]
Nurse is making wrong assessment due to false or erroneous patient data [Unlikely]
Loss of availability of monitored data on server due to erroneous data [Rare]
Confidentiality breach due to misconfiguration [Unlikely]
Minor
Major
Moderate
Moderate
Minor
Service provisioning
ESUMS data security
Compliance

Figure 14 - Threat diagram addressing risks related to misconfiguration, user data change or change of monitored data, on the ESUMS server

A threat diagram addressing the risks related to lack of scalability on the ESUMS server is shown in Figure 15. Lack of stress testing and unknown server capacity initiate the shown threat scenarios. The resulting unwanted incidents, which harm data security of service provisioning, are shown on the right hand side of

Figure 15. The threat scenario *Server goes down* is included to document further sources of risk, but the causes are not investigated further as the scenario is not related to risks that are specific for ESUMS.

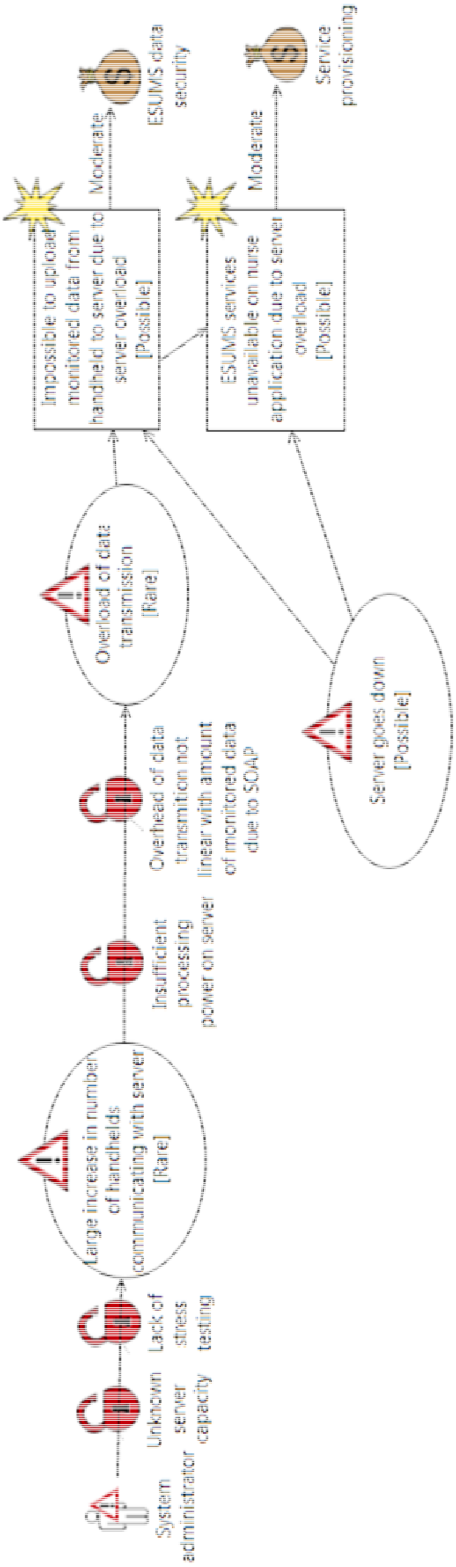

System administrator
Unknown server capacity
Lack of stress testing
Large increase in number of handhelds communicating with server [Rare]
Insufficient processing power on server
Overhead of data transmition not linear with amount of monitored data due to SOAP
Overload of data transmission [Rare]
Server goes down [Possible]
Impossible to upload monitored data from handheld to server due to server overload [Possible]
ESUMS services unavailable on nurse application due to server overload [Possible]
Moderate
Moderate
ESUMS data security
Service provisioning

Figure 15 - Threat diagram addressing risks related to lack of scalability on the ESUMS server

3.3 Risks Related to the Nurse Workstation

This section presents the threat diagrams addressing the risks related to the nurse workstation. The risks may be related to leakage of information from the nurse application, the ability of a nurse to follow up a patient exposed to an incident, or to leakage of a celebrity patient info by a nurse.

A threat diagram addressing the risks related to leakage of information from nurse application is shown in Figure 16. Lack of usability of the nurse application and insufficient work process alignment with policy, initiate the shown threat scenarios. The resulting unwanted incident, which harms compliance and data security, is shown on the right hand side.

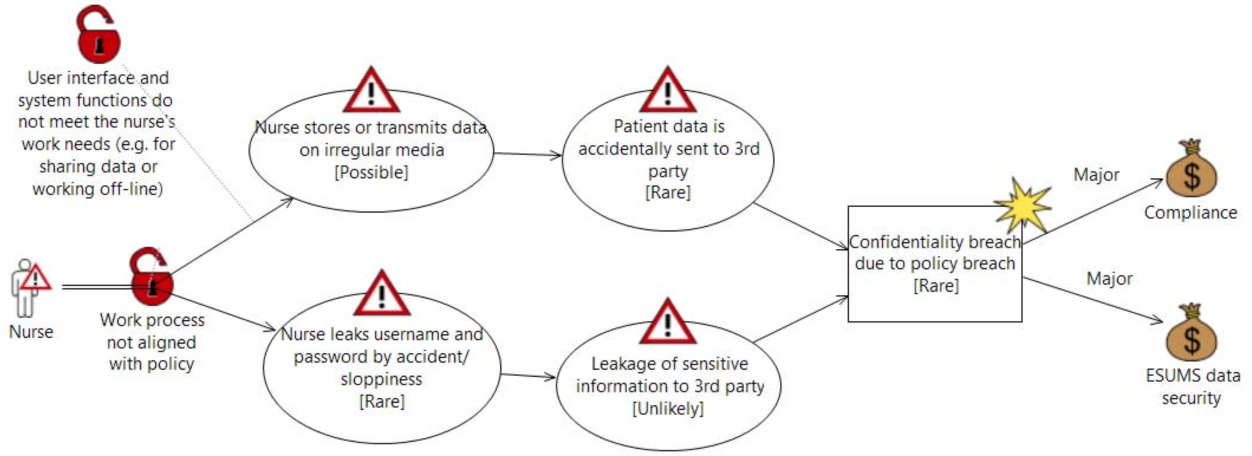

User interface and system functions do not meet the nurse's work needs (e.g. for sharing data or working off-line)
Nurse
Work process not aligned with policy
Nurse stores or transmits data on irregular media [Possible]
Nurse leaks username and password by accident/ sloppiness [Rare]
Patient data is accidentally sent to 3rd party [Rare]
Leakage of sensitive information to 3rd party [Unlikely]
Confidentiality breach due to policy breach [Rare]
Major
Major
Compliance
ESUMS data security

Figure 16 - Threat diagram addressing risks related to leakage of information from nurse application

A threat diagram addressing the risks related to the ability of a nurse to follow up a patient exposed to an incident is shown in Figure 17. Lack of quality assurance, lack of training, too high workload and insufficient routines are among the vulnerabilities which initiate the shown threat scenarios. The resulting unwanted incident, which harms the service provisioning, is shown to the right.

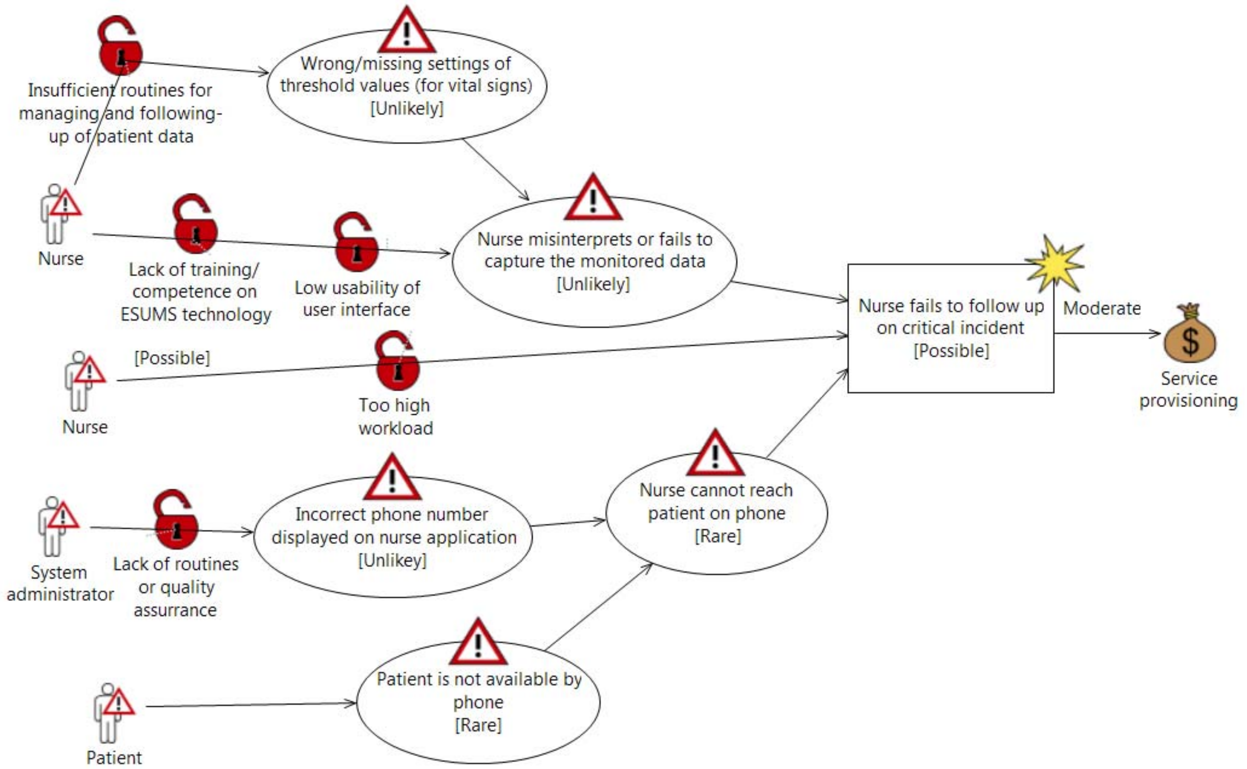

Insufficient routines for managing and following-up of patient data
Wrong/missing settings of threshold values (for vital signs) [Unlikely]
Nurse
Lack of training/ competence on ESUMS technology
Low usability of user interface
Nurse misinterprets or fails to capture the monitored data [Unlikely]
Nurse fails to follow up on critical incident [Possible]
Moderate
Service provisioning
[Possible]
Nurse
Too high workload
System administrator
Lack of routines or quality assurrance
Incorrect phone number displayed on nurse application [Unlikey]
Nurse cannot reach patient on phone [Rare]
Patient is not available by phone [Rare]
Patient

Figure 17 - Threat diagram addressing risks related to the ability of a nurse to follow up a patient exposed to an incident

A threat diagram addressing the risks related to leakage of a celebrity patient info by a nurse is shown in Figure 18. Insufficient logging and access control may be exploited to initiate the shown threat scenarios. The resulting unwanted incident, which harms the ESUMS data security, is shown on the right hand side of the figure.

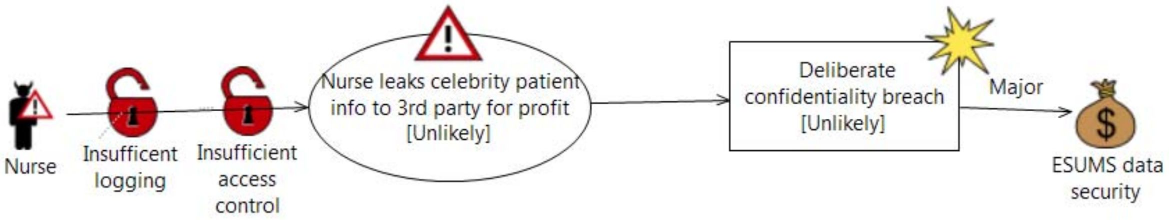

Nurse
Insuffcient logging
Insufficient access control
Nurse leaks celebrity patient info to 3rd party for profit [Unlikely]
Deliberate confidentiality breach [Unlikely]
Major
ESUMS data security

Figure 18 - Threat diagram addressing risks related to leakage of a celebrity patient info, by a nurse

3.4 Risks Related to the Infrastructure

This section presents the threat diagrams addressing the risks related to the infrastructure. The risks may be related to failure of desktop application, or risks caused by server maintenance.

A threat diagram addressing the risks related to failure of desktop application due to maintenance is shown in Figure 19. Lack of operational documentation, misconfigured workstation or insufficient testing are vulnerabilities which may be exploited to initiate the shown threat scenarios. The resulting unwanted incidents, which harm the service provisioning and ESUMS data security, are shown to the right.

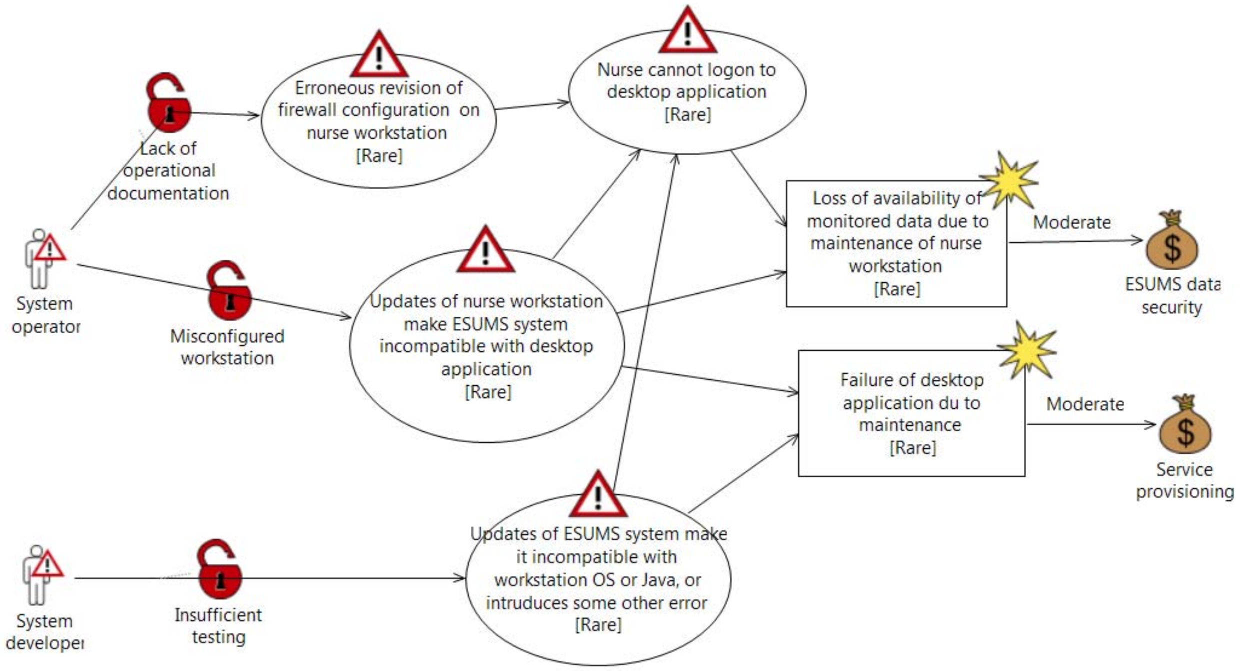

Erroneous revision of firewall configuration on nurse workstation [Rare]
Nurse cannot logon to desktop application [Rare]
Lack of operational documentation
System operator
Misconfigured workstation
Updates of nurse workstation make ESUMS system incompatible with desktop application [Rare]
Loss of availability of monitored data due to maintenance of nurse workstation [Rare]
Moderate
ESUMS data security
Failure of desktop application du to maintenance [Rare]
Moderate
Service provisioning
Updates of ESUMS system make it incompatible with workstation OS or Java, or intruduces some other error [Rare]
System developer
Insufficient testing

Figure 19 - Threat diagram addressing risks related to failure of desktop application, due to maintenance

A threat diagram addressing the risks caused by server maintenance is shown in Figure 20. Lack of operational documentation and insufficient testing are the vulnerabilities which may be exploited to initiate the shown threat scenarios. The resulting unwanted incidents, harming service provisioning and data security, are shown on the right hand side of the diagram.

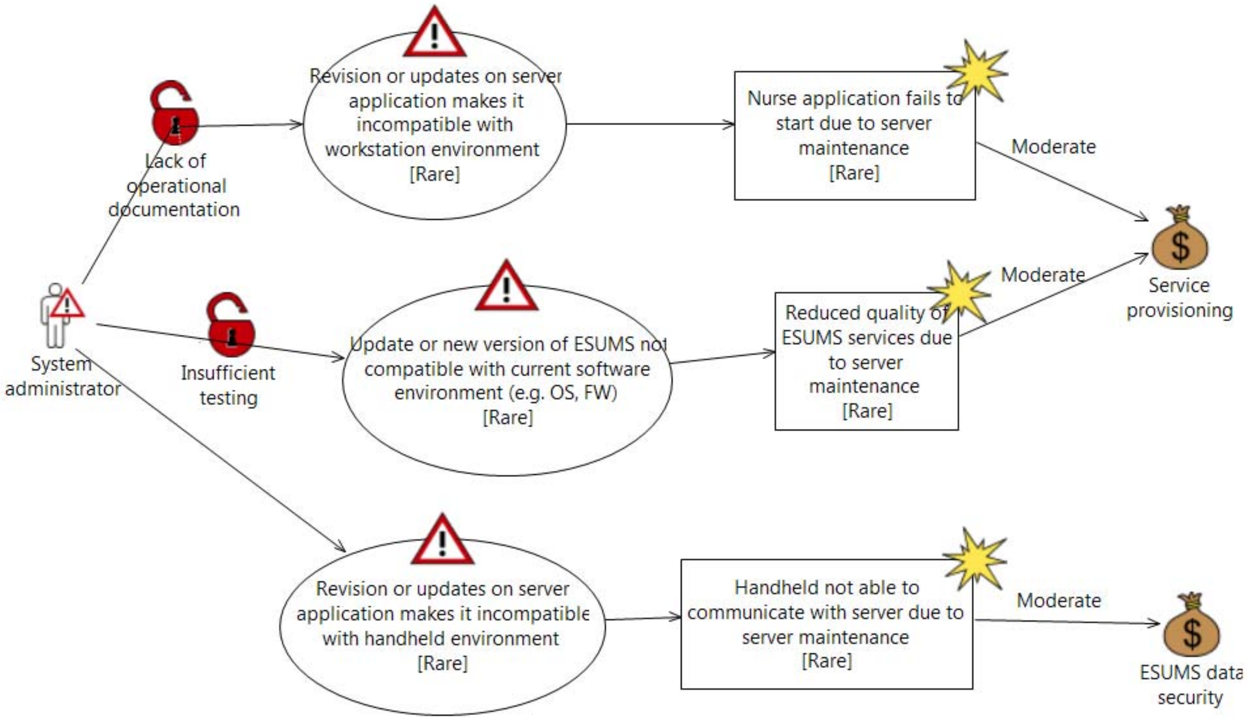

Revision or updates on server application makes it incompatible with workstation environment [Rare]
Nurse application fails to start due to server maintenance [Rare]
Lack of operational documentation
Moderate
Service provisioning
System administrator
Insufficient testing
Update or new version of ESUMS not compatible with current software environment (e.g. OS, FW) [Rare]
Moderate
Reduced quality of ESUMS services due to server maintenance [Rare]
Revision or updates on server application makes it incompatible with handheld environment [Rare]
Handheld not able to communicate with server due to server maintenance [Rare]
Moderate
ESUMS data security

Figure 20 - Threat diagram addressing risks caused by server maintenance

4 Risk Estimation

The objective of this phase is to determine the risk level of the identified risks. The phase is conducted as a workshop involving the target team. The threat scenarios and the unwanted incidents are annotated with likelihoods based on input from the target team. Each relation between an unwanted incident and an asset is annotated with the consequence describing the impact of the incident on the asset. Risk levels are documented using CORAS risk diagrams modelling each of the identified risks and their risk values as calculated from the estimated likelihoods and consequences.

The input to this phase is the CORAS threat diagrams from the risk identification phase, the likelihood scale, the consequence scales, and the risk function defined in Table 7 through Table 16. The output of this phase is the CORAS threat diagrams completed with a likelihood assigned to each unwanted incident and a consequence assigned to each relation between an unwanted incident and an asset. In addition, the output includes CORAS risk diagrams modelling the risks and their estimated risk levels.

In order to avoid repeating figures, the threat diagrams presented in Figure 6 through Figure 20 contain the likelihood and consequence estimates which are obtained from the risk estimation. Moreover, the consequences on the affected indirect assets are estimated.

As a part of the risk estimation, the consequence values of unwanted incidents on the relevant indirect assets are estimated. In order to avoid repetition, we refer to Table 17 through Table 20 for the consequence estimates.

5 Risk Evaluation

The main objective of the risk evaluation is to determine which risks need to be evaluated further for possible treatment. This is conducted by comparing the risk estimates documented in Section 4 with the risk evaluation criteria documented in Table 16 in Section 2. However, risks that in the first place are acceptable when considering them in isolation may still be unacceptable if each of them can be understood as an instance of a more general risk. For example, if several different incidents cause harm to integrity of information, it may be that the accumulated risk level with respect to integrity is unacceptable, even when each incident is acceptable when viewed in isolation. We therefore need to accumulate such risks as part of the risk evaluation.

In the next subsections we use a table format to summarise and give an overview of all risks and risk estimates. The first column is the unwanted incident, and the second column (#) is a unique number to index the incident. The third column (L) is the likelihood estimates where the numbers 1-5 denote the likelihood intervals from *Unlikely* to *Certain*. The columns 4-10 are the consequence estimates for each direct and indirect asset. DS denotes *ESUMS data security*, SP denotes *Service provisioning*, C denotes *Compliance*, CT denotes *Customer trust*, PT denotes *Patient trust*, QL denotes *Patient quality of life*, and CE denotes *Cost effectiveness*. For the consequence estimates, the numbers 1-5 denote the consequence values *Insignificant* to *Catastrophic*. A cell marked with a dash (-) denotes that the unwanted incident in question does not harm the asset in question.

Each cell in columns 4-10 with a consequence estimate hence represents a risk. We have marked with grey shading each cell that evaluates to an unacceptable risk level when comparing with the risk evaluation criteria.

5.1 Evaluation of Risks Related to Patients at Home

Table 17 gives an overview of all unwanted incidents related to patients at home together with the risk estimate for each asset that is harmed. There are three unwanted incidents that yield risks with unacceptable risk levels.

Unwanted incident	#	L	Consequence for each asset						
			DS	SP	C	CT	PT	QL	CE
Data acquisition is suspended due to lack of training	1	3	3	-	-	1	1	2	2
ESUMS system prevented from monitoring patient	2	3	-	3	-	-	3	3	3
Loss of integrity of monitored data due to belt misuse	3	2	3	-	-	2	1	2	2
Loss of monitored data on belt due to overwritten data	4	2	3	-	-	3	2	2	2
Delay of transmission of monitored data to server due to handheld failure or improper usage	5	3	-	2	-	-	1	2	2
Loss of monitored data on the handheld due to improper termination of application	6	2	3	-	-	1	1	2	2
Loss of monitored data due to technical failures	7	2	3	3	-	4	3	3	3
Transmission of data from handheld to server is interrupted or prevented due to handheld misuse	8	1	3	-	-	3	3	2	2
Loss of integrity of monitored data due to handheld or belt misuse	9	1	3	-	-	4	1	1	2
Loss of integrity of monitored data due to handheld misuse	10	1	3	-	-	-	3	2	2
Loss of monitored data due to config error	11	1	3	-	-	4	2	2	2
Loss of integrity of questionnaire answers	12	1	2	-	-	1	1	1	1
Loss of questionnaire answers due to lack of training	13	3	2	-	-	-	1	1	1

Table 17 - Overview of risk estimates: Patients at home

5.2 Evaluation of Risks Related to the ESUMS Server

Table 18 gives an overview of all unwanted incidents related to the ESUMS server together with the risk estimate for each asset that is harmed. There are two unwanted incidents that yield risks with unacceptable risk levels.

Unwanted incident	#	L	Consequence for each asset						
			DS	SP	C	CT	PT	QL	CE
Loss of integrity of server data due to break-in on server	14	1	4	4	-	4	4	2	4
Malware causes leakage of server data	15	1	4	-	4	4	4	2	4
Loss of data integrity due to malware attack	16	1	3	3	-	4	4	2	4
Loss of availability of monitored data on server due to malware	17	1	3	3	-	3	3	2	3
Nurse fails to follow up on patient due to erroneous user data	18	1	-	2	-	-	4	3	2
Nurse is making wrong assessment due to false or erroneous patient data	19	1	-	4	-	4	2	2	2
Loss of availability of monitored data on server due to erroneous data	20	2	3	-	-	2	3	2	2
Confidentiality breach due to misconfiguration	21	1	3	-	2	3	2	2	2
Impossible to upload monitored data from handheld to server due to server overload	22	3	3	-	-	4	3	2	4
ESUMS services unavailable on nurse application due to server overload	23	3	-	3	-	-	3	2	4

Table 18 - Overview of risk estimates: ESUMS Server

5.3 Evaluation of Risks Related to the Nurse Workstation

Table 19 gives an overview of all unwanted incidents related to the nurse workstation together with the risk estimate for each asset that is harmed. Two of the unwanted incidents yield risks with unacceptable risk levels.

Unwanted incident	#	L	Consequence for each asset						
			DS	SP	C	CT	PT	QL	CE
Confidentiality breach due to policy breach	24	2	4	-	4	4	2	2	4
Nurse fails to follow up on critical incident	25	3	-	3	-	4	4	4	2
Deliberate confidentiality breach	26	1	4	-	-	4	4	3	4

Table 19 - Overview of risk estimates: Nurse workstation

5.4 Evaluation of Risks Related to the Infrastructure

Table 20 gives an overview of all unwanted incidents related to the infrastructure together with the risk estimate for each asset that is harmed. Two of the unwanted incidents yield risks with unacceptable risk levels.

Unwanted incident	#	L	Consequence for each asset						
			DS	SP	C	CT	PT	QL	CE
Loss of availability of monitored data due to maintenance of nurse workstation	27	2	3	-	-	4	2	2	2
Failure of desktop application due to maintenance	28	2	-	3	-	-	2	2	3
Nurse application fails to start due to server maintenance	29	2	-	3	-	-	1	2	3
Reduced quality of ESUMS services due to server maintenance	30	2	-	3	-	-	3	3	3
Handheld not able to communicate with server due to server maintenance	31	2	3	-	-	4	2	2	2

Table 20 - Overview of risk estimates: Infrastructure

5.5 Evaluation of Accumulated Risks

There are in particular two kinds of incidents that each can be understood as a specific instance of a more general risk, namely incidents harming integrity of ESUMS data and incidents harming availability of ESUMS data.

Table 21 gives an overview of incidents that harm ESUMS data integrity. The accumulated likelihood and the accumulated consequence for each asset are given in the last row. Roughly speaking, the accumulated likelihood is the aggregate of the individual likelihoods. A precise aggregation of the likelihoods requires quantitative values as well as judgements about possible statistical relationships between the incidents. For this particular accumulation we did a rough estimate combined with the judgment of the target team. The consequence of the accumulated risk is roughly speaking the average of the individual consequences since each occurrence of the general risk is an occurrence of one of the specific instances. However, we need to consider the likelihoods to take into account that some of the specific instances are more typical than others. In practice, when an accumulated risk becomes unacceptable, treatment of the underlying risks (unwanted incidents which affect the assets involved) needs to be considered.

Considering the accumulated estimates, we see that the risk with respect to integrity is unacceptable for the asset *Service provisioning*.

Unwanted incident	**#**	**L**	**Consequence for each asset**						
			DS	**SP**	**C**	**CT**	**PT**	**QL**	**CE**
Loss of integrity of monitored data due to belt misuse	3	2	3	-	-	2	1	2	2
Loss of integrity of monitored data due to handheld or belt misuse	9	1	3	-	-	4	1	1	2
Loss of integrity of monitored data due to handheld misuse	10	1	3	-	-	-	3	2	2
Loss of integrity of server data due to break-in on server	14	1	4	4	-	4	4	2	4
Loss of data integrity due to malware attack	16	1	3	3	-	4	4	2	4
		Accumulated risk estimates							
Loss of integrity of ESUMS data	32	2	3	4	-	3	3	2	3

Table 21 - Accumulated risks: ESUMS data integrity

Table 22 gives an overview of unwanted incidents that harm ESUMS data availability. This accumulated unwanted incident yields three unacceptable risks due to the harm to *ESUMS data security*, *Service provisioning* and *Customer trust*.

Unwanted incident	**#**	**L**	**Consequence for each asset**						
			DS	**SP**	**C**	**CT**	**PT**	**QL**	**CE**
Data acquisition is suspended due to lack of training	1	3	3	-	-	1	1	2	2
Loss of monitored data on belt due to overwritten data	4	2	3	-	-	3	2	2	2
Loss of monitored data on the handheld due to improper termination of application	6	2	3	-	-	1	1	2	2
Loss of monitored data due to technical failures	7	2	3	3	-	4	3	3	3
Transmission of data from handheld to server is interrupted or prevented due to handheld misuse	8	1	3	-	-	3	3	2	2
Loss of monitored data due to config error	11	1	3	-	-	4	2	2	2
Loss of availability of monitored data on server due to malware	17	1	3	3	-	3	3	2	3
Loss of availability of monitored data on server due to erroneous data	20	2	3	-	-	2	3	2	2
Loss of availability of monitored data due to maintenance of nurse workstation	27	2	3	-	-	4	2	2	2
Handheld not able to communicate with server due to server maintenance	31	2	3	-	-	4	2	2	2
		Accumulated risk estimates							
Loss of availability of ESUMS data	33	4	3	3	-	3	2	2	2

Table 22 - Accumulated risk: ESUMS data availability

5.6 Summary of Risk Evaluation

To summarize the risk evaluation we have in Table 23 plotted all unacceptable risks into the risk evaluation matrix. In all there are 27 unacceptable risks out of a total of 165 identified risks, and all direct and indirect assets are affected. In the matrix each risk is given a unique identifier; the prefix is the number we used to index the unwanted incidents in Table 17 through Table 22, and the suffix is the abbreviations to denote the assets. The risks that accumulated are specified in *italics*.

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Unlikely					
	Rare				7CT 24DS 24C 24CT 24CE 27CT 31CT *32SP*	
	Possible			1DS 2SP 2PT 2QL 2CE 22DS 22PT 23SP 23PT 25SP	22 CT 22CE 23CE 25CT 25PT 25QL	
	Likely			*33DS 33SP 33CT*		
	Certain					

Table 23 - Overview of unacceptable risks

6 Risk Treatment

The objective of the risk treatment step is to identify cost effective treatments for the unacceptable risks. The step is conducted as a brainstorming session involving the target team. Treatments are identified by a walk-through of the threat diagrams that document the unacceptable risks and their causes.

The input to this step is CORAS risk diagrams and CORAS threat diagrams documenting the unacceptable risks. The output is the CORAS treatment diagrams documenting the identified treatments for the risks with respect to direct and indirect assets.

Figure 21 through Figure 32 show the treatment diagrams developed as a part of risk treatment identification. First, treatments are identified for the risks related to patients at home, as presented in Section 6.1. Then, treatments are identified for the risks related to ESUMS server, as presented in Section 6.2. The treatments identified for the risks related to nurse workstation are presented in Section 6.3. Finally, the treatments identified for the risks related to the infrastructure are presented in Section 6.4.

Threat diagrams documenting acceptable risks have been omitted from the treatment identification. We have also not included the indirect assets in the treatment diagrams in order to keep the diagrams as readable as possible. Since we have only two risk levels (acceptable and unacceptable), we have not annotated the risks with their risk level. Instead we used **boldface** on the description of the risks that are unacceptable. Note that some of these are unacceptable due to the indirect assets which are not shown in the treatment diagrams. The reader is referred to Section 5 for the complete documentation of the unacceptable risks. Also note that we use the naming convention from Table 23 to give each risk a unique identifier.

6.1 Treatments of Risks Related to Patients at Home

This section presents the treatment diagrams for mitigating the unacceptable risks at the home of a patient. The risks may be related to the use of the belt or the handheld, as well as software and hardware failures.

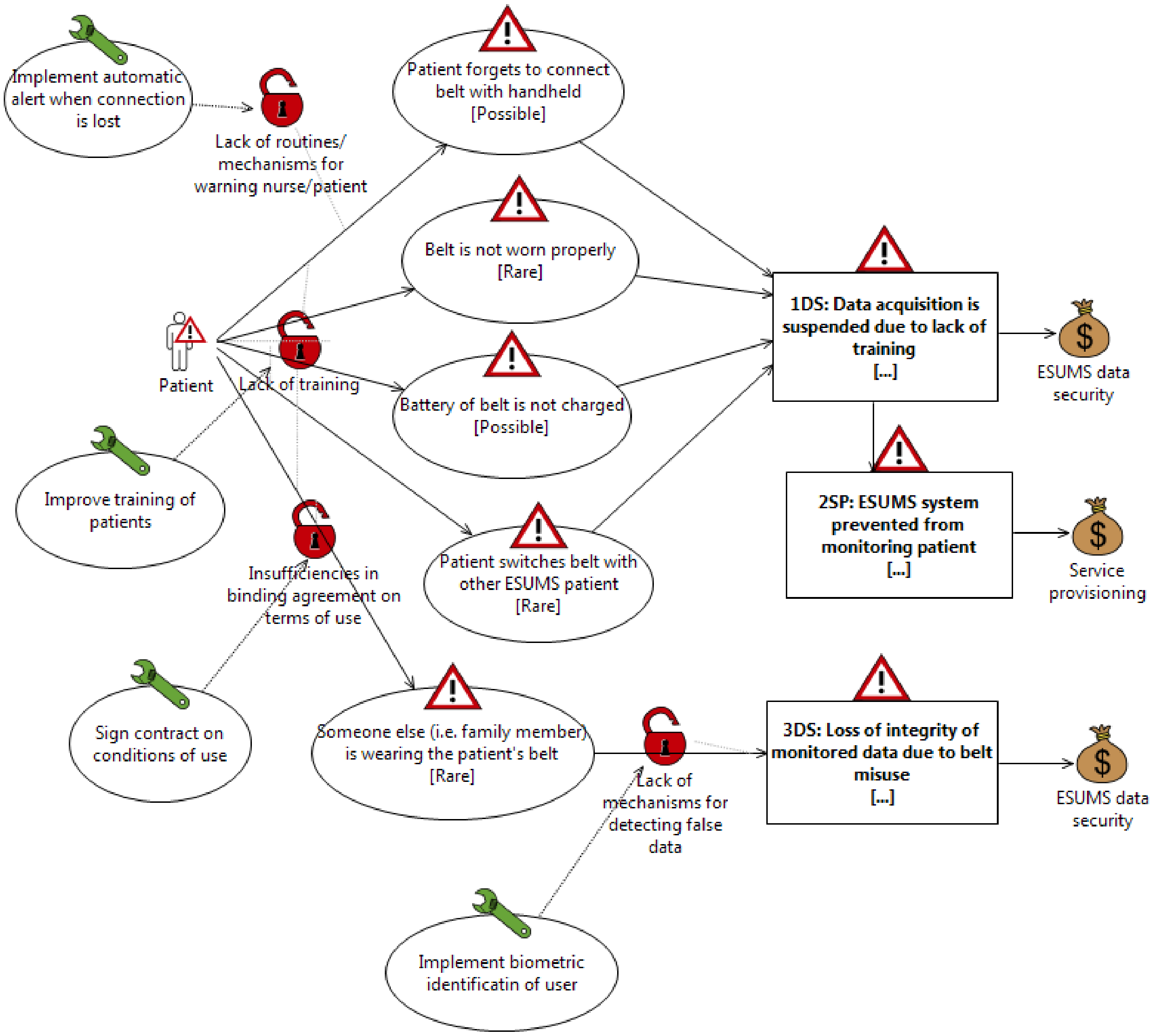

Implement automatic alert when connection is lost
Lack of routines/ mechanisms for warning nurse/patient
Patient forgets to connect belt with handheld [Possible]
Belt is not worn properly [Rare]
Patient
Lack of training
Battery of belt is not charged [Possible]
Improve training of patients
Insufficiencies in binding agreement on terms of use
Patient switches belt with other ESUMS patient [Rare]
1DS: Data acquisition is suspended due to lack of training […]
ESUMS data security
2SP: ESUMS system prevented from monitoring patient […]
Service provisioning
Sign contract on conditions of use
Someone else (i.e. family member) is wearing the patient's belt [Rare]
Lack of mechanisms for detecting false data
3DS: Loss of integrity of monitored data due to belt misuse […]
ESUMS data security
Implement biometric identificatin of user

Figure 21 - Treatment diagram addressing risks related to use of belt at home

A treatment diagram addressing the risks related to the use of belt at home is shown in Figure 21. The main vulnerabilities are treated through automatic alerts when connection is lost, improved training of patients, contract on conditions of use, and biometric authentication of user.

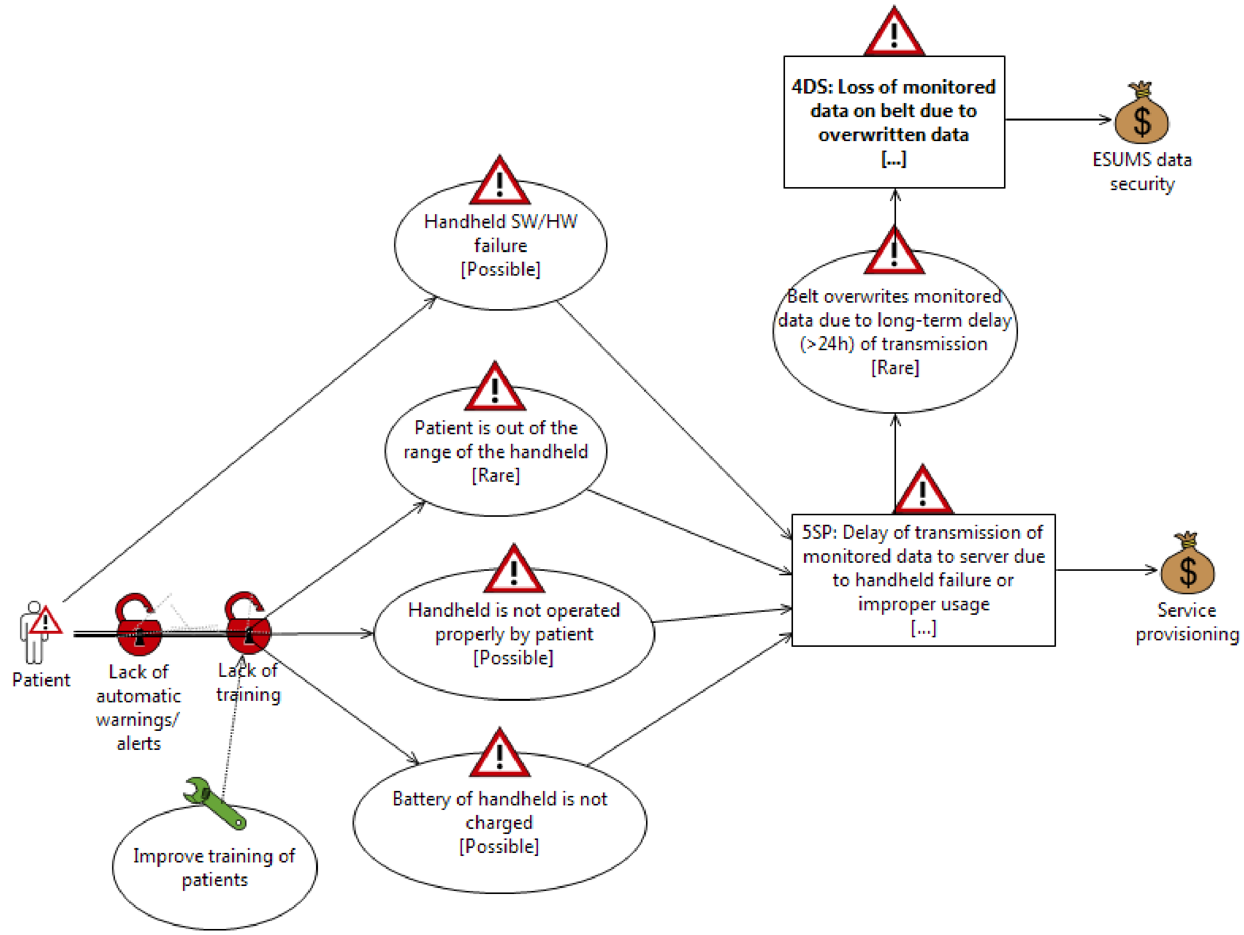

4DS: Loss of monitored data on belt due to overwritten data
[...]
ESUMS data security
Handheld SW/HW failure
[Possible]
Belt overwrites monitored data due to long-term delay (>24h) of transmission
[Rare]
Patient is out of the range of the handheld
[Rare]
5SP: Delay of transmission of monitored data to server due to handheld failure or improper usage
[...]
Service provisioning
Patient
Lack of automatic warnings/ alerts
Lack of training
Handheld is not operated properly by patient
[Possible]
Battery of handheld is not charged
[Possible]
Improve training of patients

Figure 22 - Treatment diagram addressing risks related to handheld

A treatment diagram addressing the risks related to the handheld is shown in Figure 22. The lack of training is treated through improved patient training.

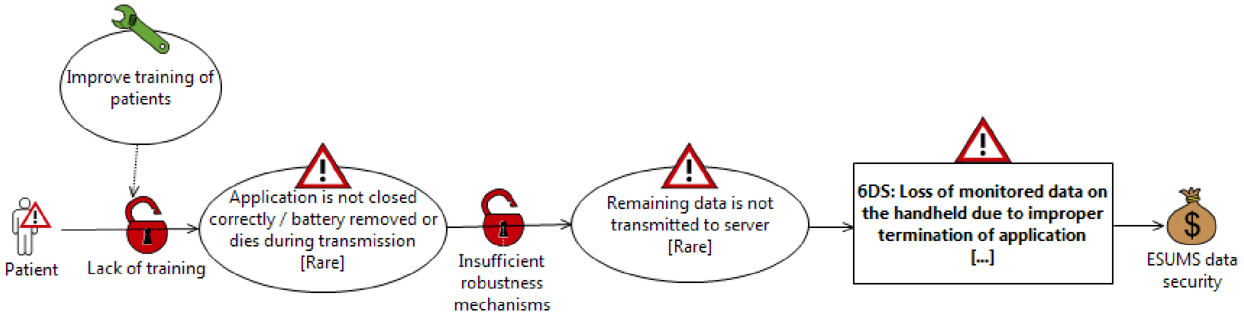

Improve training of patients
Patient
Lack of training
Application is not closed correctly / battery removed or dies during transmission
[Rare]
Insufficient robustness mechanisms
Remaining data is not transmitted to server
[Rare]
6DS: Loss of monitored data on the handheld due to improper termination of application
[...]
ESUMS data security

Figure 23 - Treatment diagram addressing a risk related to SW application on the handheld

A treatment diagram addressing the risks related to the software application installed on the handheld is shown in Figure 23. The lack of training is treated through improved patient training.

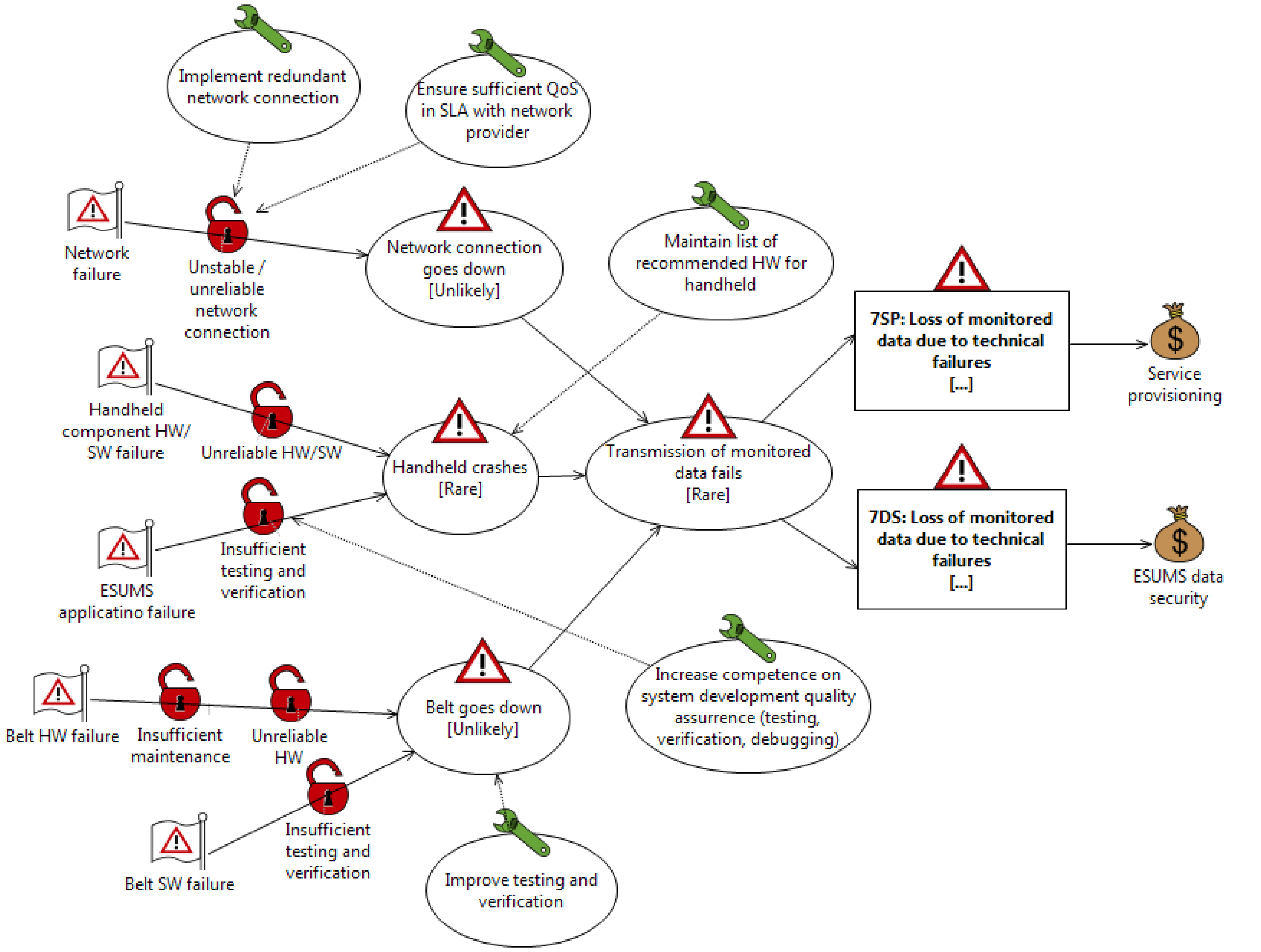

Implement redundant network connection
Ensure sufficient QoS in SLA with network provider
Network failure
Unstable / unreliable network connection
Network connection goes down [Unlikely]
Maintain list of recommended HW for handheld
7SP: Loss of monitored data due to technical failures [...]
Service provisioning
Handheld component HW/ SW failure
Unreliable HW/SW
Handheld crashes [Rare]
Transmission of monitored data fails [Rare]
7DS: Loss of monitored data due to technical failures [...]
ESUMS data security
ESUMS applicatino failure
Insufficient testing and verification
Increase competence on system development quality assurrence (testing, verification, debugging)
Belt HW failure
Insufficient maintenance
Unreliable HW
Belt goes down [Unlikely]
Belt SW failure
Insufficient testing and verification
Improve testing and verification

Figure 24 - Treatment diagram addressing risks related to SW and HW failures at home

A treatment diagram addressing the risks related to software and hardware failures at home is shown in Figure 24. The major vulnerabilities and unwanted incidents are treated through network redundancy, service level agreement, recommended list of handheld hardware and improved testing.

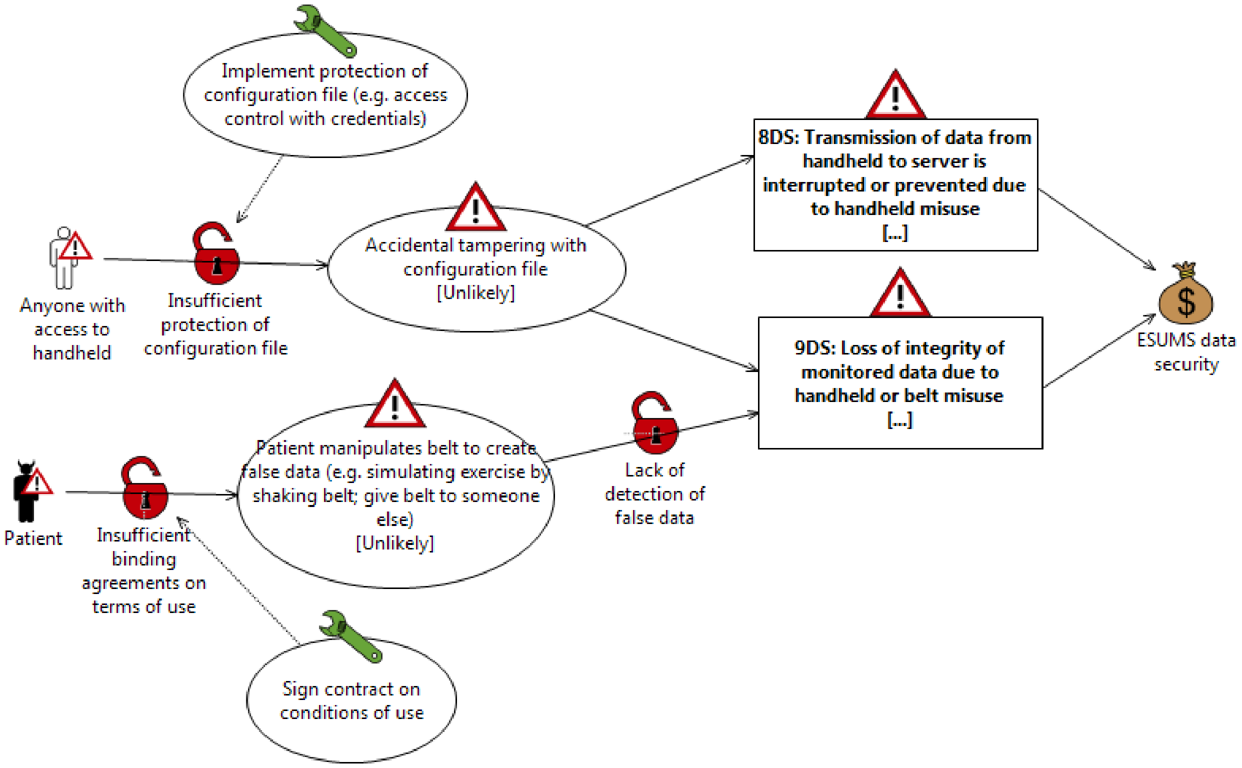

Implement protection of configuration file (e.g. access control with credentials)
Anyone with access to handheld
Insufficient protection of configuration file
Accidental tampering with configuration file [Unlikely]
8DS: Transmission of data from handheld to server is interrupted or prevented due to handheld misuse [...]
9DS: Loss of integrity of monitored data due to handheld or belt misuse [...]
$
ESUMS data security
Patient
Insufficient binding agreements on terms of use
Patient manipulates belt to create false data (e.g. simulating exercise by shaking belt; give belt to someone else) [Unlikely]
Lack of detection of false data
Sign contract on conditions of use

Figure 25 - Treatment diagram addressing risks related to misuse of belt or tampering with config file

A treatment diagram addressing the risks related to misuse of belt or tampering with config file is shown in Figure 25. The major vulnerabilities are treated through contract on conditions of use and protection of config file.

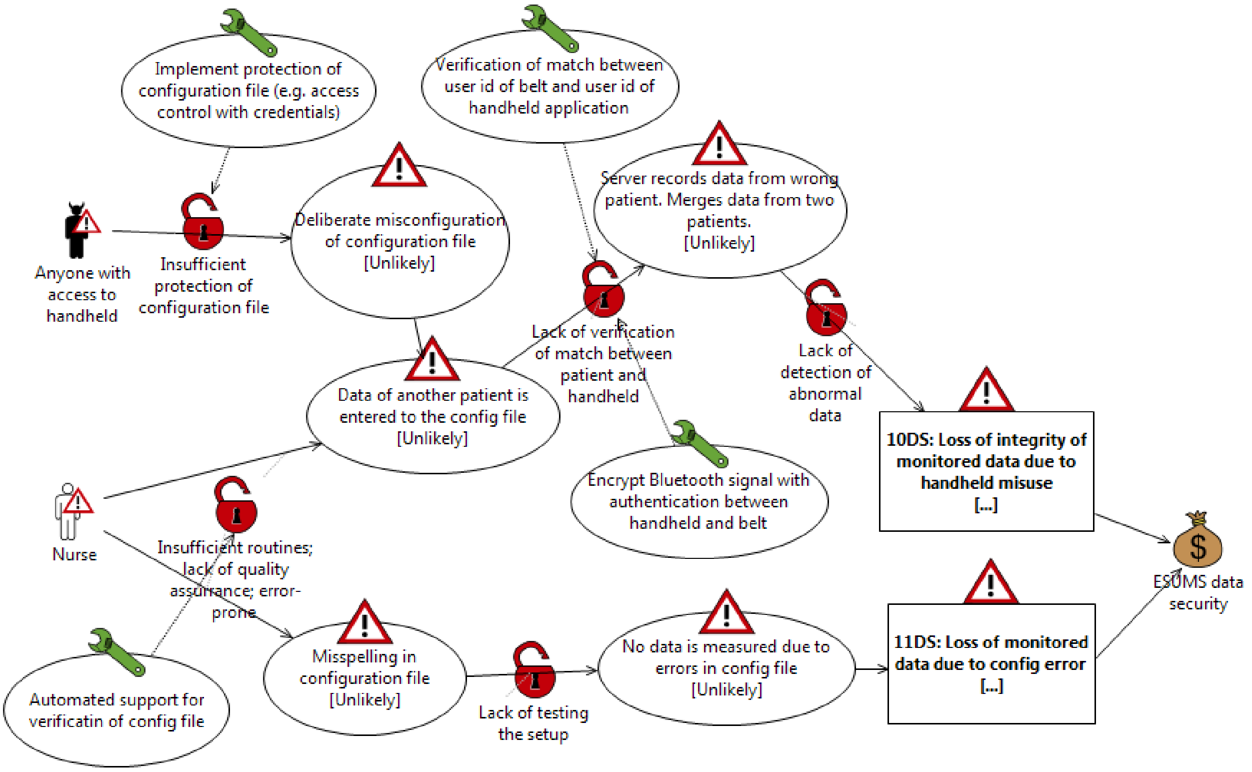

Implement protection of configuration file (e.g. access control with credentials)
Verification of match between user id of belt and user id of handheld application
Anyone with access to handheld
Insufficient protection of configuration file
Deliberate misconfiguration of configuration file [Unlikely]
Server records data from wrong patient. Merges data from two patients. [Unlikely]
Lack of verification of match between patient and handheld
Lack of detection of abnormal data
Data of another patient is entered to the config file [Unlikely]
10DS: Loss of integrity of monitored data due to handheld misuse [...]
Encrypt Bluetooth signal with authentication between handheld and belt
Nurse
Insufficient routines; lack of quality assurrance; error-prone
ESUMS data security
11DS: Loss of monitored data due to config error [...]
No data is measured due to errors in config file [Unlikely]
Misspelling in configuration file [Unlikely]
Lack of testing the setup
Automated support for verificatin of config file

Figure 26 - Treatment diagram addressing risks related to config file on the handheld

A treatment diagram addressing the risks related to to config file on the handheld is shown in Figure 26. The major vulnerabilities are treated through automated support for verification of configuration of config file, protection of config file, unique identity match between belt and handheld, and encryption of the signal between the handheld and the belt.

6.2 Treatments of Risks Related to the ESUMS Server

This section presents the treatment diagrams for mitigating the unacceptable risks related to the ESUMS server. The risks may be related to the use of the belt or the handheld, as well as software and hardware failures.

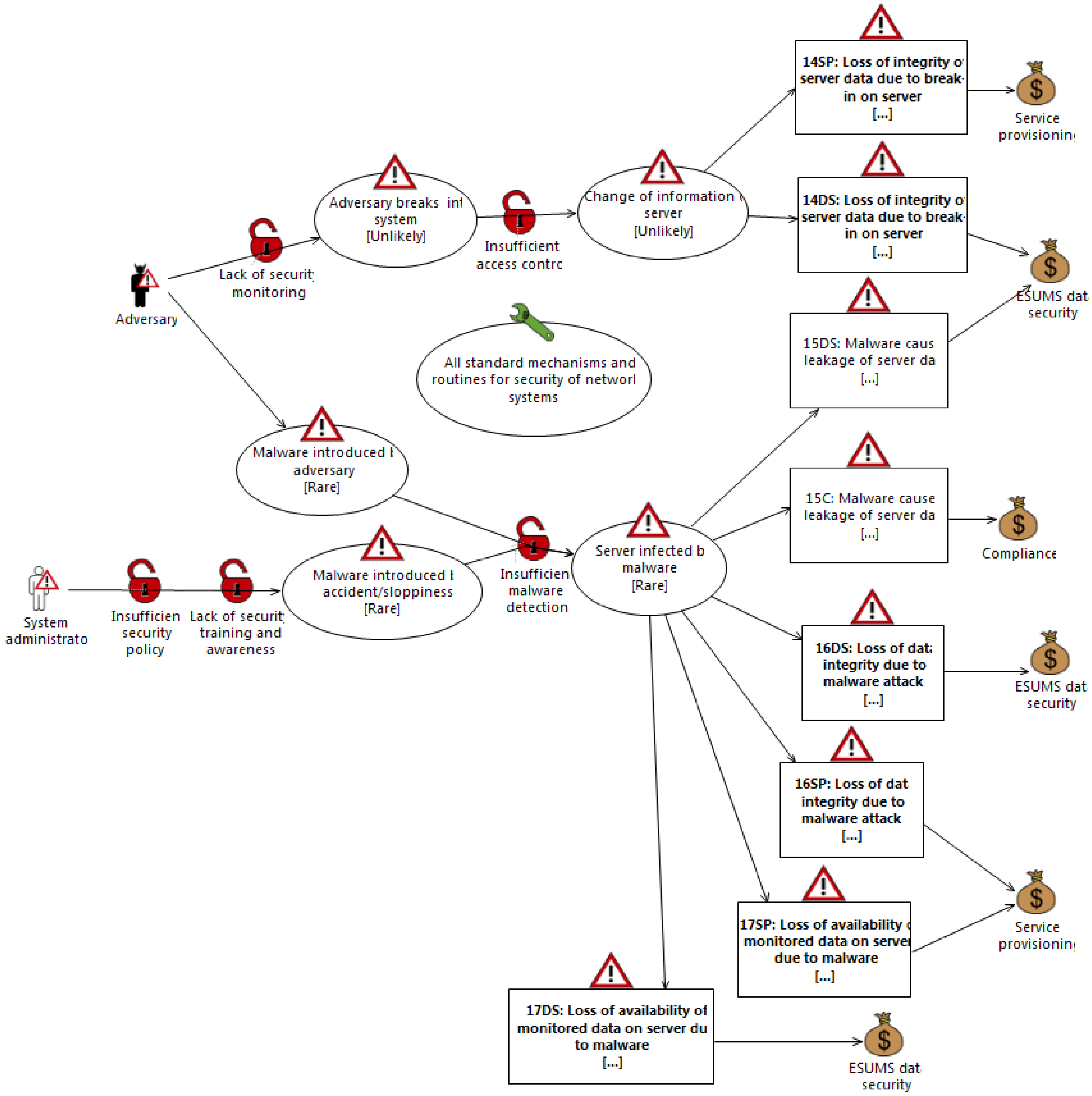

14SP: Loss of integrity o server data due to break in on server [...]
Service provisionin
Adversary breaks int system [Unlikely]
Change of information server [Unlikely]
14DS: Loss of integrity o server data due to break in on server [...]
Lack of securit monitoring
Insufficient access contrc
ESUMS dat security
Adversary
15DS: Malware caus leakage of server da [...]
All standard mechanisms and routines for security of networl systems
Malware introduced I adversary [Rare]
15C: Malware cause leakage of server da [...]
Compliance
Server infected b malware [Rare]
Malware introduced I accident/sloppiness [Rare]
Insufficien malware detection
System administrato
Insufficien security policy
Lack of securit training and awareness
16DS: Loss of dat integrity due to malware attack [...]
ESUMS dat security
16SP: Loss of dat integrity due to malware attack [...]
17SP: Loss of availability monitored data on serve due to malware [...]
Service provisionin
17DS: Loss of availability of monitored data on server du to malware [...]
ESUMS dat security

Figure 27 - Treatment diagram addressing risks related to the break-in or malware on the ESUMS server

A treatment diagram addressing the risks related to misconfiguration, user data change or change of monitored data, on the ESUMS server, is shown in Figure 27. The risks can be treated through the standard mechanisms and routines for security of networked systems. Because of its general description the treatment applies to all sources of risks documented in this diagram. We have therefore omitted the treatment relations.

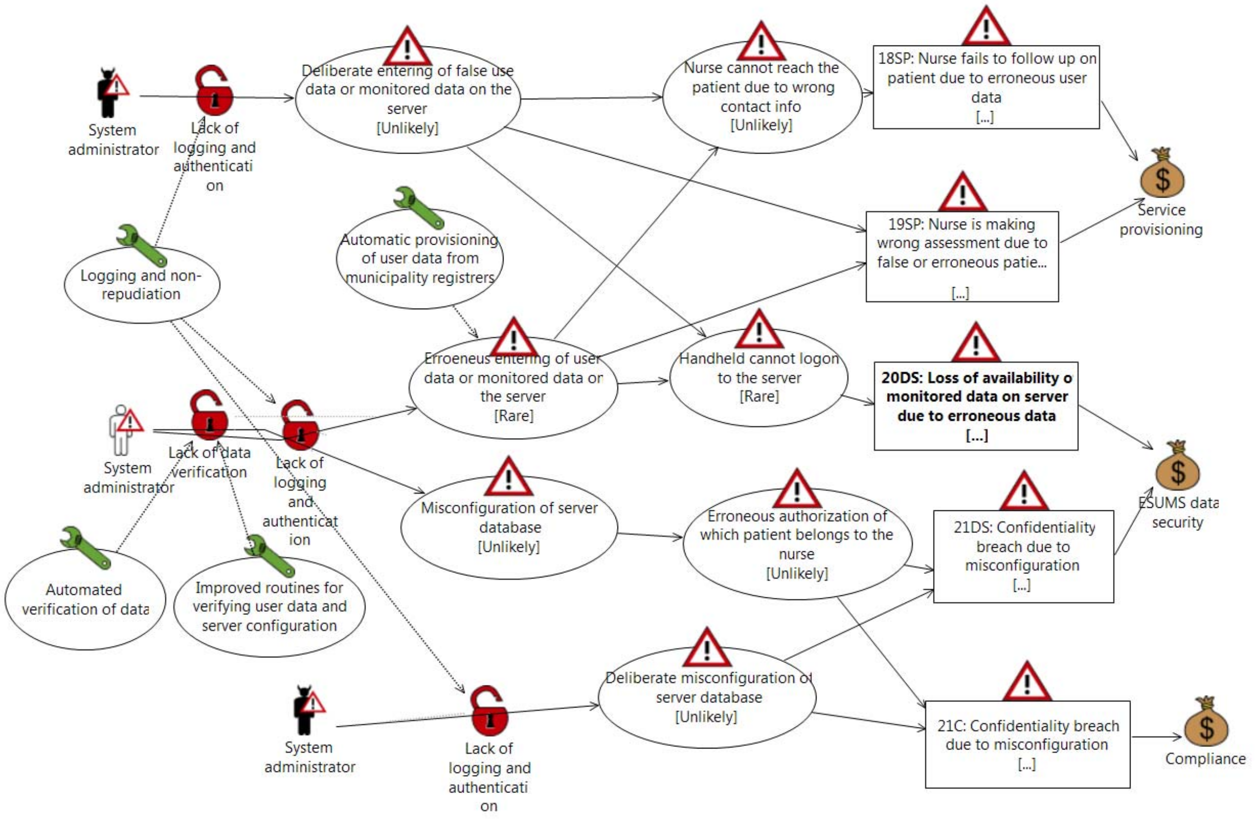

System administrator
Lack of logging and authentication
Deliberate entering of false use data or monitored data on the server [Unlikely]
Nurse cannot reach the patient due to wrong contact info [Unlikely]
18SP: Nurse fails to follow up on patient due to erroneous user data [...]
Service provisioning
19SP: Nurse is making wrong assessment due to false or erroneous patie... [...]
Automatic provisioning of user data from municipality registrers
Logging and non-repudiation
Erroneus entering of user data or monitored data or the server [Rare]
Handheld cannot logon to the server [Rare]
20DS: Loss of availability o monitored data on server due to erroneous data [...]
System administrator
Lack of data verification
Lack of logging and authentication
Misconfiguration of server database [Unlikely]
Erroneous authorization of which patient belongs to the nurse [Unlikely]
21DS: Confidentiality breach due to misconfiguration [...]
ESUMS data security
Automated verification of data
Improved routines for verifying user data and server configuration
Deliberate misconfiguration of server database [Unlikely]
System administrator
Lack of logging and authentication
21C: Confidentiality breach due to misconfiguration [...]
Compliance

Figure 28 - Treatment diagram addressing risks related to misconfiguration, user data change or change of monitored data, on the ESUMS server

A treatment diagram addressing the risks related to misconfiguration, user data change or change of monitored data on the ESUMS server is shown in Figure 28. The major vulnerabilities and unwanted incidents are treated through logging and non-repudiation, automatic provisioning of user data, automated verification of data, and improved routines for verifying used data and server configuration.

6.3 Treatments of Risks Related to the Nurse Workstation

This section presents the treatment diagrams for mitigating the unacceptable risks related to the nurse workstation. The risks may be related to leakage of information from the nurse application or the ability of a nurse to follow up a patient exposed to an incident.

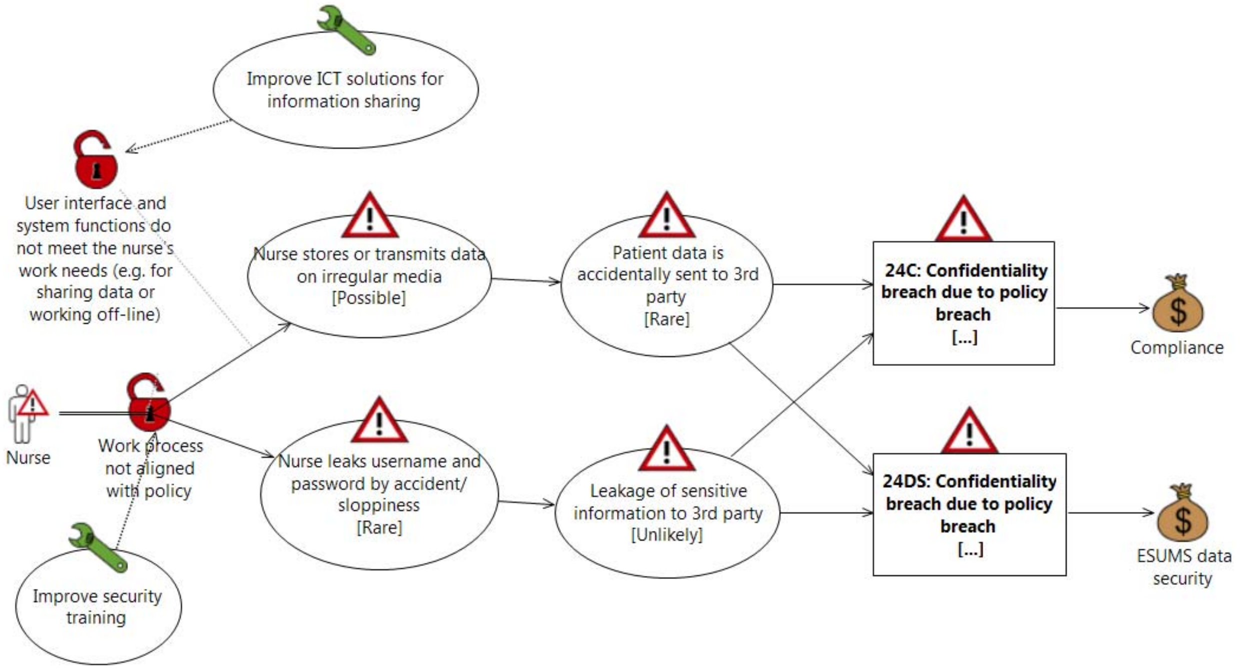

Improve ICT solutions for information sharing
User interface and system functions do not meet the nurse's work needs (e.g. for sharing data or working off-line)
Nurse
Work process not aligned with policy
Improve security training
Nurse stores or transmits data on irregular media [Possible]
Nurse leaks username and password by accident/ sloppiness [Rare]
Patient data is accidentally sent to 3rd party [Rare]
Leakage of sensitive information to 3rd party [Unlikely]
24C: Confidentiality breach due to policy breach [...]
24DS: Confidentiality breach due to policy breach [...]
Compliance
ESUMS data security

Figure 29 – Treatment diagram addressing risks related to leakage of information from nurse application

A treatment diagram addressing the risks related to leakage of information from nurse application is shown in Figure 29. The vulnerabilities are treated through improved security training and improved solution for information sharing.

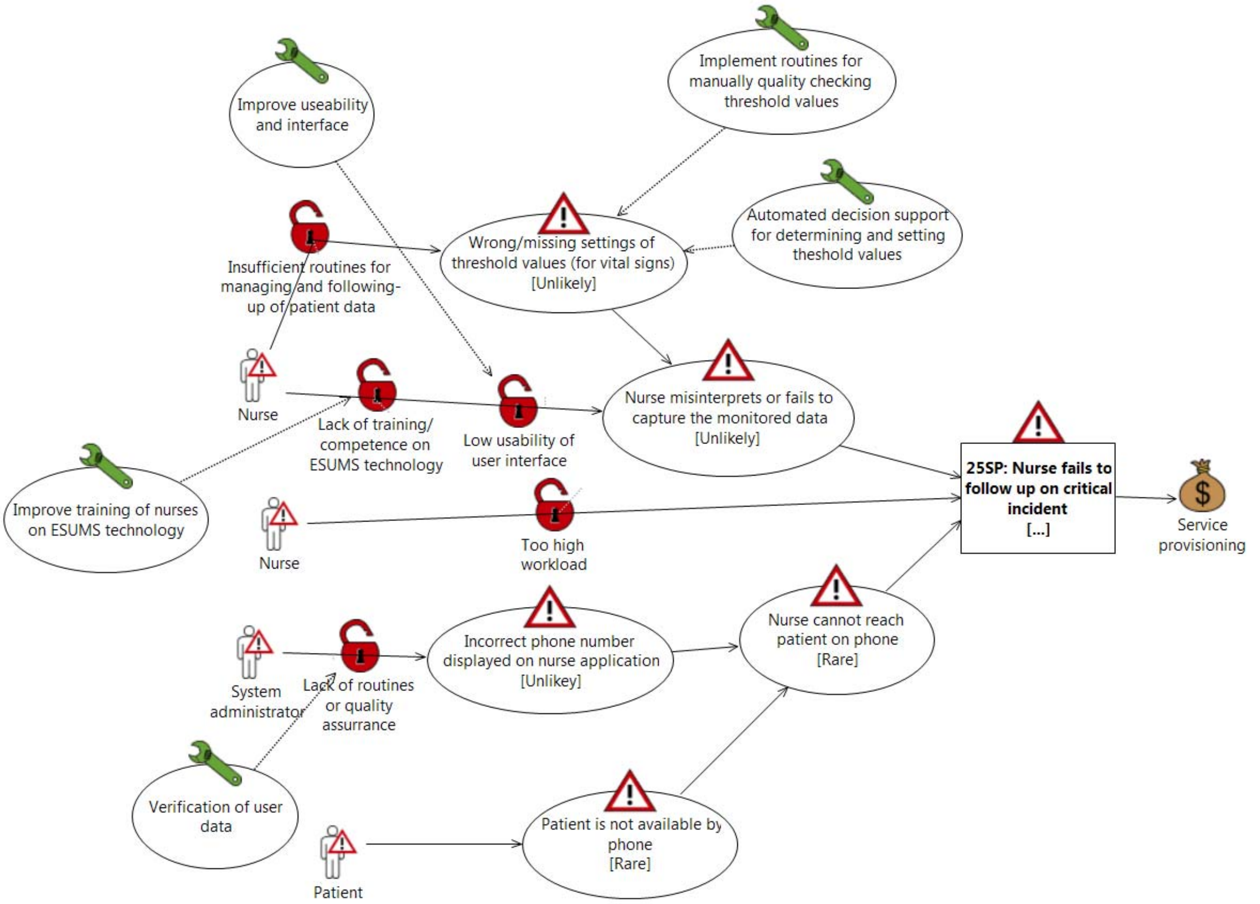

Improve useability and interface
Implement routines for manually quality checking threshold values
Automated decision support for determining and setting theshold values
Wrong/missing settings of threshold values (for vital signs) [Unlikely]
Insufficient routines for managing and following-up of patient data
Nurse
Lack of training/ competence on ESUMS technology
Low usability of user interface
Nurse misinterprets or fails to capture the monitored data [Unlikely]
25SP: Nurse fails to follow up on critical incident [...]
Service provisioning
Improve training of nurses on ESUMS technology
Nurse
Too high workload
System administrator
Lack of routines or quality assurance
Incorrect phone number displayed on nurse application [Unlikey]
Nurse cannot reach patient on phone [Rare]
Verification of user data
Patient
Patient is not available by phone [Rare]

Figure 30 – Treatment diagram addressing risks related to the ability of a nurse to follow up a patient exposed to an incident

A treatment diagram addressing the risks related to the ability of a nurse to follow up a patient exposed to an incident is shown in Figure 30. The major vulnerabilities and unwanted incidents are treated through improved training of nurse on ESUMS technology, verification of user data, improved usability and interface, routines for manually quality checking threshold values, and automated decision support for determining and setting threshold values.

6.4 Treatments of Risks Related to the Infrastructure

This section presents the treatment diagrams for mitigating the unacceptable risks related to the infrastructure. The risks may be related to failure of desktop application, or risks caused by server maintenance.

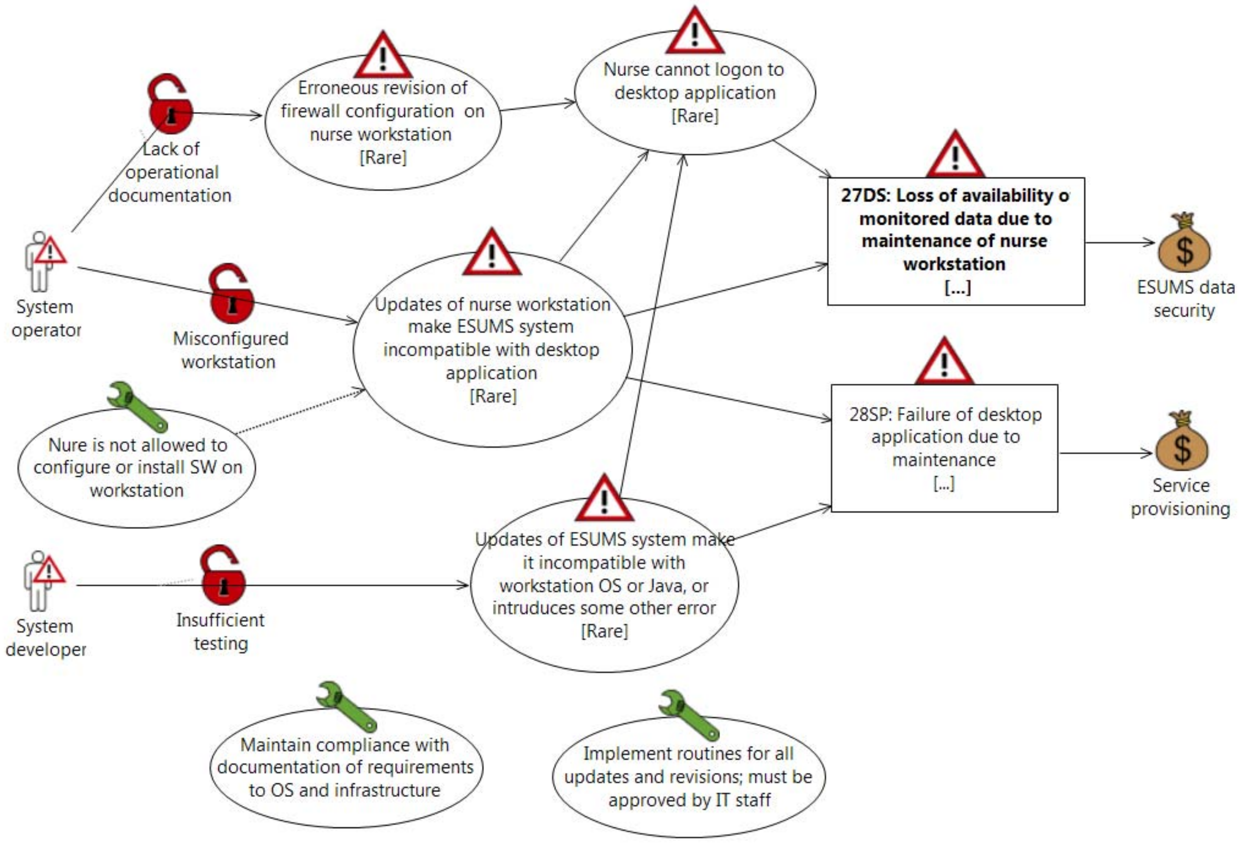

Erroneous revision of firewall configuration on nurse workstation [Rare]
Nurse cannot logon to desktop application [Rare]
Lack of operational documentation
System operator
Misconfigured workstation
Updates of nurse workstation make ESUMS system incompatible with desktop application [Rare]
27DS: Loss of availability o monitored data due to maintenance of nurse workstation [...]
ESUMS data security
28SP: Failure of desktop application due to maintenance [...]
Service provisioning
Nure is not allowed to configure or install SW on workstation
System developer
Insufficient testing
Updates of ESUMS system make it incompatible with workstation OS or Java, or intrudusces some other error [Rare]
Maintain compliance with documentation of requirements to OS and infrastructure
Implement routines for all updates and revisions; must be approved by IT staff

Figure 31 - Treatment diagram addressing risks related to failure of desktop application, due to maintenance

A treatment diagram addressing the risks related to failure of desktop application due to maintenance is shown in Figure 31. The major vulnerabilities and unwanted incidents are treated through preventing a nurse from configuring or installing software on workstation, compliance with documentation of requirements to operating system and infrastructure, and implementation of routines for all updates and revisions so that they are approved by the ICT staff. The two treatments at the bottom are applicable to all sources of risk documented in this diagram, and we have therefore omitted the relations.

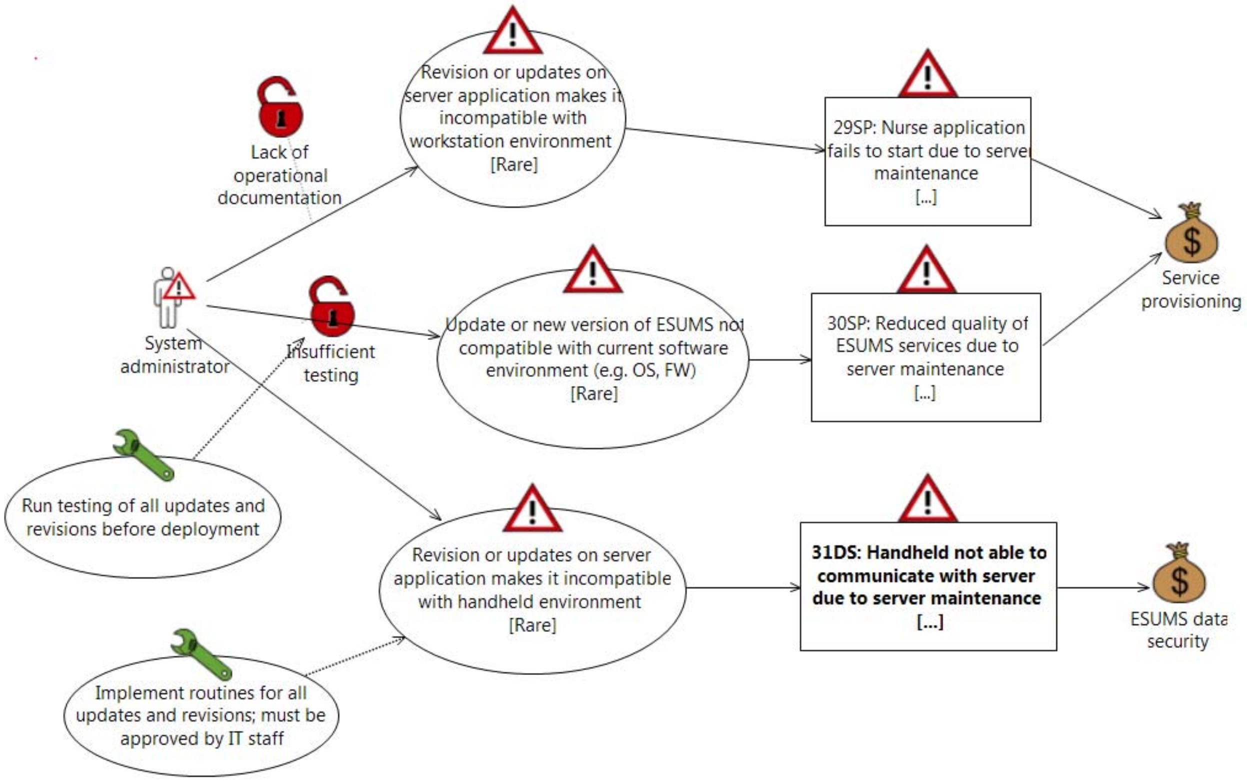

Revision or updates on server application makes it incompatible with workstation environment [Rare]
29SP: Nurse application fails to start due to server maintenance [...]
Lack of operational documentation
Service provisioning
System administrator
Insufficient testing
Update or new version of ESUMS not compatible with current software environment (e.g. OS, FW) [Rare]
30SP: Reduced quality of ESUMS services due to server maintenance [...]
Run testing of all updates and revisions before deployment
Revision or updates on server application makes it incompatible with handheld environment [Rare]
31DS: Handheld not able to communicate with server due to server maintenance [...]
ESUMS data security
Implement routines for all updates and revisions; must be approved by IT staff

Figure 32 - Treatment diagram addressing risks caused by server maintenance

A treatment diagram addressing the risks caused by server maintenance is shown in Figure 32. The main vulnerability (insufficient testing) is treated through testing of all updates and revisions before deployment.

7 Conclusion

In this report we have documented the results of a risk analysis within the domain of welfare services and welfare technology. More specifically, the target of analysis was the ESUMS (Enhanced Sustained Use Monitoring System) prototype system and the patient monitoring services provided by ESUMS. The risk analysis focused in particular on security needs of stakeholders with respect to properties such as confidentiality, integrity and availability of sensitive or critical information, as well as privacy and data protection which are highly relevant in the eHealth domain. The CORAS framework for model-driven risk analysis was the selected risk analysis method for the case study. The risk analysis was conducted over a timespan of 10 weeks and included six workshops.

The assets that were considered during the risk identification were *compliance* with data protection laws and regulations, *service provisioning*, i.e. the ability of the system to maintain an expected level of service, and *ESUMS data security*, i.e. the confidentiality, integrity and availability that is processed by and communicated within the system. In addition to these (direct) assets, four other (indirect) assets were taken into account after the risk identification to identify further risks that may arise as a consequence of risks with respect to the direct assets. Indirect assets are assets that, with respect to the target and scope of the analysis, are harmed only via harm to other assets.

The risk identification was structured by considering four different parts or aspects of the target of analysis in turn, namely risks related to the patient at home, risks related to the ESUMS server, risks related to the nurse workstation, and risks related to the underlying infrastructure. All assets, both direct and indirect, were addressed for each of these aspects of ESUMS. The risk analysis resulted in 153 identified and documented risks. In addition, 12 more high-level risks were identified by accumulating those of the 153 risks that can be considered as special instances of the same more general risks. Hence, a total of 165 risks were identified. Out of these 165 risks, 27 risks were evaluated as unacceptable and therefore considered for possible treatment and mitigation.

There is a large variety between the identified risks with respect to where they arise and which assets that are harmed. However, one aspect that often was held as a potential source of risk is the deliberate or accidental misuse of the ESUMS system by its users. First, patients may be a threat in case they use the system erroneously, in case they are sloppy, or in case they do not bother to follow-up their responsibilities in an adequate manner. Second, nurses may be a threat in case they bypass any security routines or policies, or in case the ESUMS security mechanisms are insufficient.

As a conclusion, many of the identified risk treatments to improve the risk picture are concerned with improving competence and with preventing accidents or misuse by implementing security mechanisms. For the patients that are being monitored at home, improved training in the use of ESUMS is recommended. Additionally, contracts on conditions of use should be considered to make clear what are the responsibilities and liabilities of the users of ESUMS. To further prevent accidental or deliberate system misuse by patients, improved mechanisms for identification and authentication should be considered. Also for the nurses, improved training is recommended, both with respect to the ESUMS technology and with respect to security. Routines or mechanisms for data verification and quality checking are also recommended.

Acknowledgements: This work has been partially funded by SINTEF ICT via the SINTEF project FRISK, and partially by the European Commission via the NESSoS (256980) network of excellence.

8 References

[1] M. S. Lund, B. Solhaug and K. Stølen. Model-Driven Risk Analysis – The CORAS Approach. Springer, 2011.

[2] I. Svagård, F. Strisland, J. Vedum, T. Seeberg and M. Borch. Enhanced Sustained Use Monitoring System – Deliverable 1: Requirements Specification. Technical Report F12602, SINTEF ICT, 2009.

[3] Health Information Management Systems Society (HIMSS)] http://www.himss.org/ASP/index.asp Accessed 21. March 2012

[4] T. M. Seeberg, M. Hjelstuen, H. Opsahl, J. Vedum and F. Strisland. Enhanced Sustained Use Monitoring System – Deliverable 2: ESUMS System specification – Chest unit specification. Technical Report F14307, SINTEF ICT, 2010.

[5] I. Svagård , S. Walderhaug, H. Opsahl Austad, A. Kofod-Petersen, E. Stav. Enhanced Sustained Use Monitoring System – Deliverable 2: ESUMS System specification – Handheld and server specification. Technical Report F14310, SINTEF ICT, 2010.

[6] ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary. http://www.27000.org/ Accessed March 22 2012

[7] European Commission http://ec.europa.eu/index_en.htm Accessed March 22 2012

A Appendix: Target Description

In this appendix we give a more detailed description of the target of analysis. The description is based on ESUMS specifications as described in several documents [2][4][5]. Some of the figures in this appendix are snipped from these documents, while others are slightly adapted. As shown by Figure 33, the main components of the ESUMS system include chest unit, handheld, server, external sensor unit and desktop unit for the nurse. In addition, there is a standalone application for sharing of full ECG and other ESUMS data, real-time. The chest unit is fully implemented in terms of software and hardware. Software for the handheld is fully developed, while hardware is "component off the shelf" (COTS). Server is also a COTS and contains ESUMS data only. The comments from the nurse are stored on the local workstation. External sensor unit is COTS with Bluetooth interface.

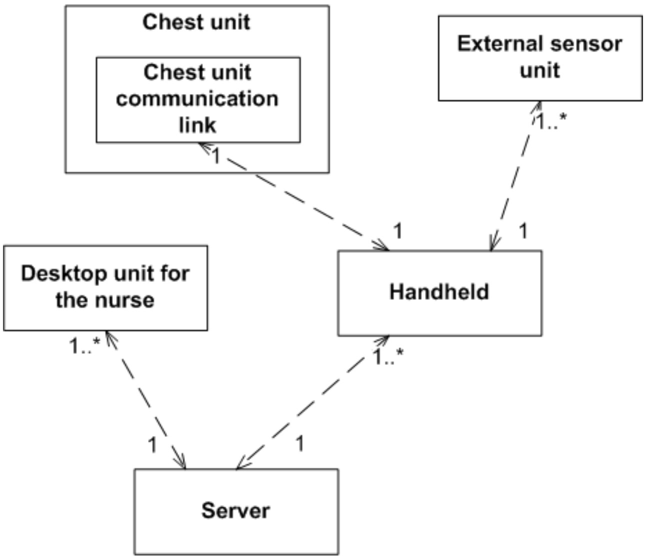


Figure 33 - ESUMS main components

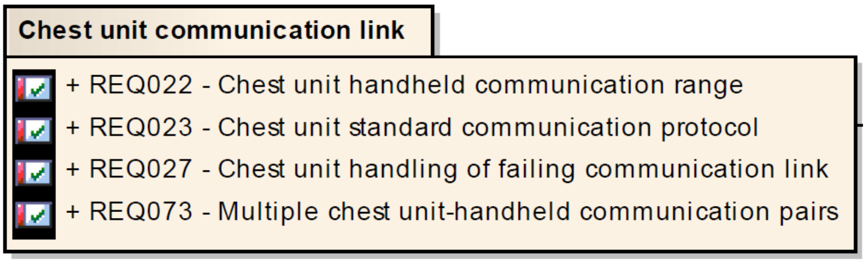
The main actors are specified in Figure 34. We distinguish between "system actors", "person roles" and "external actors". An overview of the requirements to the chest unit communication link is given in Figure 35. For the detailed specification of each requirement, the reader is referred to [2].

System actors
Chest unit
ESUMS central server
Patient handheld
Desktop

Person roles
Patient
Monitoring nurse
Next of kin
Service provider
Health care provider

External actors
Electronic health record
External sensor unit

Figure 34 - Main actors

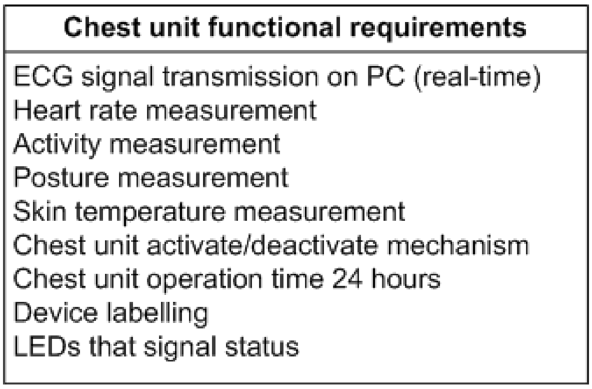


Chest unit communication link

☑ + REQ022 - Chest unit handheld communication range
☑ + REQ023 - Chest unit standard communication protocol
☑ + REQ027 - Chest unit handling of failing communication link
☑ + REQ073 - Multiple chest unit-handheld communication pairs

Figure 35 - Communication links

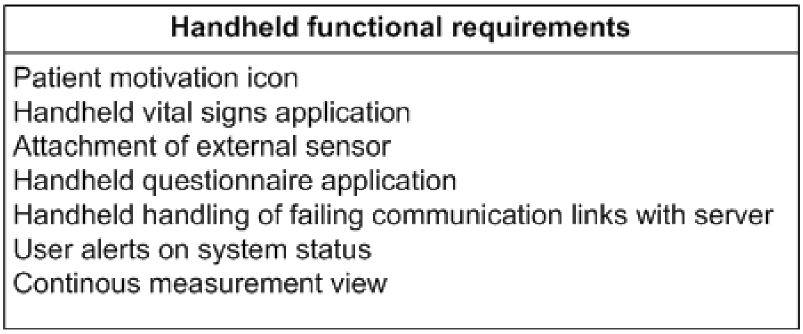
The chest unit can be connected to monitoring nurse workstation for configuring the monitoring. The functional requirements of the chest unit are listed in Figure 36, and the functional requirements for the handheld are listed in Figure 37.



Chest unit functional requirements

ECG signal transmission on PC (real-time)
Heart rate measurement
Activity measurement
Posture measurement
Skin temperature measurement
Chest unit activate/deactivate mechanism
Chest unit operation time 24 hours
Device labelling
LEDs that signal status

Figure 36 - Chest unit functional requirements

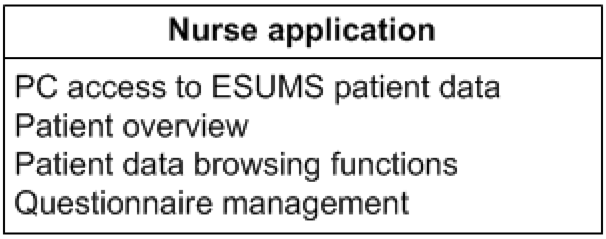


Handheld functional requirements

Patient motivation icon
Handheld vital signs application
Attachment of external sensor
Handheld questionnaire application
Handheld handling of failing communication links with server
User alerts on system status
Continous measurement view

Figure 37 - Handheld functional requirements

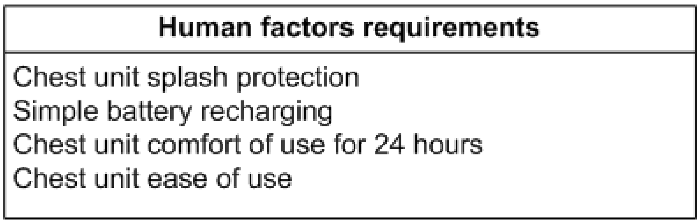
Vital signs threshold management is achieved through the configuration file stored on the PC. Monitoring nurse client is included here. The ESUMS documentation on requirements incorrectly treats server and nurse application as one functional unit. If the system was to be implemented in a real setting, there would be several more requirements for the server, for example on reliability, dependability, etc. Functional requirements for the monitoring application are specified on Figure 38. The human factor requirements are listed in Figure 39.



Nurse application

PC access to ESUMS patient data
Patient overview
Patient data browsing functions
Questionnaire management

Figure 38 - Monitoring application functional requirements

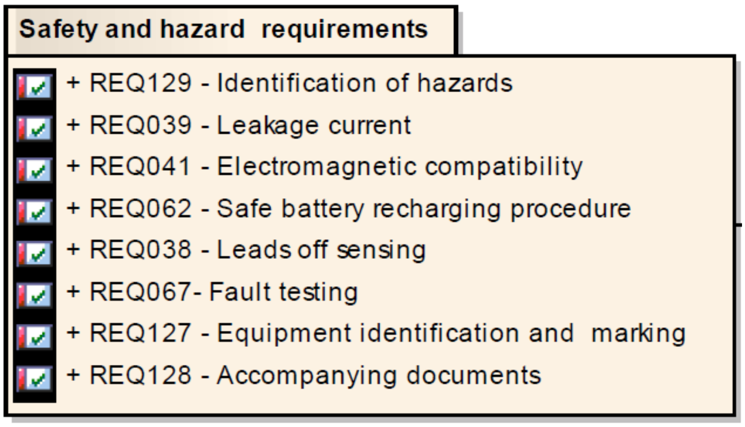


Human factors requirements

Chest unit splash protection
Simple battery recharging
Chest unit comfort of use for 24 hours
Chest unit ease of use

Figure 39 - Human factors requirements

The safety and hazard requirements are specified in Figure 40. These requirements are largely adopted from relevant standards for such equipment. Hazard identification is on safety w.r.t. the devices. These requirements are mainly related to requirements for FDA approval. FDA has checklists for these requirements. These requirements are only partially tested.

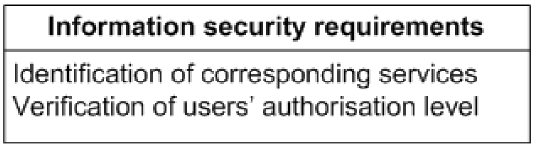


Safety and hazard requirements

- ✓ + REQ129 - Identification of hazards
- ✓ + REQ039 - Leakage current
- ✓ + REQ041 - Electromagnetic compatibility
- ✓ + REQ062 - Safe battery recharging procedure
- ✓ + REQ038 - Leads off sensing
- ✓ + REQ067- Fault testing
- ✓ + REQ127 - Equipment identification and marking
- ✓ + REQ128 - Accompanying documents

Figure 40 - Safety and hazard requirements

Information security requirements are specified in Figure 41. All “high-importance” requirements are met. In terms of integrity and confidentiality, data is transmitted by 3G and there is no encryption of data. Only 3G communication coding and protocol is implemented. Database is not encrypted. There is no logging or traceability.

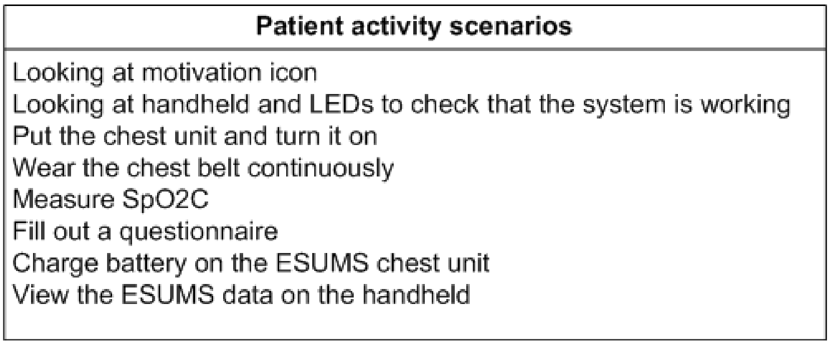


Information security requirements

Identification of corresponding services
Verification of users’ authorisation level

Figure 41 - Information security requirements

Patient activity scenarios are listed in Figure 42. Alarm button is not implemented. The use cases for the patient are specified in Figure 43. The use cases for the nurse are specified in Figure 44. The use cases for the handheld are specified in Figure 45. The state chart specified in Figure 46 specifies the states that the chest unit can be in, and the triggers for entering each state.



Patient activity scenarios
Looking at motivation icon
Looking at handheld and LEDs to check that the system is working
Put the chest unit and turn it on
Wear the chest belt continuously
Measure SpO2C
Fill out a questionnaire
Charge battery on the ESUMS chest unit
View the ESUMS data on the handheld

Figure 42 - Patient activity scenarios

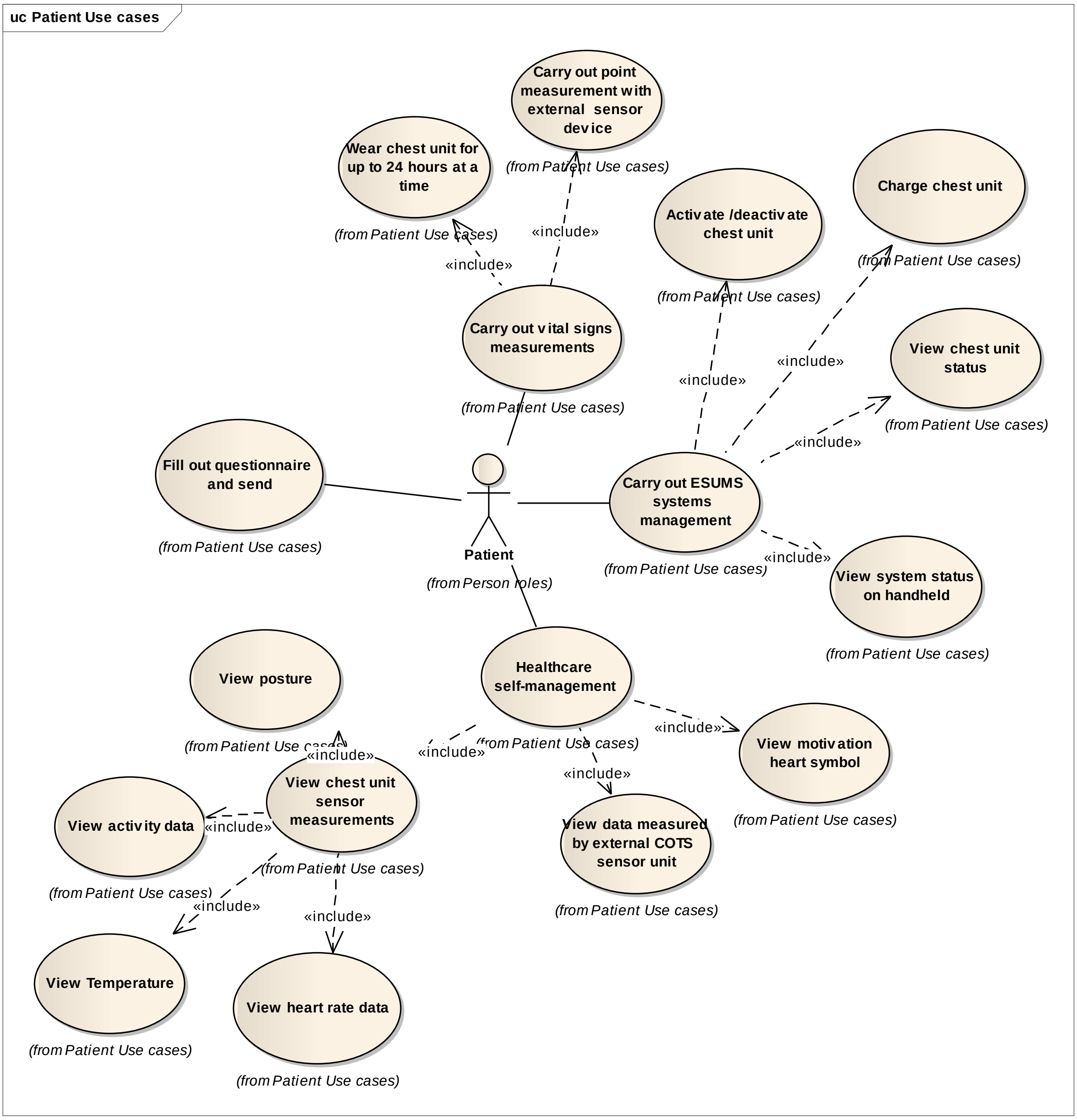


Figure 43 - Patient use cases

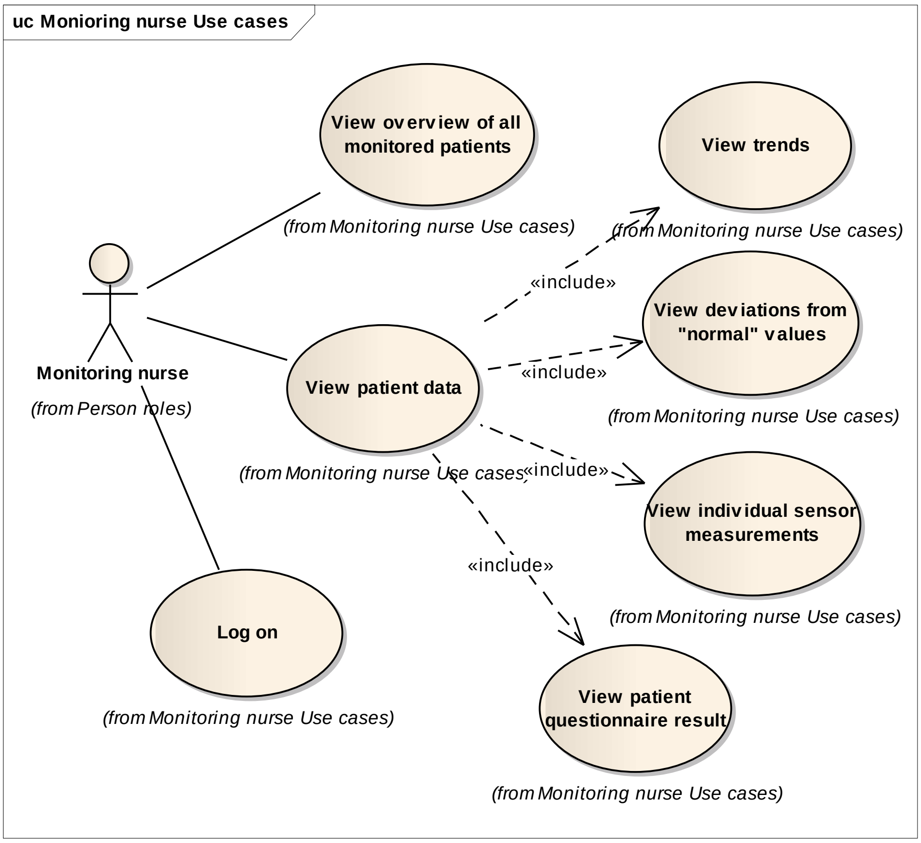

uc Monioring nurse Use cases
View overview of all monitored patients
(from Monitoring nurse Use cases)
View trends
(from Monitoring nurse Use cases)
«include»
View deviations from "normal" values
«include»
(from Monitoring nurse Use cases)
Monitoring nurse
(from Person roles)
View patient data
(from Monitoring nurse Use cases)
«include»
View individual sensor measurements
«include»
(from Monitoring nurse Use cases)
Log on
(from Monitoring nurse Use cases)
View patient questionnaire result
(from Monitoring nurse Use cases)

Figure 44 - Nurse use cases

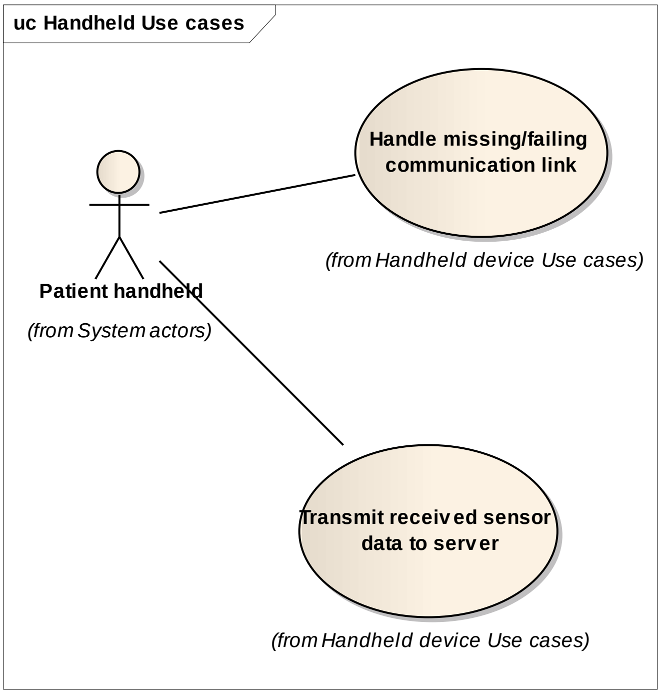

uc Handheld Use cases
Handle missing/failing communication link
(from Handheld device Use cases)
Patient handheld
(from System actors)
Transmit received sensor data to server
(from Handheld device Use cases)

Figure 45 - Handheld use cases

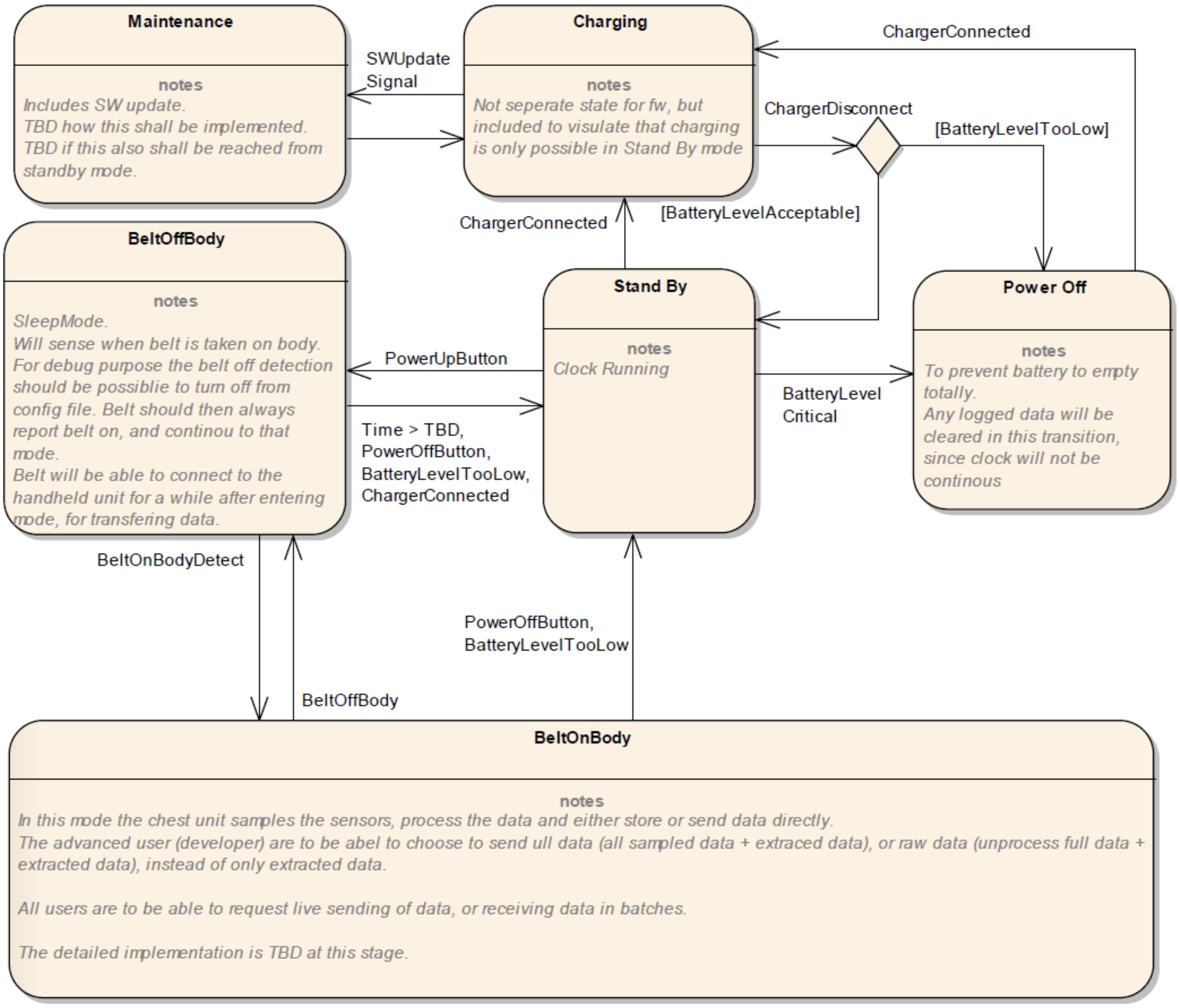

Maintenance
notes
Includes SW update.
TBD how this shall be implemented.
TBD if this also shall be reached from standby mode.
SWUpdate Signal
Charging
notes
Not seperate state for fw, but included to visulate that charging is only possible in Stand By mode
ChargerConnected
ChargerDisconnect
[BatteryLevelTooLow]
[BatteryLevelAcceptable]
ChargerConnected
BeltOffBody
notes
SleepMode.
Will sense when belt is taken on body.
For debug purpose the belt off detection should be possiblie to turn off from config file. Belt should then always report belt on, and continou to that mode.
Belt will be able to connect to the handheld unit for a while after entering mode, for transfering data.
PowerUpButton
Time > TBD, PowerOffButton, BatteryLevelTooLow, ChargerConnected
Stand By
notes
Clock Running
BatteryLevel Critical
Power Off
notes
To prevent battery to empty totally.
Any logged data will be cleared in this transition, since clock will not be continous
BeltOnBodyDetect
BeltOffBody
PowerOffButton, BatteryLevelTooLow
BeltOnBody
notes
In this mode the chest unit samples the sensors, process the data and either store or send data directly.
The advanced user (developer) are to be abel to choose to send ull data (all sampled data + extraced data), or raw data (unprocess full data + extracted data), instead of only extracted data.
All users are to be able to request live sending of data, or receiving data in batches.
The detailed implementation is TBD at this stage.

Figure 46 - State chart for chest unit

SINTEF

Technology for a better society

www.sintef.no