DEGREE PROJECT IN TECHNOLOGY,
FIRST CYCLE, 15 CREDITS
STOCKHOLM, SWEDEN 2020

Legal and Security Issues of Data Processing when Implementing IoT Solutions in Apartments

JOHAN EDMAN

WILHELM ÅGREN

KTH ROYAL INSTITUTE OF TECHNOLOGY
SCHOOL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE

Legal and Security Issues of Data Processing when Implementing IoT Solutions in Apartments

JOHAN EDMAN, WILHELM ÅGREN

Bachelor in Information Technology
Date: June 5, 2020
Supervisor: Viktor Engström
Examiner: Robert Lagerström
School of Electrical Engineering and Computer Science
Host company: SVEA Smart Grid AB
Swedish title: Rättsliga och säkerhetsrelaterade problem med databehandling för IoT-lösningar i bostädsrätter

Abstract

The concept of the Internet of Things (IoT) and connected devices is a growing trend. New ways to integrate them with Smart Home Technology emerge each day. The use of sensors in IoT solutions enables large scale data collection that can be used in various ways. The European Union recently enforced a General Data Protection Regulation (GDPR) that sets guidelines for the collection and processing of personal information. The communication protocol M-Bus is a European standard (EN 13757-x) mainly used for remote reading of electrical, gas and water meters. M-Bus is being integrated with sensors because the protocol offers long battery times. There are however some known flaws with the protocol that might make it unsuitable for a large scale data collection system. A conceptualized data collection scenario with a system utilizing M-Bus is presented. The authors aim to investigate some of the security flaws with the M-Bus protocol, while also investigating the GDPR demands of the system. The thesis supplements a System Requirement Specification (SyRS) which can be used as a template for organizations implementing a similar system. An analysis of the system based on the SyRS is conducted to identify any shortcomings. Modifications to the system are proposed in order to comply with the defined SyRS. The authors concluded that M-Bus is a sufficiently reliable protocol to be used in the system, and has no inherent conflicts with GDPR. The system has a few flaws in terms of GDPR compliance, which require both administrative and technical work to comply with. The suggested modifications of the system are mainly focused on how the data is stored in various parts of it.

Keywords: Smart Buildings, IoT, M-Bus, GDPR, SyRS

Sammanfattning

Konceptet med Internet of Things (IoT) och uppkopplade enheter är en växande trend, och nya sätt att integrera dem med det smarta hemmet framträder varje dag. Den Europeiska Unionen har nyligen verkställt en ny dataskyddsförordning, General Data Protection Regulation (GDPR), som sätter krav på insamling och behandling av personlig data. Användandet av IoT lösningar skapar möjligheten för storskalig datainsamling som kan användas på flera sätt. Kommunikationsprotokollet M-Bus är en europeisk standard (EN 13757-x) som huvudsakligen är framtagen för att avlägset läsa av el-, gas- och vattenmätare. På grund av ett litet avtryck och enkel implementation av sitt protokoll så är M-bus ofta ett val till uppkoplade sensorer för att möjliggöra lång drifttid. Det finns däremot ett antal säkerhetsbrister med protokollet som kan göra det olämpligt för ett datainsamlingssystem. Ett konceptualiserat datainsamlingscenario med ett system som utnyttjar M-Bus presenteras. Författarnas mål är att undersöka några av säkerhetsbristerna med M-Bus protokollet, samtidigt som det undersöker vilka krav GDPR ställer på ett sådant system. Uppsatsen sammanställer en kravspecifikation som kan användas som grund och riktlinje för organisationer som ska implementera liknande system. En analys av det konceptualiserade systemet baserat på kravspecifikationen genomförs för att identifiera potentiella brister. Modifikationer till system föreslås för att uppnå kraven definierade i kravspecifikationen. Författarna drog slutsatsen att M-Bus är ett tillräckligt tillförlitligt protokoll som kan användas för system likt detta. Det analyserade systemet har några brister gällande GDPR, som kräver både tekniska och administrativa åtgärder. De föreslagna modifikationerna av systemet är fokuserade primärt på hur den personliga informationen lagras i de olika delarna av systemet.

Nyckelord: Smarta Byggnader, IoT, M-Bus, GDPR, SyRS

Contents

1 Introduction **1**
- 1.1 Problem formulation . . . 2
- 1.2 Research question . . . 3
- 1.3 Study limitations and restrictions . . . 3

2 Background **4**
- 2.1 Data collection scenario . . . 4
- 2.2 Privacy and legislation . . . 6
- 2.3 M-Bus and wireless communication . . . 7

3 Method and Implementation **10**
- 3.1 Requirements elicitation . . . 10
  - 3.1.1 Semi-structured interview . . . 10
  - 3.1.2 Literature study . . . 11
- 3.2 System requirement specification . . . 12

4 Results **13**
- 4.1 Internal stakeholder requirements . . . 13
  - 4.1.1 Semi-structured interview . . . 13
- 4.2 Literature study . . . 16
  - 4.2.1 General Data Protection Regulation . . . 16
  - 4.2.2 M-Bus systems . . . 18
- 4.3 Requirement specification . . . 20
- 4.4 Conceptual redesign of system . . . 21
  - 4.4.1 General Data Protection Regulation . . . 21
  - 4.4.2 M-Bus protocol . . . 22

5 Discussion **23**
- 5.1 Conclusions . . . 24

5.2 Future work 25

Bibliography **26**

A Interview Questions **30**

B System Requirement Specification **32**

Chapter 1

Introduction

The use of connected devices, or smart devices, is a rapidly growing trend in the world today. The concept of Internet of Things (IoT) was coined by Kevin Ashton in 1999 and emerged as an umbrella term for connected devices that contain some form of microprocessor or sensor [1]. These devices have gained a strong foothold in production industries and have been acting as a catalyst for the fourth industrial revolution according to Saleem et al. [2]. The use of IoT devices is also present in households, and Ericsson[1] expects that there will be 24.9 billion connected devices in the world by the year 2025.

IoT solutions have many different kinds of applications, and the areas of use are expanding as technology keeps developing. Smart Home Technology, or simply Smart Homes[2], are buildings equipped with various IoT devices. These connected devices can be anything from a connected refrigerator to an autonomous vacuum cleaner. Smart Homes can also be equipped with various sensors that collect data and information about the household climate or residents[3]. The use of sensors in IoT solutions enables large scale data collection. Data that can be used to understand consumer behaviour, their habits as well as adjusting energy consumption based on that [3]. The European Union firmly believes that the integration of these devices in the building sector is important to reach the environmental goals that are set [4]. The sector is today alone responsible for roughly 30% of the energy use in the EU as well as 24% of global emissions [5].

Establishing a network infrastructure that continually collects data in homes

[1] https://www.ericsson.com/en/internet-of-things

[2] Houses equipped with Smart Home Technology is often referred to as Smart Homes.

[3] https://internetofthingsagenda.techtarget.com/definition/smart-home-or-building

with IoT sensors can be done with the Meter Bus (M-Bus) protocol and the wireless alternative wM-Bus [6]. The M-Bus protocol is defined by the Open Metering Systems (OMS) group and is a declared standard in the EU. The protocol enables good battery longevity due to its low overhead in the stack implementation. Because of the battery life reaching up to 10 years, IoT sensors that communicate via M-Bus are a good choice for Smart Home solutions [7]. The wM-Bus protocol has some security flaws, and it is according to Compass Security AG vulnerable on several areas when it comes to network attacks that modify or delete data. According to the M-Bus standard, the protocol should be robust enough to protect the data against Network Traffic Analysis (NTA)[4]. However, Compass Security AG do not think that the M-Bus standard holds to this fact and they claim it is not robust enough to be a reliable standard [8].

Apart from security difficulties that arise when implementing an IoT system that collects user data, one has to take personal integrity and privacy into account. One of the first definitions for privacy that became popularised was "the right to be left alone", as defined by Warren and Brandeis in 1890 in the article "The Right to Privacy". It proved to be an important stepping stone towards legislation and rights to personal information [9]. The General Data Protection Regulation (GDPR) was enforced by the EU in 2018. The regulation defines when the collection and processing of personal data are justified and acts as guidelines for organizations that aim to collect user data in any way. It is important for these companies to completely comply with the GDPR in order to avoid any fines[5].

Privacy together with the GDPR creates important boundaries for companies when designing a sensor network. These boundaries outline the scope of the network and define both the processing and collecting of the user data. Because of this, it is important to have clear standards and specifications for the system that should comply with the GDPR. There are specifications for individual IoT devices utilizing M-Bus but there is no general specification for a wider sensor network.

1.1 Problem formulation

The problem is that there are no general specifications for organizations implementing sensors networks. These sensor networks might collect a large

[4]Recording, analyzing and intercepting communication patterns in a network.
[5]https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules

amount of user data which raises privacy questions. An individual might not be sure what is gathered and how it is handled by the organization. There might be personal information that allows data to be uniquely tied to an individual and their habits without justification. Although what applies to collecting and handling such data have been specified in regulations such as the GDPR, many businesses fail to follow this and are heavily fined[6]. Another problem with sensor networks utilizing M-Bus is the security aspect of the protocol. The protocol currently has some flaws that make the system vulnerable to network attacks. These attacks can modify, delete and potentially steal data according to Compass Security AG [8]. Before implementing a sensor network utilizing M-Bus, it would be wise to, based on the GDPR, define a specification for a system and verify whether or not the M-Bus protocol complies to it.

1.2 Research question

This study aims to investigate and analyze how a conceptualized data collection scenario holds in regards to newly established privacy and data security regulations. What must be held to mind when implementing it as to not violate any data or privacy laws and regulations? The data collection scenario in question is a system utilizing the M-Bus protocol. It will be investigated if the protocol is robust enough in terms of security and if it indeed is suited for the use case. How well does a system utilizing M-Bus achieve compliance with GDPR? To determine what requirements that are deemed necessary for such a system to fulfill, a System Requirement Specification (SyRS) will be proposed. With the specification, it can then be determined whether such a scenario is secure enough and in compliance with data and privacy regulations. A proposition of modifications will be presented for the system if it does not completely comply with the defined specification.

1.3 Study limitations and restrictions

As this study analyzes system compliance regarding the GDPR, the specification is only relevant to countries of the European Union, or for companies located elsewhere that have customers in member countries. It will not attempt to evaluate or provide any reflection on the regulation itself. The M-Bus protocol is standardized in the EU, and will thus be the protocol in focus. Equipment in the scenario will be limited to the one found at SVEA Smart Grid AB, as research purpose is on their behalf. There will be no additional study and analysis of the M-Bus protocol to find new vulnerabilities regarding security.

[6] https://www.enforcementtracker.com/

Chapter 2

Background

2.1 Data collection scenario

Most housing associations today have the same way of measuring the electric energy consumption for their residents. Each residential building has one electrical meter that connects to the electrical grid and measures the total electric energy consumption. The total consumption is then evenly divided and billed over all the apartments, as it is not possible to know if any apartment had higher or lower usage than the other. The proposed solution by SVEA Smart AB is to act as a middle hand between the electricity provider and the housing association and its residents. SVEA Smart AB installs their own electrical meters and measures each resident's individual consumption. This setup allows the housing association to see the apartments individual electrical energy consumption and allows them to more correctly bill for electrical energy consumed. A visualization of the system can be seen in figure 2.1. The electrical meter system that SVEA Smart Grid AB installs, consists of three main devices. Firstly the electrical energy meter; secondly, a gateway capable of communicating via the M-Bus protocol and finally a microcontroller unit (MCU). The MCU enables internet connectivity for the system so that the data can be uploaded to a web service.

Further on, the SVEA Smart Grid AB solution allows further integration of sensor devices within the housing. These devices could include sensors that report indoor climate, i.e. temperature, humidity, air quality and status of emergency equipment such as smoke detectors. This data can be used by the housing association to get an insight into the current and prior climate in their

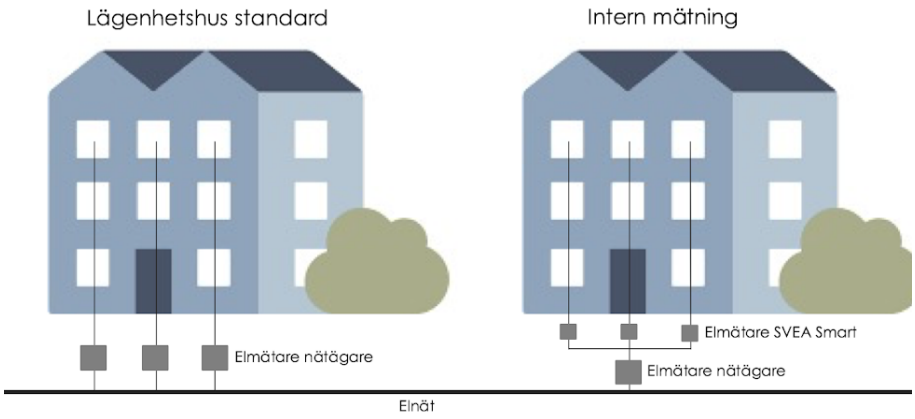

Figure 2.1: Electrical metering system. Reproduced with permission of SVEA Smart Grid AB

apartments. With this knowledge, the housing association can then try and see if there is any form of correlation between electric energy consumption and indoor climate. If such is the case, then it could, for example, be a sign of the residential housing needing renovation as it is badly insulated. Depending on the intentions and goals of the housing association, other types of personal data could potentially be collected as well. This could lead to personally infringing data being collected.

As residential housings can vary in both size and distribution of the apartments, the implementations of the system will differ. Some might require strategically placed repeaters that extend the wireless range of the sensors, allowing them to be placed further away from the main gateway. Some buildings share a main electrical meter, which means that the wired M-Bus alternative might be reliable for locations where the use of repeaters is unavailable. Because of this, the system needs to be flexible in order to be a viable solution for the majority of buildings that could exist.

2.2 Privacy and legislation

In the year of 2018, the General Data Protection Regulation, the GDPR, was enforced across the EU. It introduced large reforms on principles of data protection with a focus on the individuals right. The regulation also alters how businesses and organisations may handle or process the information, with potential for large fines if failing to do so properly [10]. The GDPRs overarching framework is often represented as seven key principles, as stated in the EU's *Handbook on European data protection law*, namely the following [11, pp. 115-116]:

General Data Protection Regulation - Seven key principles

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

The intention of the GDPR is not to restrict nor limit the collection or processing of personal data. The regulations establish that there must be a legitimate reason which justifies the need for collecting the data. It also requires that the data controller[1], must be fair and transparent in what data is being collected. Such that an individual is aware of what type of data is being collected, how much, during what time period and for how long the data will be stored. The individual always has the right to request its removal [10]. The latter regulation is based on Article 8 of the *Charter for Fundamental Rights of the European Union*, and states that "Everyone has the right to the protection of personal data concerning him or her."[2]. Further on, the GDPR also imposes boundaries for the correctness of the personal information collected, that it is relevant and up to date[3] [11].

[1] A term declared in GDPR as "Whoever determines the means and purposes of processing the personal data of others is a 'controller' under data protection law; if several persons take this decision together, they may be 'joint controllers'." [11, p. 101]

[2] https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data

[3] https://gdpr.eu/article-1-subject-matter-and-objectives-overview/

2.3 M-Bus and wireless communication

The M-Bus protocol and its corresponding wireless complement, wM-Bus, is an interface for primarily reading heat, gas and electrical meters [12]. The interface has been standardized in the EU by the European Committee for Standardization and is explained by the EN 13757 standard [13]. The OMS group defines systems standards in Europe for smart metering. The specification is primarily developed to provide the industry with a future-proof communication standard. A standard that enables the use of various sensors and meters in one unified network system [14]. The current OMS group standard supports uni- and bidirectional communication via gateways and meters using wM-Bus, and a specification for wired M-Bus is currently under development [15].

The wired M-Bus system is hierarchical and consists of a master that controls communication and several slaves that reports data to the master. It is physically implemented with two-way communication between the master and slaves with either a star or strand topology network [6]. To accomplish different bit values between master and slave, there is a change in either voltage or current in the physical medium between them. Whenever the master communicates to the slave it uses voltage modulation where a logical 1 corresponds to +36V DC and a logical 0 corresponds to +24V DC. The slave uses current modulation to communicate back to the master, where +1.5mA corresponds to a logical 1 and a logical 0 is read somewhere between +11mA and +20mA [16].

The wireless M-Bus protocol functions similarly to wired M-Bus, in that it is hierarchical and can be implemented with the same topology structure. The protocol stack for wM-Bus is defined by several of the EN 13757-x standards[4]. The stack consists of four layers; application layer defined by EN 13757-3, network layer defined by EN 13757-5, data-link and physical layer defined by EN 13757-4[5]. The traditional OSI model contains three more layers, but are not used by the wM-Bus protocol since it is not a traditional network. The simplicity and low overhead of the wM-Bus stack make it energy efficient [17]. Even though the M-Bus and wM-Bus protocols are certified standards, there are possibilities for manufacturers to produce slightly modified variants in the application layer or so-called dialects. This opens up for developers to integrate different application layers not specified in the EN 13757-x standards [18].

The wM-Bus package frame is structured according to table 2:1 [19].

[4]The notation -x includes all of the standards under EN13757.

[5]The data link and physical layer in the wired M-Bus protocol is defined by EN 13757-2.

1 Byte	1 Byte	2 Bytes	6 Bytes	1 Byte	n Bytes	1 Byte
Length	C	ManID	Address	CI	AppLayer	RSSI

Table 2.1: wM-Bus frame structure.

The first field in the frame specifies the length of the active data in the telegram. The C field declares the message type. ManID is the manufacturer ID. The Address field contains the address of the sender. CI declares the communication layer, the transport direction and application protocol. AppLayer contains all the active data, generated by the application layer. RSSI contains information about the signal strength [14].

The wM-Bus protocol communicates on three different bandwidths and utilizes different modes for communication. The standard specification for wM-Bus supports several modes, such as mode S, T and N. A summary of the different modes and bandwidths can be seen in table 2:2 [20].

Mode	**Frequency**	**Range**	**Characteristics and usage**
S1	868 MHz	500m	Few daily transmissions. Optimized for stationary operation. Unidirectional.
S2	868 MHz	500m	Same as S1. Bidirectional.
T1	868 MHz	500m	Frequent transmissions. Unidirectional.
T2	868 MHz	500m	Same as T1. Bidirectional.
N1a-f	169 MHz	2000m	Narrowband transmission. Unidirectional.
N2a-f	169 MHz	2000m	Same as N1a-f. Bidirectional.

Table 2.2: Representation of wM-Bus modes and frequencies.

All modes support both unidirectional and bidirectional[6] communication. The latter mode is used for polling between master and slaves. Mode S and T both support 433 MHz bandwidth for whenever the 868 MHz alternative is not allowed on the market or in the country [17]. Utilizing the N mode at 169 MHz to transmit packages leads to reduced path loss for the propagating

[6]Two-way communication, but never simultaneous transmission.

signal compared to the 868 MHz alternative [21]. Propagating data at the lower frequency demands more energy than on the 868 MHz counterpart, but is according to Squartini et al. a viable option whenever building a wireless M-Bus network [22].

There are known vulnerabilities and shortcomings within the wM-Bus protocol, even though it today utilizes AES-128[7] encryption for communication. These vulnerabilities have been identified and published by Compass Security AG in an attempt to verify the robustness and reliability of the protocol in 2013 and 2014 [8]. At the time of the publication, the wM-Bus protocol only supported encryption key length of 64 bits. After Compass Security AG published a report detailing general security issues with wM-Bus, the OMS group updated the wM-Bus standard[8]. This countermeasure update included two new modes in the protocol, mode 7 and 13. Mode 7 added additional support for AES-CBC using dynamic keys, and mode 13 added TLS 1.2[9] support for wM-Bus [23].

Compass Security AG claimed that the protocol was not secure enough to be a reliable standard, mainly because of missing support for authentication in the protocol. Since then, the OMS group has declared a more recent standard[10] in 2019 that supports authentication in combination with the other security modes. The essence of the authentication is done by providing a Message Authentication Code (MAC) that is encapsulated in one Data Link Layer [14]. The wM-Bus protocol is today still vulnerable to sniffing and Man In The Middle attacks that modify or delete data. By doing this, either the consumer using the wM-Bus system or a third party entity can modify or falsify data being sent [23].

[7] Advanced Encryption Standard 128. The symmetric cypher used for key encryption.
[8] OMS Specification Volume 2 Primary Communication Issue 4.0.2.
[9] Transport Layer Security 1.2 defined in the RFC-5246 standard.
[10] OMS Specification Volume 2 Primary Communication Issue 4.2.1.

Chapter 3

Method and Implementation

3.1 Requirements elicitation

The design science framework in use throughout the thesis is based on the requirement specification chapter in the book *Design Science Methodology* by Roel J. Wieringa. The methodology describes how to justify choices regarding design decisions based on a contribution agreement[1]. It also defines different kinds of requirements and indicators and norms which serve as motivation and evidence for the necessity of the requirement [24]. Wieringa classifies requirements in two different ways; functional requirements which describe a wanted functionality of the product and non-functional requirements that refer to qualitative properties. Such properties are for example requirements on accuracy, usability or efficiency of the product [24]. The process of identifying requirements is performed by conducting a semi-structured interview and a literature study.

3.1.1 Semi-structured interview

To identify the current state and requirements of the system, a semi-structured interview with the business and system stakeholder at SVEA Smart Grid AB is conducted. The authors of the thesis are the extractors in the interview scenario and the stakeholder is the respondent. The extractors present prepared questions for the respondent during the interview, and the answers are recorded. Interview guidelines are also used to keep the semi-structured interview non-

[1] Used whenever the stakeholder does not directly specify a requirement.

formal. The recorded interview is transcribed to identify the stakeholders desired requirements and properties of the system [25]. The questions and guidelines used during the interview can be found in Appendix A.

3.1.2 Literature study

A literature study is performed to identify existing external requirements and standards for the system. The literature study together with the interview lay the foundation for the system requirement specification to be defined. In order to perform research on the subject field, a wide search is conducted. The study includes earlier publications, technical documents and standard documents.

Prior studies

The initial part is a wide search on some common publication databases such as *Google Scholar*, *IEEE Xplore*, *Scopus*, *ACM Digital Library* and *KTH Primo*. The publications found in this part of the literature study are used throughout the thesis. They act as a knowledge-base for work that has already been conducted within the field. The found publications include whitepapers, conference proceedings and peer-reviewed publications.

To find relevant publications in the databases, the following keywords are used either individually or in combination: IoT, M-Bus, Wireless M-Bus, GDPR, privacy. In order to narrow the results, limiters are applied to the search results where possible. Boolean operators are used to combine certain keywords, for example, 'IoT' and 'M-Bus' with the AND operator. The search results are also filtered to only show matches where the title or abstract contain the keyword. Only publications in English or Swedish are included in the study. Should the number of search results still exceed what is reasonable to sort through, only the first 50 are processed, as they are sorted by relevance.

Publications regarding M-Bus older than 10 years are avoided in favour of new ones. This seems appropriate since even though there may be newly defined standards, it often takes time before they are implemented in devices found on the market. In the case of protocol standards and legislation, the latest available versions are aimed to be used.

Technical reports and manuals

The second part of the literature study is done by reading manuals and technical reports that have been published by manufacturers. M-Bus protocol manuals

are used heavily to describe the functionality of the protocol. Those published or confirmed by the OMS group are assumed relevant and reliable and are thus used in the thesis. Technical reports from other sources than the OMS group are also used to get a non-biased analysis on the technology used.

Legal and standard documents

The final part is done by identifying and reading legal and standard documents. The scope of the documents is related to the privacy and GDPR questions raised earlier in the thesis. Since the GDPR was formed by the European Union, for the European Union, direct sources from any EU agency is to be considered reliable in this thesis. Sources explaining the legal terminology may be used if the source includes references to the original regulation document for the GDPR[2].

3.2 System requirement specification

The requirements will be specified with influence from the IEEE recommendations for 'Software Requirements Specifications'. A few good characteristics of a requirement is that it should be correct, verifiable, unambiguous and ranked for importance. The ranking is used to differentiate the requirements internally when implementing the system. The ranking ranges from very high, to low. A requirement with a higher ranking should be prioritized over one with a lower, but all requirements should be met at some point in time [26, 27].

Defining the requirement specification for the system is performed in three ways. Firstly, identifying internal stakeholder requirements, both existing and innovative, from the semi-structured interview. Secondly, identifying external stakeholder requirements and regulations, such as the GDPR from the legal documents[3]. Thirdly, by identifying requirements from the studies of the M-Bus protocol.

[2]Regulation (EU) 2016/679 of the European Parliament and of the council [10].

[3]IEEE states that local regulatory authorities should be viewed as a second stakeholder since they assert external requirements for the system [27].

Chapter 4

Results

4.1 Internal stakeholder requirements

4.1.1 Semi-structured interview

The interview conducted on the 8th of March 2020 with the internal stakeholder at SVEA Smart Grid AB was performed in a non-formal manner. The extractors decided to present rather vague questions instead of direct ones that unwillingly might bias the interview. The conceptualized system is in early development and there are no established design decisions yet, except that it should be compatible with the existing one. Because of this, using vague questions regarding the system design and requirements opened up a discussion between the extractors and the respondent. The discussion brought forth several new ideas and through this, the stakeholder/respondent could establish functional and qualitative needs. By analyzing what was brought up during the interview it was possible to define system requirements. The defined functional and qualitative requirements for the system can be seen in table 4.1 and the qualitative requirements are explained in text thereafter. Following are some excerpts from responses of the internal stakeholder that helped define said system requirements.

Interview responses

Upon asking about functional requirements the internal stakeholder responded that *"På vår nuvarande plattform så kan de boende se statistik över deras elförbrukning, och vi vill att de ska kunna få samma överblick över annan data också."* [On the current platform, the residents can view statistics of their

electricity consumption, and we want them to get the same overview of other data as well.]. Further on, it was added that the housing association should be able to view the statistics in a similar manner. When discussing what the system currently looks like and what functionality is desired in the future, the stakeholder stated that *"Det viktigaste är att nya funktioner kan integreras i det nuvarande systemet."* [The most important aspect is that the new functions can be integrated in the current system.]. Thus it needs to be compatible with the current M-Bus solutions used, so easiest is to keep using M-Bus devices when expanding.

Regarding the operating environment conditions the stakeholder stated that *"Vi använder oss av molntjänster för lagring i dagsläget, så en stabil uppkoppling krävs."* [We are currently using cloud services for storage, so a stable connection is required.]. Most of the time a wired connection is possible, but sometimes they have to rely on 4G modules when wired options are unavailable. Further on they mentioned that the location for the installed system and the materials in each building varies a lot. Some have thick concrete walls that might make it so the wireless signal won't reach the repeaters. The signals thus need enough strength to reach the repeaters.

The internal stakeholder stated that the electrical meters have a certain precision of decimals and that they want the same accuracy for the M-Bus sensors if possible. It was also mentioned that rounded integer values might be acceptable in some cases, for example, temperature, as it does not differ that much between $23°$C and $24°$C.

Functional requirements

FR ID	FR Description	Importance
FR.01	Statistics of collected data shall be available to the customer through the platform.	very high
FR.02	The sensors in the system shall be able to report their battery health status.	very high
FR.03	There shall be an internet connection available to the system.	very high
FR.04	The upload of the data to the web service shall use a reliable transmission protocol.	very high
FR.05	The upload of the data to the web service shall be encrypted.	very high
FR.06	Statistics of collected data shall be available to the resident through the platform via a unique access token.	high
FR.07	The system shall be restricted to the use of the M-Bus protocol for data collection.	high
FR.08	The system shall be configurable over the air on the interval of data retrieval.	medium

Table 4.1: Functional requirements for the system determined by the internal stakeholder.

Qualitative requirements

The wireless devices in the system shall support transmission ranges up to 2000m.

- The installation site for the system might vary greatly. Taking various factors into account such as thick concrete walls, long ranges between gateway and apartments, tall buildings, etc. the minimum transmission range of 2000m was decided, to have a clear lower boundary.

The sensor devices measuring temperature shall have a resolution of at least one decimal place.

- The majority of OMS-group certified M-Bus temperature sensors on the market support resolutions of one or more decimal places, but some sensors have a margin of error greater than 1°C for certain temperatures.

The sensor devices measuring temperature shall have a maximum deviation in measurements of 0.3 units.

- The majority of OMS-group certified[1] M-Bus temperature sensors have a margin of error somewhere between $\pm\ 0.2°$C and $\pm\ 0.6°$C for temperatures ranging between $0°$C and $30°$C. The intended use for the sensors is in residential areas, which generally keep a temperature of around $20°$C.

The sensor devices measuring humidity shall have a maximum deviation in measurements of 3 per cent RH[2].

- For the average M-Bus humidity sensor[1], the RH levels ranging from 10% to 90% have a margin for error around $\pm$ 2%. Extreme conditions such as below 10% RH or above 90% RH has a margin of error around $\pm$ 4%.

4.2 Literature study

4.2.1 General Data Protection Regulation

The study of the GDPR was done by reading the official legal document [10] and various relating EU sources explaining some of the legal terminology used. The GDPR acts as an external stakeholder for the system. The GDPR uses specific terminology, and definitions for the terms can be found in the System Requirement Specification included in Appendix B [11]. The identified functional system requirements can be seen in table 4.2 and the qualitative requirement is explained in plain text.

[1] https://oms-group.org/en/product-certification/certified-products

[2] **RH** - Relative Humidity

Functional requirements

FR ID	FR Description	Importance
FR.09	When personal data is transmitted to the gateway, the system shall encrypt the data to the extent possible of the communication protocol.	very high
FR.10	When personal data is stored, the system shall encrypt, psuedonymize or anonymize the data to the extent possible.	very high
FR.11	When the customer requests personal data, the system shall provide the data to them within a month.	very high
FR.12	When the customer requests the removal of personal data, non-compulsory data shall be removed.	very high
FR.13	When a customer requests cessation of personal data processing, the system shall stop processing the customers non-compulsory data.	high
FR.14	When a customer changes controller, the customer shall be able to export the personal data from the current controller.	medium
FR.15	If personal information is incorrect, the information shall be corrected by the data subject.	medium

Table 4.2: Functional requirements for the system based on GDPR and legislation.

Qualitative requirement

The data collection shall be justified by a lawful basis.

- There must be a lawful basis established that justifies the collection and processing of the personal data. The basis must establish the necessity of the purpose for which the data is collected. It should be determined beforehand and not be altered at a later date without a new consent given. The notice given to customers should include this basis as well as the purpose of the processing.

4.2.2 M-Bus systems

In a technical report by Silicon Labs, Vivek Mohan details information and guidelines on how to set up a wM-Bus solution [28]. Mohan presents several core components that are required to achieve a high-performance wM-Bus solution. The first requirement is a low-power MCU to achieve wanted power usage since the protocol is designed to be power efficient. The second requirement is a high-performance radio transceiver that operates at sub-GHz frequency. The wM-Bus protocol standard specifies frequency modes ranging from 169 MHz to 868 MHz, so a transceiver operating outside of that frequency band is redundant. The third requirement is a wM-Bus software stack that is flexible enough to support various security features and wireless communication requirements. The final requirement is an evaluation tool used to verify prior requirements and later deploy the solution. Because the wM-Bus protocol has low overhead, the software stack can be implemented on 32KB of flash-memory according to Mohan. By doing this, the possibilities to use smaller and cheaper MCU's arise [28].

The wM-Bus protocol is according to Flammini et al. [20] lacking regarding the time representation. The OMS standard defines time encoding in five different modes[3] based on what application layer is being used. The protocol utilizes a synchronization mechanism in order to synchronize all M-Bus devices on the same network. This is done with mode I and the field consist of 3 words[4]. The field is divided into groups which represent time units such as year, month, day etc. The most accurate time precision among the different modes is in seconds. Flemmini et al. state that because of this, the wM-Bus protocol is not suitable for advanced measurements and the native synchronization mechanism require an improvement [20].

Mihajlović et al. [29] published a report in 2016 detailing how a universal electronic device can be used both as a gateway and a concentrator[5] for automatic reading M-Bus systems. The device was developed and designed with consideration to the Dutch Smart Meter Requirements. Because of this, the functionality of the device is heavily based on the standards and requirements found in Germany. In the report, Mihajlović et al. presented five specific requirements for the device, which can be summarized by:

[3] Mode F, G, I, J, K.
[4] 48 bits, each word is 16bits.
[5] Collecting and redistributing data records from meters.

- It must be a microcontroller-based system that supports communication over several protocols.
- The system must support both wired M-Bus and wM-Bus.
- The system must consist of a gateway with functionality that transmits the data to a server.
- The system power supply must be modular to streamline the installation process.
- The system software can be changed over the air.

The focus of the design was modularity and flexibility, which enabled the device to be used in multiple scenarios and for diverse applications. Mihajlović et al. analyzed how external factors impacted the communication quality. The analysis concluded that the meters could always communicate with the concentrators at a range of 100m, thus making the device both reliable and flexible [29].

Zeman et al. [19] published a paper in 2017 named "Wireless M-Bus in Industrial IoT: Technology Overview and Prototype Implementation". In this paper, Zeman et al. detailed a technological overview of the wM-Bus protocol within an industrial IoT environment. The overview contained a section where Zeman et al. explored the wM-Bus data frame structure. Tests were conducted where they sniffed both unencrypted and encrypted data telegrams. The encryption used was AES-128, but Zeman et al. were still able to extract valuable data from the telegram. The extracted data contained; information detailing what encryption was used, the compilation of the encryption initialization vector and the encrypted data. Through this, the relevant AES-128 key could be downloaded and thereafter the telegram was decrypted and the data could be accessed[6]. Zeman et al. mention that the data packages are not implemented similarly across different manufacturers, which means that the sniffed data has to be analyzed individually depending on the device. Because of this, it is recommended to only rely on one manufacturer to keep the data packages consistent in the system [19].

The identified functional requirements can be seen in table 4.3 and the qualitative requirements are described in plain text.

[6]Further parsing of the telegram is needed to retrieve the wanted data.

Functional requirements

FR ID	FR Description	Importance
FR.16	The radio transceiver in the sensors shall operate at the defined wireless M-Bus frequencies.	very high
FR.17	The wM-Bus software stack used shall support encryption.	very high
FR.18	The system shall support the wired M-Bus protocol.	very high
FR.19	The system shall support the wireless M-Bus protocol.	very high
FR.20	The system shall contain a gateway that collects data from the sensors.	very high
FR.21	The system shall contain a MCU that uploads the data from the gateway to the web service.	very high
FR.22	The wM-Bus software stack used shall support authentication.	high

Table 4.3: Functional requirements for the system identified from prior studies in the field.

Qualitative requirement

The M-Bus devices in the system shall be limited to at most two different manufacturers.

- Manufacturers might construct their data packages differently. Thus by only relying on a small number of manufacturers, the reading and parsing of the data packages will become a more streamlined process.

4.3 Requirement specification

A composition of the identified system requirements can be found in the System Requirement Specification included in Appendix B. It is a complete SyRS document written according to the IEEE standard [27]. The requirement definitions are specified according to *Design Science Methodology* by Wieringa [24].

4.4 Conceptual redesign of system

4.4.1 General Data Protection Regulation

As a result of the analysis of the systems GDPR compliance, aspects which complied with regulations and some that did not were identified (FR.09-15). One of the most important aspects is the lawful basis for data processing, in accordance with article[7] 6. The company SVEA Smart Grid AB will collect the data as a service offered to the Housing Association. Some of the data is required to be collected as it serves as the basis for electrical bills. If environmental data is opted to be collected as well, it could be justified by the Swedish law (2014:267) *"Lag om energimätning i byggnader"* [Energy measurements in Buildings]. The law states that such data should be collected in each apartment if deemed cost-effective.

Other aspects of the GDPR refer to the security of the personal data during storage and transmission. The transmitted and stored data shall be encrypted and anonymized, pseudonymized or encrypted. In the system analyzed, three phases which this would apply to were identified. The first stage is the collection and transmission of the data from the sensors to the gateway. At this stage, the data can be encrypted according to the M-Bus protocol as aforementioned, but it is not pseudonymized. The second stage is the storage of the data within the gateway and electrical meters, where it is neither possible to encrypt nor pseudonymize with current hardware. The final stage refers to the transmission of the data from the gateway and MCU to the cloud service. During this stage, it is still not pseudonymized but is transferred according to secure communication protocols, in this case, HTTP over TLS.

As evident, the most susceptible stage is the storage of personal data within the gateway - where the suggested improvement is to limit unauthorized access by requiring authentication. Any remote access to the device should also use built-in encrypted alternatives over the non-encrypted. In regards to anonymization and pseudonymization of the data, it is currently tied to apartment units and not directly tied to individuals. It is suggested that apartments are replaced by a unique string such as UUIDs for better pseudonymization. The connection between the UUIDs should preferably be stored separately from the data.

[7] https://gdpr.eu/article-6-how-to-process-personal-data-legally/

4.4.2 M-Bus protocol

The M-Bus protocol was deemed to be compliant with the possible identified security aspects and GDPR according to the studied research (FR.16-22). The aforementioned security flaws within the protocol have been updated by the OMS group in later standards, thus adding extra security to the protocol. There were some vulnerabilities and aspects identified which could be improved to make the protocol a more reliable standard.

Zeman et al. sniffed data packages when using wM-Bus and were able to retrieve the encrypted data. Zeman et al. were able to do this because the data package also contained the initialization vector used for the AES-128 encryption, and could through this download the relevant key to decrypt the data [19]. It was determined that a user would require intrinsic knowledge about the sensors in order to decrypt and modify transmissions. The weakness identified was in using a pre-defined initialization vector for encryption set by the manufacturer. The suggested modification would be to allow the use of a user-defined initialization vector and encryption key.

The M-Bus protocol is not suited for advanced measurements according to Flammini et al. because of the lacking precision in time representation. The current most accurate time precision is in seconds, and this causes the devices in M-Bus systems to become unsynchronized at times. Flammini et al. proposes that the native synchronization mechanism needs improvement in the M-Bus standard [20]. This weakness can be mitigated by modifying the AppLayer field in the data frame. The AppLayer contains data constructed by the M-Bus application layer and one could increase the number of bits used to represent time. The M-Bus stack is as mentioned highly customizable and developers can implement their desired functionalities in the application layer. DLMS/COSEM is an application layer which can represent time to the hundredths of a second, making it suitable for more advanced measurements [20]. This could improve time representation and theoretically prevent the devices from becoming unsynchronized.

Chapter 5

Discussion

The enforcement of the GDPR is making it more challenging to deploy systems like the one analyzed. Even if the guidelines are rather straight forward to understand, one is easily overwhelmed by the sheer amount of regulations. There is always room for own interpretation of legislative publications, which could prove economically disastrous if interpreted incorrectly.

A common practice when dealing with data collection is to rely on so-called cloud providers for data storage and services, which raises several questions. It is often not specified exactly how or where the data is stored and this might be in conflict with the GDPR. We thus recommend that an investigation of the cloud service is carried out before integrating it in the system. This is to make sure that the provided solution is secure enough and that it complies with the GDPR and local legislation.

In regards to the issues found with the lack of encryption of the stored personal data, we suggest some other solutions. One solution could instead be to employ "software" encryption on their own throughout the system if supported by the hardware. Thus they do not rely on any other party to encrypt and secure their data. However, it requires more processing power and knowledge to employ this solution. This would safeguard against any physical/remote attacks against the gateway in the building but also if the database in the web service should be compromised in some way, which is not unheard of.

Regarding the inaccuracy in time representation that Flammini et al. proposed; we do not consider this to be a big issue for this use case. The current system does not send multiple packets per second nor does it require such high precision timestamps for its measurements. It is, however, good to incorporate the

possibility to have high-resolution timestamps for the system to be scalable and modifiable. Since the application layer is open for modifications there are no restrictions in the standard itself.

One limitation throughout our work has been when trying to access standard documents. For example, when investigating the M-Bus protocol we sometimes had to rely on secondary sources as most of the up to date standards must be purchased. This made it difficult to fully explore all the details and features of the protocol.

We believe that the conducted work is relevant to the problem brought to us by SVEA Smart Grid AB. If they follow the presented SyRS, they should have a good foundation for a secure M-Bus based system that complies with the core GDPR demands. Although, parts of the GDPR might be oversimplified as there might be more parties[1] involved that have to take responsibility for the data collection.

Even if the work was targeted to SVEA Smart Grid AB's needs, one can still conclude best practices for M-Bus based systems from the work done. As the discussed conceptualized system is flexible and can be installed in a majority of facilities; we consider that the produced SyRS can be generalized and used as a boilerplate for similar systems.

5.1 Conclusions

We concluded that the conceptualized system has a few flaws in terms of GDPR compliance. Both technical and administrative work is needed in order to completely comply. The administrative work relates around appointing a GDPR responsible spokesman at the organization and the technical work focuses on how the data is processed, stored and transmitted. The M-Bus protocol is according to us a fitting choice for this type of system. It is a well-known standard in Europe and the standard has undergone several updates that improve on the protocols security aspects. We consider it to be sufficiently secure when the wM-Bus protocol operates in Mode 7 or 13, utilizing AES128-CBC or TLS 1.2. Wireless systems will always be susceptible to network attacks. For example, as Zeman et al. showed, data packages transmitted with wM-Bus can still be exposed to Man in The Middle Attacks and be sniffed and decrypted.

[1] Parties other than SVEA Smart Grid AB, such as the companies providing cloud services or the housing association.

5.2 Future work

Even if M-Bus is a well known and employed standard, other types of protocols could be investigated. For example, LoRaWAN, Low-power Wide-area Network, could be an alternative as it also offers high energy efficiency, long-range and low cost for devices. It was also specifically developed with IoT devices in mind.

As mentioned in the discussion, there were some limitations on how thoroughly we were able to analyze the M-Bus protocol. There is certainly room for a more deep dive into the protocol if one has access to the complete standard. Similarly, this would apply to other protocols, if others are to be investigated.

We would also recommend further work into investigating GDPR and other legislation for similar scenarios. There may, for example, be more complications with cloud services and GDPR that are not mentioned in the discussion. There often exist local legislation detailing where, i.e. geographic constraints, data is allowed to be stored and one should investigate this before fully deploying the system.

Finally, the system could be evaluated by another methodology with another perspective. As the conceptualized system will be deployed widely, it is susceptible to malicious attacks and a threat modeling approach could prove useful. It is a methodology that has gained traction in the recent years, as can be seen by the numerous amount of related articles covered in a systematic literature reviewed by Xiaong and Lagerström [30]. We would suggest the pwnPr3d approach developed by Johnson et al [31] instead of evaluating the system against literature and the system requirement specification. It is a probabilistic threat modeling approach used to provide stakeholders with a comprehensive high-level overview and technical insight into the system. The results from this methodology could then have been evaluated against GDPR and M-Bus in a similar manner.

Bibliography

[1] Véronique Heiwy. “Design Guidelines for the Internet of Things”. In: *Proceedings of the 15th Ergo’IA “Ergonomie Et Informatique Avancée” Conference*. Ergo’IA ’16. Bidart, France: Association for Computing Machinery, 2016. ISBN: 9781450347853. DOI: 10.1145/3050385.3050392.

[2] Jibran Saleem et al. “IoT Standardisation: Challenges, Perspectives and Solution”. In: *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*. ICFNDS ’18. Amman, Jordan: Association for Computing Machinery, 2018. ISBN: 9781450364287. DOI: 10.1145/3231053.3231103.

[3] P. Masek et al. “A Perspective on Wireless M-Bus for Smart Electricity Grids”. In: *2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*. 2019, pp. 730–735.

[4] *Communication from The Commission to The European Parliament, The Council, The European Economic and Social Comittee and The Committee of The Regions, "Addressing the challenge of energy efficiency through Information and Communication Technologies"*. Comission of The European Communities. May 13, 2008. URL: https://ec.europa.eu/information_society/activities/sustainable_growth/docs/com_2008_241_all_lang/com_2008_241_1_en.pdf (visited on 04/23/2020).

[5] *Energy, transport and environment statistics : 2019 edition*. Luxembourg, 2019. DOI: 10.2785/66014.

[6] Z. Li-li et al. “Design of a sensor network based on M-Bus”. In: *Proceedings of 2011 International Conference on Fluid Power and Mechatronics*. 2011, pp. 857–860.

[7] W. Anani, A. Ouda, and A. Hamou. “A Survey Of Wireless Communications for IoT Echo-Systems”. In: *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*. 2019, pp. 1–6.

[8] Cyrill Brunschwiler. *Wireless M-Bus Security Whitepaper Black Hat USA 2013 June 30th, 2013*. Rev. 1.01. June 2013, pp. 17–56.

[9] Samuel D. Warren and Louis D. Brandeis. *Harvard Law Review*. Vol. IV No. V. Dec. 1890, pp. 193–220.

[10] Council of European Union. *Regulation (EU) 2016/679 of The European Parliament and of The Council. on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Council of European Union, Apr. 27, 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (visited on 04/02/2020).

[11] *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union, 2018. ISBN: 9789294919014. DOI: 10.2811/343461.

[12] *Overview - M-Bus*. M-Bus. URL: https://m-bus.com/overview (visited on 03/19/2020).

[13] *EN 13757 | European Innovation Partnership*. European Commission. URL: https://ec.europa.eu/eip/ageing/standards/ict-and-communication/data/en-13757_en (visited on 03/19/2020).

[14] *Open Metering System Specification*. Volume 2 Primary Communication Issue 4.2.1 RELEASE. Open Metering System. Nov. 2019, pp. 1–121.

[15] *Open Metering System - OMS Specification*. Generation 4 Specification. OMS. URL: https://oms-group.org/en/open-metering-system/oms-specification (visited on 03/26/2020).

[16] *Wired M-Bus Specification*. M-Bus. URL: https://m-bus.com/documentation-wired/04-physical-layer (visited on 03/19/2020).

[17] P. Masek et al. “Advanced Wireless M-Bus Platform for Intensive Field Testing in Industry 4.0-Based Systems”. In: *European Wireless 2018; 24th European Wireless Conference*. 2018, pp. 1–6.

[18] *Wireless M-Bus Technology Overview*. Radiocrafts AS. URL: https://radiocrafts.com/technologies/wireless-m-bus-technology-overview/ (visited on 03/23/2020).

[19] K. Zeman et al. "Wireless M-BUS in Industrial IoT: Technology Overview and Prototype Implementation". In: *European Wireless 2017; 23th European Wireless Conference*. 2017, pp. 1–6.

[20] A. Flammini, S. Rinaldi, and A. Vezzoli. "The sense of time in Open Metering System". In: *2011 IEEE International Conference on Smart Measurements of Future Grids (SMFG) Proceedings*. 2011, pp. 22–27.

[21] S. Spinsante et al. "Evaluation of the Wireless M-Bus standard for future smart water grids". In: *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*. 2013, pp. 1382–1387.

[22] S. Squartini et al. "Wireless M-Bus sensor nodes in smart water grids: The energy issue". In: *2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP)*. 2013, pp. 614–619.

[23] Cyrill Brunschwiler. *Energy Fraud and Orchestrated Blackouts, Issues with Wireless Metering Protocols (wM-Bus)*. Hack in Paris presentation. Compass Security AG. June 2014.

[24] Roel Wieringa. *Design science methodology for information systems and software engineering*. Heidelberg: Springer, 2014. ISBN: 9783662438398.

[25] Anne Galletta. *Mastering the Semi-Structured Interview and Beyond*. New York University Press, June 17, 2013. 258 pp. ISBN: 0814732941. URL: https://www.ebook.de/de/product/20091877/anne_galletta_mastering_the_semi_structured_interview_and_beyond.html.

[26] "IEEE Recommended Practice for Software Requirements Specifications". In: *IEEE Std 830-1998* (1998), pp. 1–40.

[27] "ISO/IEC/IEEE International Standard - Systems and software engineering – Life cycle processes – Requirements engineering". In: *ISO/IEC/IEEE 29148:2018(E)* (2018), pp. 1–104.

[28] Vivek Mohan. *An Introduction to Wireless M-Bus*. Silicon Labs. URL: http://pages.silabs.com/rs/634-SLU-379/images/introduction-to-wireless-mbus.pdf (visited on 03/19/2020).

[29] Ž. Mihajlović et al. “Implementation of wireless M-bus concentrator/gateway for remote reading of smart gas meters”. In: *2016 24th Telecommunications Forum (TELFOR)*. 2016, pp. 1–4.

[30] Wenjun Xiong and Robert Lagerström. *Threat modeling – A systematic literature review*. QC 20190403. 2019. DOI: 10.1016/j.cose.2019.03.010.

[31] Pontus Johnson et al. “pwnPr3d: an Attack Graph Driven Probabilistic Threat Modeling Approach”. In: *Availability, Reliability and Security (ARES), 2016 11th International Conference on*. IEEE conference proceedings, 2016. DOI: 10.1109/ARES.2016.77.

Appendix A

Interview Questions

- What does the system currently look like? What components are there?
- How do you differentiate the apartments when collecting it?
- How do tenants access the system/website? Authentication?
- Have you considered any other equipment/protocols? (Other than M-Bus)
- Are there any technical requirements wanted for the devices?
- What functionality is desired by the system?
- What functionalities does the customer need?
- What functionalities does the housing association need?
- For how long is the data stored?
- For how long is it required that the data is stored?
- What connectivity options are required?
- Do you know if the collection is justified by Swedish law?
- How is data currently stored?
- Where is the data currently stored?
- Is there any personally identifying information collected?
- If so, is there any kind of anonymization or psuedonymization?

- Should the users be able to refuse to data collection?
- Does the users have the right/opportunity to ask for the removal of their stored personal data?
- What does the situation look like if a new tenant acquires an apartment? Is the statistics of the prior tenant removed? or is the data simply anonymized?
- Does the housing association have rights to view all types of data?

Appendix B

System Requirement Specification

System Requirements Specification

Johan Edman, Wilhelm Ågren

KTH Royal Institute of Technology
Bachelor in Information Technology
Supervisor: Viktor Engström
Examiner: Robert Lagerström
School of Electrical Engineering and Computer Science
Host company: SVEA Smart Grid AB

May 20, 2020

Contents

Revision History **1**

1 Introduction **2**

1.1 Purpose 2

1.2 Intended audience and reading suggestions 2

1.3 Scope 2

1.4 Definitions and acronyms 3

1.5 Sources 4

2 Overall description **5**

2.1 Product perspective 5

2.2 Purpose and benefits 5

2.3 Project scope 5

2.4 User classes and characteristics 6

2.5 Operating environment 6

2.6 Design and implementation constraints 6

3 Functional requirements **8**

4 Qualitative requirements **10**

Revision History

Revision	Date	Author(s)	Description
1.0	2020.04.16	J.Edman, W.Ågren	First draft of document.
1.1	2020.05.11	J.Edman, W.Ågren	Included references/sources for requirements.
1.2	2020.05.13	J.Edman, W.Ågren	Imported operating environment visualization. Restructured user classes and characteristics.

Chapter 1

Introduction

1.1 Purpose

This document aims to give a detailed description and overview of how the platform to be implemented is designed. It will be illustrated through a conceptualized overview of the ecosystem with declaration and explanation. The systems constraints and interaction with other systems will also be stated.

1.2 Intended audience and reading suggestions

The SyRS is mainly intended to serve as a guideline for SVEA Smart Grid AB when implementing their system. It aims to help identify shortcomings with the system in regards to GDPR and relevant security aspects. Companies that are developing an M-Bus based system or want input on such systems may also find the contents interesting. Further information on the requirement specification and the system overall is available in the bachelor thesis that this document was developed in conjunction with.

1.3 Scope

The document will provide descriptions of the conceptualized system and the requirements established by stakeholders. The requirements are restricted and divided into three main parts. Firstly, European Union data legislation, i.e. the GDPR, since the host-company is based in the EU. Secondly, the intentions and desires of the internal stakeholders at the host-company. Thirdly, requirements identified by studying published work that deals with M-Bus reliant systems. The purpose of the requirements is to verify that the system to some extent complies to GDPR and basic security practices. Diagrams will also be provided to give a clear overview of the different actors involved and their interaction.

1.4 Definitions and acronyms

Term	Definition
GDPR	The General Data Protection Regulation is European Union's data privacy and security law and was enforced across the EU on the 25th of May 2018.
Personal Data	"Any information relating to an identified or identifiable natural person, a.k.a. a data subject; an identifiable natural person is one who directly or indirectly can be identified by reference to an identifier. Such identifiers could be; name, identification number, location data, online identifier or one or more of the physical factors such as physiological, genetic, mental, economic, cultural and social identity of that natural person."
Processing	"Any operation which is performed on personal data or a collection of such. Either through automated means, such as collecting, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or in other ways making available, alignment or combination, restriction, erasure or destruction."
Controller	"The entity, be it natural or legal person, agency or organisation, that determines the purposes and means of the processing of personal data."
Pseudonymisation	"The means of processing personal data in such a way that it can no longer be tied directly to a data subject without the use of additional data. Such additional data is kept separately and is not attributed to an identified or identifiable natural person."
M-Bus	The Meter Bus is a serial communication protocol mainly used for remote reading of electricity, water and gas. It is a European standard defined by EN 13757-2 and EN 13757-3. The wireless alternative wM-Bus is further specified in EN 13757-4.
OMS group	The Open Metering System group defines open communication standards based on European norms, focused on the M-Bus protocol.
RH	Relative humidity, which depends on the pressure and temperature of the system.
MCU	A microcontroller unit, used together with a gateway in the system.

Table 1.1: Explaining terms and abbreviations used in the requirements.

1.5 Sources

The requirements regarding GDPR were based upon REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. The following papers were used as sources when identifying requirements from prior studies: Flammini et al.[1], Zeman et al.[2], Mihajlović et al.[3], Vivek Mohan[4].

[1] "The sense of time in Open Metering System", 2011.
[2] "Wireless M-BUS in Industrial IoT: Technology Overview and Prototype Implementation", 2017.
[3] "Implementation of wireless M-bus concentrator/gateway for remote reading of smart gas meters", 2016.
[4] "An Introduction to Wireless M-Bus", 2020.

Chapter 2

Overall description

2.1 Product perspective

The ecosystem to be developed is aimed at housing associations. The system will act as a middle-hand between the electrical meter installed by the provider and the housing association. Its main focus is to provide insight into each apartments electrical power consumption. The system should then be flexible and act as a stepping stone where various types of sensors can be integrated. Thus housing associations can get greater insight into their residential buildings and the apartments.

2.2 Purpose and benefits

The main purpose of this solution is to provide insight for housing associations into their residential buildings. By choosing to install the system from SVEA Smart Grid AB, they do not only get lowered expenses - in comparison to installing a similar system themselves. They also get access to an expandable platform where vital statistics on their properties can be presented.

2.3 Project scope

The expected outcome is a system that measures each apartments electrical consumption and other sensor data. The system redistributes and stores the data for housing associations to monitor the climate and consumption in their buildings. To properly measure the data, a planned installation of the sensors in the system is necessary. Understanding the strengths and weaknesses of the communication protocols used is important to know how the system can be installed and maintained. The system will be used by both housing associations and their residents. The housing association will mainly focus on the overall status of their buildings, and intended focus for the residents is the statistics regarding their indoor climate and electrical consumption.

The conceptualized system is presented in figure 2.1, it illustrates a simplified model for how the housing association and residents interact with the system.

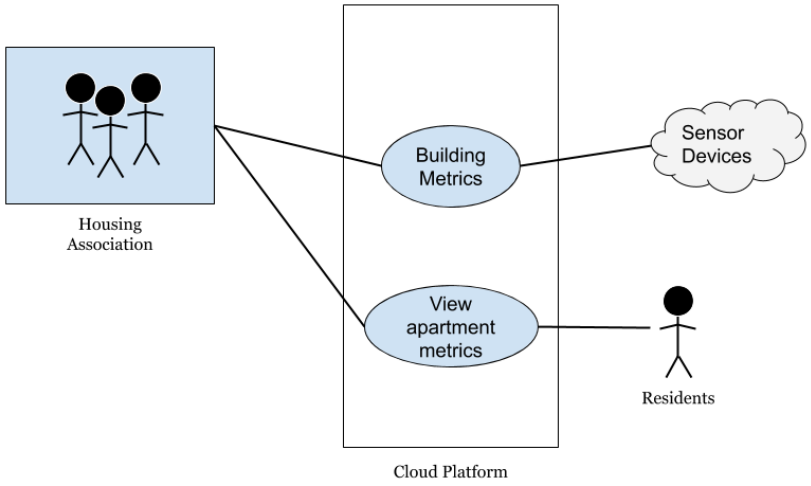

Figure 2.1: **System platform design.**
A conceptual overview of the platform from SVEA Smart AB.

2.4 User classes and characteristics

- **Provider**: Company providing the installation and maintenance of the system.
- **Customer**: Targeted towards housing associations that purchase the system from the provider.
- **Resident**: The residents that occupy the housing associations buildings.

2.5 Operating environment

The system is designed to operate in residential buildings owned by for example Housing Associations. The interaction with the data collected is performed via the platform portal. The different components of the system should be able to be remotely managed and updated from the platform. The operating environment is visualized in **figure 2.2**.

2.6 Design and implementation constraints

The hardware implementation, i.e. the sensors and gateways, must be able to communicate via the M-bus protocol. This data must then be collected and uploaded in a compatible format to the database services being run at a cloud service provider. The database system must be chosen with consideration as there will be large volumes of data as customers increase and time passes.

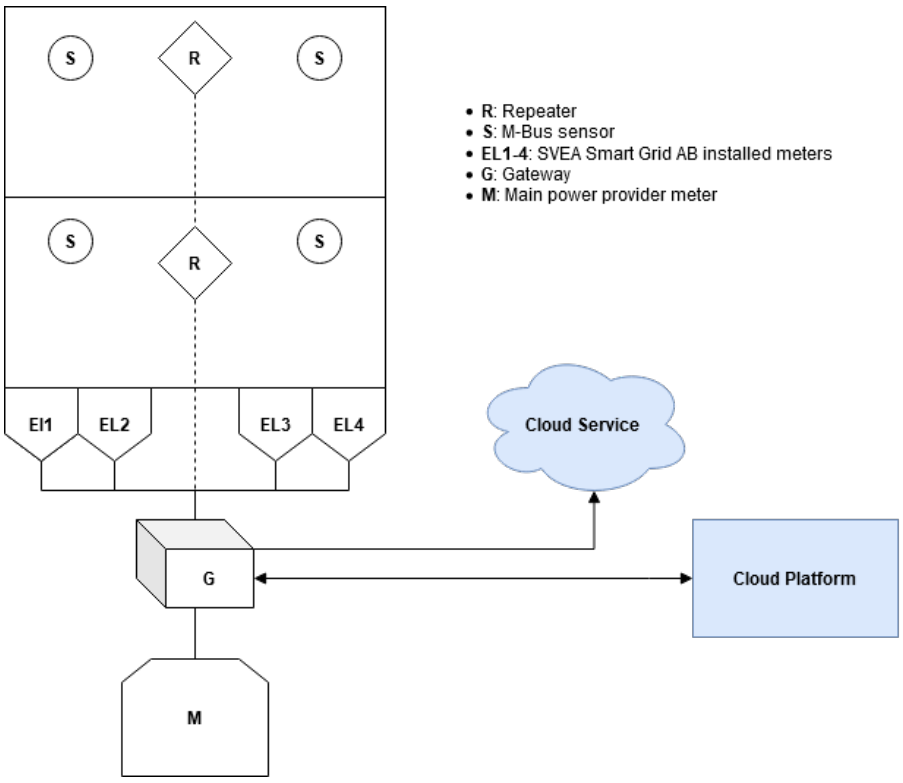

Figure 2.2: **System operating environment**.

Chapter 3

Functional requirements

The functional requirements (FR) are categorized according to the division of requirements mentioned in the product scope. This means that there is one table for GDPR related requirements, one table for internal stakeholder requirements and one for technical requirements.

The tables all follow the same structure. The first column specifies the functional requirement ID (FR ID); the second column describes the requirement in its entirety; the third column details the priority of the requirement in the development phase, relative to the other requirements.

FR ID	**FR Description**	**Importance**
FR.01	When personal data is transmitted to the gateway, the system shall encrypt the data to the extent possible of the communication protocol.	very high
FR.02	When personal data is stored, the system shall encrypt, psuedonymize or anonymize the data to the extent possible.	very high
FR.03	When the customer requests personal data, the system shall provide the data to them within a month.	very high
FR.04	When the customer requests the removal of personal data, non-compulsory data shall be removed.	very high
FR.05	When a customer requests cessation of personal data processing, the system shall stop processing the customers non-compulsory data.	high
FR.06	When a customer changes controller, the customer shall be able to export the personal data from the current controller.	medium
FR.07	The data subject shall be able to edit information within the system.	medium

Table 3.1: Functional requirements for the system based on GDPR & legislation.

FR ID	FR Description	Importance
FR.08	Statistics of collected data shall be available to the customer through the platform.	very high
FR.09	The sensors in the system shall be able to report their battery health status.	very high
FR.10	There shall be an internet connection available to the system.	very high
FR.11	The upload of the data to the web service shall use a reliable transmission protocol.	very high
FR.12	The upload of the data to the web service shall be encrypted.	very high
FR.13	Statistics of collected data shall be available to the resident through the platform via a unique access token.	high
FR.14	The system shall be restricted to the use of the M-Bus protocol for data collection.	high
FR.15	The system shall be configurable over the air in the interval of data retrieval.	medium

Table 3.2: Functional requirements for the system determined by the internal stakeholders.

FR ID	FR Description	Importance
FR.16	The radio transceiver in the sensors shall operate at the defined wireless M-Bus frequencies.	very high
FR.17	The wM-Bus software stack used shall support encryption.	very high
FR.18	The system shall support the wired M-Bus protocol.	very high
FR.19	The system shall support the wireless M-Bus protocol.	very high
FR.20	The system shall contain a gateway that collects data from the sensors.	very high
FR.21	The system shall contain a MCU that uploads the data from the gateway to the web service.	very high
FR.22	The wM-Bus software stack used shall support authentication.	high

Table 3.3: Functional requirements for the system identified from prior studies in the field.

Chapter 4

Qualitative requirements

The qualitative requirements (QR) will be presented in tabular form. The QR are not rated for importance. The first column in the table specifies the ID for the qualitative requirement (QR ID) and the second column describes the requirement. Explanations for each QR can be found below the table.

QR ID	**QR Description**
QR.01	The wireless devices in the system shall support transmission ranges up to 2000m.
QR.02	The sensor devices measuring temperature shall have a resolution of at least one decimal place.
QR.03	The sensor devices measuring temperature shall have a maximum deviation in measurements of 0.3 units.
QR.04	The sensor devices measuring humidity shall have a maximum deviation in measurements of 3 percent RH.
QR.05	The M-Bus devices in the system shall be limited to at most two different manufacturers.

Table 4.1: Qualitative requirements set by external stakeholders, internal stakeholders and prior studies.

- **QR.01:** The installation site for the system might vary greatly. Taking various factors in to account such as thick concrete walls, long ranges between gateway and apartments, tall buildings, etc. the limit of 2000m transmission range was decided to have a clear upper boundary.
- **QR.02:** The majority of OMS-group certified M-Bus temperature sensors on the market support resolutions of one or more decimal places, but some sensors have a margin of error greater than 1°C for certain temperatures.
- **QR.03:** The majority of OMS-group certified M-Bus temperature sensors have a margin of error somewhere between ± 0.2°C and ± 0.6°C for temperatures ranging between 0°C and 30°C. The intended use for the sensors are in residential areas, which generally keep a temperature of around 20°C.
- **QR.04:** For the average M-Bus humidity sensor, the RH levels ranging from 10% to 90% have a margin for error around ± 3%. Extreme conditions such as below 10% RH or above 90% RH has a margin of error around ± 4%.

- **QR.05:** Manufacturers might construct their data packages differently. Thus by only relying on a small number of manufacturers, the reading and parsing of the data packages will become a more streamlined process.

TRITA-EECS-EX-2020:207