Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona
Switzerland

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Wireless M-Bus Security Whitepaper Black Hat USA 2013 June 30th, 2013

Document Name:	compass_security_wmbus_security_whitepaper_v1.01.docx
Version:	v1.01
Author(s):	Cyrill Brunschwiler, Compass Security AG
Date of Delivery:	June 30th, 2013
Classification:	PUBLIC

Executive Summary

Government requirements [1], [2], new business cases and consumer behavioural changes [3], [4] drive energy market players to improve the overall management of energy infrastructures.

While the energy infrastructure is steadily maintained and improved, some significant changes have been introduced to the power grids of late. Actually, the significance of the changes could be compared to the early days of the Internet where computers started to become largely interconnected. Naturally, questions arise whether a grid composed of so many interacting components can still meet today's requirements for reliability, availability and privacy.

Nations absolutely recognise the criticality of the energy infrastructure for their economic and political stability. Therefore, various initiatives to ensure reliability and availability of the energy infrastructures are being driven at nation as well as at nation union levels. In order to contribute to the evaluation of national cyber security risks, the author decided to conduct a security analysis in the fields of smart energy.

Utilities have started to introduce new field device technology - smart meters [5]. As the name implies, smart meters do support many more use cases than any old conventional electricity meter did. Not only does the new generation of meters support fine granular remote data reading, but it also facilitates remote load control or remote software updates. Hence, to build a secure advanced metering infrastructure (AMI), communication protocols must support bi-directional data transmission and protect meter data and control commands in transit.

Therefore, analysis of smart metering protocols is of great interest. The work presented has analysed the security of the Meter Bus (M-Bus) as specified within the relevant standards [6], [7], [8], [9]. The M-Bus is very popular in remote meter reading within Europe and has its roots in the heat metering industries. It has continuously been adopted to fit more complex applications during the past twenty years. According to a workshop note [10], an estimated 15 million devices were relying on the wireless version of M-Bus in 2010. It was analysed whether smart meters using wireless M-Bus do fit the overall security and reliability needs of the grid or whether such devices might threaten the infrastructure.

To justify the scope of the study, a brief introduction into the electrical infrastructure, smart grids and smart metering is provided. Moreover, relevant security standards and guidance are being referenced.

Finally, the M-Bus standard has been analysed whether it provides effective security mechanisms. It can be stated that wireless M-Bus seems to be robust against deduction of consumption behaviour from the wireless network traffic. For this reason, it is considered privacy-preserving against network traffic analysis. Unfortunately, vulnerabilities have been identified that render that fact obsolete. The findings are mainly related to confidentiality, integrity and authentication. It is being emphasised, that all identified issues rely on theoretical verification and pose conceptual issues under certain assumptions whereby only few of the issues have been verified in practise.

However, theoretically, smart meters relying on wireless M-Bus and supporting remote disconnects are prone to become subject to an orchestrated remote disconnect which poses a severe risk to the grid [12]. Further issues may lead to zero consumption detection, disclosure of consumption values and disclosure of encryption keys.

Following that, the availability and reliability of the smart grid may not be guaranteed.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Table of Contents

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

List of Figures

List of Tables

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

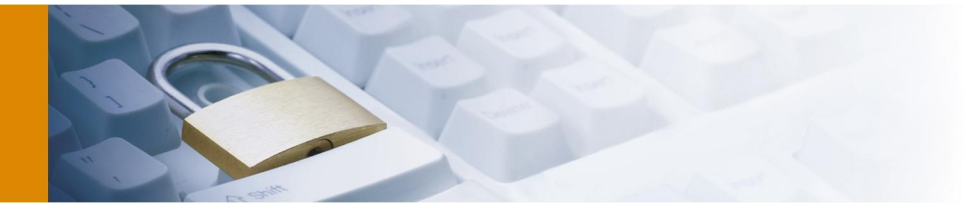
T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

List of Abbreviations

ACC	Access Number
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
AMR	Advanced Meter Reading
ANSI	American National Standards Institute
BAN	Building Area Network
BCP	Business Continuity Management
BS	British Standard
BSI	British Standards Institution
BSI Germany	Federal Office for Information Security (BSI) in Germany
Cx	Ciphertext Block Number x
CBC	Cipher Block Chaining Mode of Operation
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CI	Control Information Field
CIA	Confidentiality, Integrity and Availability
CIRT	Computer Incident Response Team
CMAC	Cipher-based Message Authentication Code
COSEM	Companion Specification for Energy Metering
CPA	Chosen Plaintext Attack
CPP	Critical Peak Pricing
CRC	Cyclic Redundancy Check
CTR	Counter Mode of Operation
D	Detective Control
DAL	M-Bus Dedicated Application Layer
DARPA	Defence Advanced Research Projects Agency
DER	Distributed Energy Resource
DES	Data Encryption Standard
DFD	Data Flow Diagram
DG	Distributed Generation
DIF	Data Information Field
DIFE	DIF Extension
DLMS	Device Language Message Specification
DMZ	Demilitarized Zone
DNAT	Destination Network Address Translation
DoS	Denial of Service
DSL	Digital Subscriber Line
DSO	Distribution System Operator
DSS	Digital Signature Standard
EAX	Cryptographic Mode of Operation for AEAD
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECRYPT II	European Network of Excellence in Cryptology II

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch



ELL	M-Bus Extended Link Layer
ENISA	European Network and Information Security Agency
EU	European Union
ETSI	European Telecommunications Standards Institute
FAN	Field Area Network
FIPS	Federal Information Processing Standards
FOC	Fibre Optic Cable
GPRS	General Packet Radio Service
GND	Common Ground
HLS	High Level Security
HMAC	Keyed-Hash Message Authentication Code
HVAC	Heating, Ventilation and Air Conditioning
EN	European Standard
Enc	Encryption Algorithm
EURELETRIC	Union of the Electricity Industry
EV	Electrical Vehicle
HAN	Home Area Network
HDLC	High-Level Data Link Control
HES	Head-end System
HHU	Hand-held Unit
IAN	Industrial Area Network
ICS	Industrial Control System
IV	Initialization Vector
IoT	Internet of Things
ISMS	Information Security Management Systems
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International organisation for Standardization
IT	Information technology
JAR	Jam and Replay Attack Technique
JTAG	Joint Test Action Group
KEK	Key Encryption Key
kV	Kilovolts
kWh	Kilowatt hour
LMS	Local metrological network
LSB	Least Significant Byte
LSBit	Least Significant Bit
M2M	Machine to Machine
MAC	Message Authentication Code
MDM	Meter Data Management
MitM	Man-in-the-Middle
MK	Master Key
MPLS	Multi-protocol Label Switching
MSB	Most Significant Byte
MSBit	Most Significant Bit
MW	Megawatts
N/A	Not applicable
NAN	Neighbourhood Area Network
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
NRZ	No-return-to-zero line code
OBIS	Object Identification System
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OFB	Output Feedback Mode
OMS	Open Metering System
OTP	One-time Pad
P	Preventive Control

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Px	Plaintext Block Number x
PDU	Protocol Data Unit
PHPDU	Physical Layer PDU
PLC	Power Line Carrier
PQ	Power Quality
prEN	European Draft Standard
PV	Photo Voltaic
RES	Renewable Energy Resources
RFC	Request for Comments
RNG	Random Number Generator
ROM	Read-only Memory
RTP	Real-time Pricing
RTT	Round Trip Time
RxD	Received Data
RSSI	Received Signal Strength Indication
SAR	Shield and Replay
SCADA	Supervisory Control And Data Acquisition
SDL	Security Development Life cycle
SFR	Security Functional Requirement
SMCG	CEN/CENELEC/ETSI Smart Meter Co-ordination Group
SN	Session Number
SRD	Short Range Devices
SSL	Secure Socket Layer
TOE	Target of Evaluation
TLS	Transport Layer Security
TMTO	Time-Memory Trade-Off
TSO	Transmission System Operator
TxD	Transmitted Data
US	United States of America
UML	Unified Modelling Language
VIF	Value Information Field
VIFE	VIF Extension
VLAN	Virtual Local Area Network
WAN	Wide Area Network
Wh	Watt hour

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

1 Introduction

1.1 Overview

This work aims to analyse the security of the Meter Bus (M-Bus [20]) as specified in the relevant International organisation for Standardization (ISO) documentation [6], [7], [8], [9]. M-Bus has its roots in the heat metering industries and was continuously adopted to fit more complex applications. M-Bus is the communication bus of choice of several meter manufacturers and its applications span from drive-by wireless meter reading over to meter-to-meter and mesh networking to meter-to-collector communication. M-Bus implementations support different media types such as power line carrier (PLC) or twisted-pair bus. To avoid the wiring efforts at the distribution level, utilities, metering companies and manufacturers tend to more frequently choose wireless protocols for communication. Accordingly, the analysis will mainly concentrate on M-Bus wireless based communication – wM-Bus.

There are two major questions that this work will attempt to answer. It shall attempt to verify whether the security of M-Bus can still compete with today's challenges and an analysis will be conducted to determine if any known wireless and network security issue apply to M-Bus.

To justify the scope of this paper, chapter 2 and 3 provide a brief introduction into the electrical infrastructure, smart grids and smart metering. It will very briefly discuss the approaches for metering and explain some basic terminology by means of architecture blue prints. It further introduces common threats towards industrial control systems (ICS) and specifically for the smart grid and points out issues for the AMI and meters.

In chapter 4, the wireless M-Bus and the dedicated M-Bus application layer will be introduced. The standard series is then analysed for confidentiality, integrity, availability, authenticity and non-repudiation. The chapter will further outline how already known cryptographic issues apply to the M-Bus. Subsections of chapter 4 will provide modelling and explanation of attack scenarios and their feasibility. The security analysis within that chapter relies on study of current and draft M-Bus standards and a practical analysis of real-world implementations in some points.

Some of the questions being answered in chapter 4 include:

- Does M-Bus defeat eavesdropping and preserve the consumer's privacy?
- Does M-Bus prevent unauthorised modification of data in transit?
- Does M-Bus avoid impersonation and man-in-the-middle attack scenarios?
- Does M-Bus ensure proper key management?

The document will then conclude the security level of M-Bus and point out major issues. It will further recommend topics and fields for future research and appreciate current developments in the fields of M-Bus.

The author is currently not aware of any publicly available security analysis on wireless M-Bus. Although, the Open Metering System Group (OMS Group) and the German Federal Office for Information Security (BSI Germany) have recently undertaken significant efforts drafting improvements for wireless M-Bus. This allows for speculation that some yet undisclosed studies on the security of M-Bus exist. However, the analysis of that draft [13], has not been included as part of this study. Such analysis would definitely contribute to the overview on the wireless M-Bus stack security, appreciate the latest developments and hopefully provide solutions to most of the identified issues.

Generally speaking, the author assumes that legacy protocols need to adopt the core principles of information security soon and well established standards and security protocols will significantly gain momentum. In that context, it is not only interesting to understand whether M-Bus can compete with current challenges but also, whether it can compete against other technology stacks in the long term.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

2 Electrical Grid

2.1 Introduction to Electrical Grids

This section gives a short introduction into electrical grids in general, aims to introduce general terms and to state the difference between the former electrical grid architecture and the smart grid. Additionally, paradigm changes and challenges [3] to the current grid will be pointed-out and the conclusion will include some reasoning for a more flexible architecture – the smart grid.

Electrical grids consist of power plants that create electricity from some form of energy. They consist of towers and poles that hold wires to transport the electricity and finally make it available to the consumer. Figure 1 provides an overview how these facilities are logically grouped into four major domains. The domain concept is not entirely new and was similarly outlined in a description of cyber security on the essential parts of the smart grid [21].

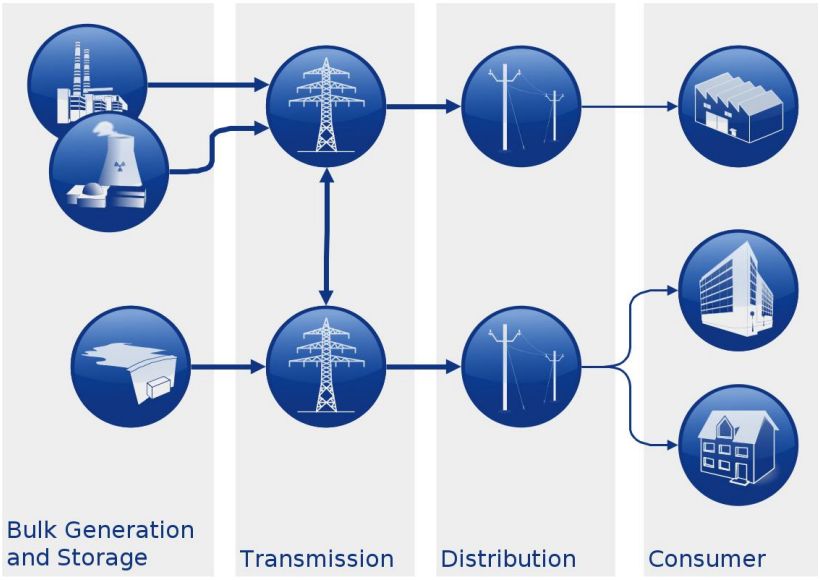


Figure 1: General Electrical Grid Domains and Architecture

Generator domain: includes all sorts of bulk power generation plants such as nuclear reactors, fossil fuel (coal or gas) plants as well as hydroelectricity plants. Typically, these are power plants that can continuously generate electricity of several hundred mega watts (MW).

Transmission domain: represents the long-distance transmission network components. This includes large interconnection nodes, substations or cables either mounted on towers or buried underground. The voltage for transmissions networks is several hundred kilo volts (kV). Among Europe typically values are 230kV and 400kV. Traditionally, the domain is under control of the transmission system operator (TSO). In some countries a national body or a super body of utilities operates that domain.

Distribution domain: provides the whole infrastructure to bring power to the end user (consumer). The domain also includes transformer equipment which is necessary to reduce the voltage as power is transported to the consumer. Bulk consumers typically get their power at higher voltages, for example 16kV, then common households for which 230 Volts and 400 Volts present common values. The domain is managed by the so-called distribution system operator (DSO).

Consumer domain: groups all sort of consumers. The industries as well as households regardless of the amount of consumption and the consumer geographical location.

The four domain model gives a good introduction into the basic concept of an electrical grid but it does by no means appreciate the full detail of the electrical grid nor does it fully model the energy flow. Due to the liberalisation of the power market the generation domain is not exclusively subject to large utilities any more. For example, house owners may want to invest into renewable energy such as photo voltaic (PV) equipment

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

or wind turbines in order to cover their own power consumption and to supply current out of surplus production to others. After all, consumers are becoming producers or producing consumers *"prosumers"* [22].

Comparable changes also apply to the distribution domain. Local utilities more frequently setup own facilities to generate some power by themselves. Power generated will be feed-in directly at the distribution level at high voltages. Distributed generation (DG) is nothing new to grid operators and utilities as it was already discussed in literature [23] in 2001. The referenced book [23] also introduces several forms of generators and recognises the technical and financial impact of distributed generation to the grid. The reader will find information on combustion turbines, PV systems, micro turbines, fuel cells, combined heat and power as well as background information on grid operations with distributed generation and storage. However, security relevant aspects are not being discussed.

Since 2001 distributed power generation significantly emerged due to renewable energy gaining political attention and national funding [24]. These funds do not only focus on large installations but also take small generators in home scale into account. Meanwhile, distributed generation has taken off and demands for advances in measurement and operations of the electrical grid to be able to coordinate all generators and thus to ensure reliability of the grid. The following section will introduce and discuss some of the smart grids features.

2.2 Introduction to Smart Grids

The section will briefly introduce the major aspects and goals of smart grids. It aims to describe the challenges and requirements smart grids are contending with. Beyond that, the need for an intelligent measurement network – the advances metering infrastructure (AMI) will be outlined.

Smart grids have been defined as follows: *"A Smart Grid is an electricity network that can intelligently integrate the behaviour and actions of all users connected to it -generators, consumers and those that do both – in order to efficiently ensure sustainable, economic and secure electricity supply."* [25]. The definition clearly refers to the challenging dynamics of renewable energy resources (RES) whose generation heavily relies on the intermittent availability of sun light, wind or maybe tides. Unfortunately, it less clearly addresses changes in behaviour whereby the smart grid should not only be capable to react on actions but should also directly or indirectly influence consumption behaviour.

There have been six major characteristics [26], [27] identified. These characteristics describe the key benefits of a smart grid. The references even provide additional detail on the characteristics:

1) *"Enables Informed Participation by Customers*
2) *Accommodates All Generation & Storage Options*
3) *Enables New Products, Services, & Markets*
4) *Provides Power Quality for the Range of Needs*
5) *Optimizes Asset Utilization & Operating Efficiency*
6) *Operates Resiliently to Disturbances, Attacks, & Natural Disasters" [26], [27]*

The first three of the characteristics are probably the most interesting from a retail consumer's view. This report however, will direct attention to the part "Operates Resiliently to Disturbances, Attacks" of item six.

For the smart grid the basic electrical grid in figure 1 is enriched with new elements. The basic domain structure persists but an additional domain, hosting distributed generators and distributed storage devices, have been added to the smart grid blue print shown in figure 2.

The newly introduced "DG and Storage" domain hosts all sort of distributed energy resources (DER) such as generators and storages. The blueprint introduces a small wind park which contributes to the distribution domain and a PV installation with rechargeable batteries as buffer storage. In addition, a freezer and an electrical vehicle (EV) were added to the consumer domain. Actually, the EV is not only a consumer but may also

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

contribute to the grid as a storage in peak times. It's not the single items which are challenging for the grid but it's the masses which require for more 'smartness'. Small systems could also be grouped and centrally managed as a combined power plant to form a steady power resource. A more detailed view on improvements in the transmission and distribution domains with focus on security is provided in [28].

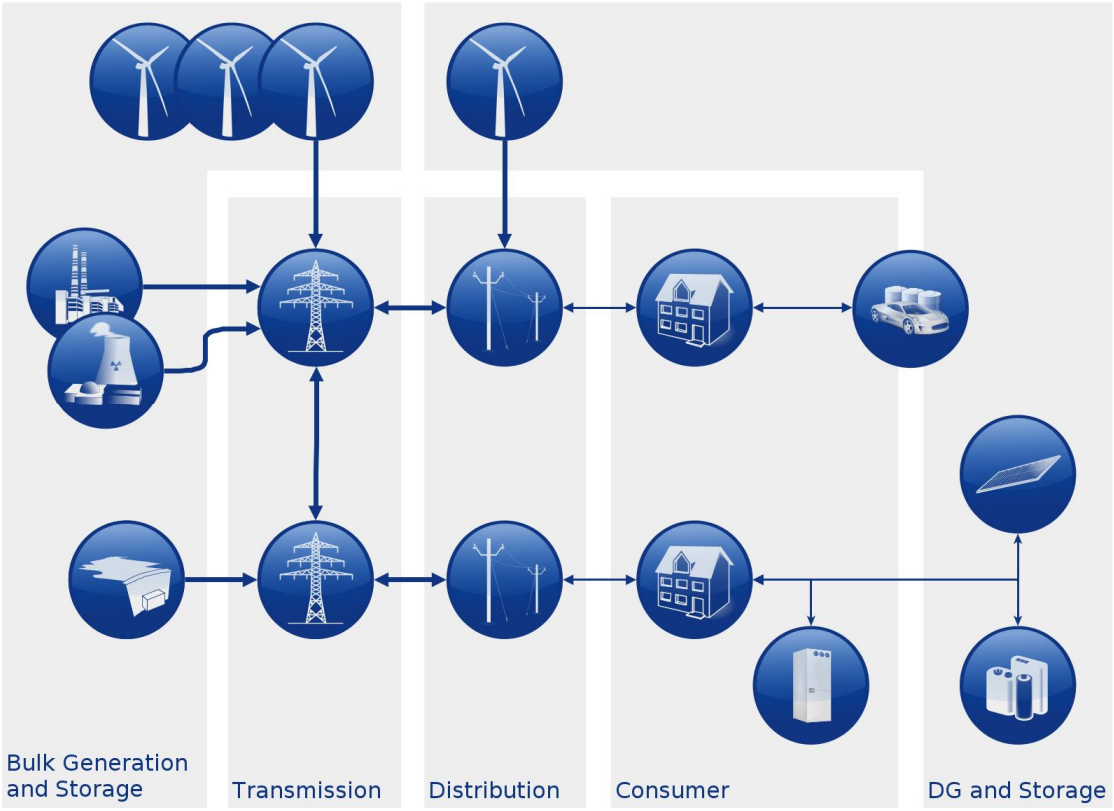


Figure 2: Smart Grid and Distributed Generation Blueprint

To ensure reliability of the grid the DSO and TSO must ensure that the power consumed and the power generated stays balanced otherwise efficiency and power quality (PQ) suffer. Unfortunately, poor PQ may quickly result in damaged consumer devices. To avoid such a scenario, live information and detailed statistics of the consumer behaviour, of generators capacity and of storage capacity is needed. Moreover, the operator will need to smartly attach or detach generators and consumer devices, such as EVs, to their local storage or to the grid according to the power needs. The management of the grid balance is also known as demand-response. As good as it sounds, management of so many components is much more complex and the recovery of a failure will demand for a controlled re-launch of DERs and bulk generators simultaneously at both ends of the grid.

Additionally, dynamic-pricing or real-time pricing (RTP) or critical peak pricing (CPP) could help to reduce peak loads and would result in lower demand-response efforts. For real-time pricing, consumers will be kept informed on the current power rates. Consumers could then decide on whether to run heavy loads at the current pricing.

Hence, reporting consumption and switching loads will require a bi-directional channel being established between operator and consumer. The channel would then allow for delivery of detailed measurement from the consumer and DG side to the operators. Furthermore, it would enable the operator to actively manage DER and to push real-time information to the consumer facilities. The equipment and network necessary is known as the AMI.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

3 Metering Infrastructure

This chapter will focus on the advanced metering infrastructure - its benefits and issues. A short introduction into use cases and approaches will be provided. Further, terms will be introduced and the necessary components and its capabilities will be discussed in more detail. Some relevant standards and specifications will be outlined and referenced.

3.1 Purpose of Smart Meters

The reason for smart meters is to enable the operators to improve their infrastructure towards a smarter grid and its six characteristics outlined in section 2.2. A smart meter has several advantages over a traditional mechanical meter. A smart meter does lots more [28], [29] than just providing detailed power consumption data to the operator. Primarily, a smart meter can significantly support the DSO to balance the network load and improve reliability.

A smart meter does not only lower manual reading cost but also enables to more efficiently estimate the load on the generators. It helps to more efficiently integrate DERs and helps to monitor the distribution network in order to identify PQ issues, misrouted energy flows or fire alerts in case a consumer outage is being detected. Beyond that, a meter could be used to push real-time pricing information to the consumer in order to allow appliances in the local network to optimise their power consumption according to the current rates. During an emergency, a meter could allow to disconnect consumers from the power grid. A meter could limit the consumption to a specified amount or could enforce pre-payment for defaulting customers.

Yet, at time of writing, the effective use cases implemented heavily differ from operator to operator. Whereby all of them support at least remote meter reading. However, a security analysis should take all potential use cases into consideration since it is likely that firmware and hardware is being enhanced to support additional use cases in the near future.

3.2 Approaches to Metering

3.2.1 Meter Reading vs. Metering Infrastructure

Typically, literature differs between advanced meter reading (AMR) and the advanced metering infrastructure (AMI) whereby AMR is to be seen as a subset of AMI [30].

AMR provides the metering company with usage data only. AMR does not allow for remote controlled action or advanced collection of power information. Thus, one-way communication from meter to the metering company is sufficient for that approach.

AMI will allow for remote initiated actions and therefore requires a two-way communication protocol. Though the border between the two approaches fades since remote initiated reading will also require for a two-way channel in AMR setups.

The remainder of the paper will focus to the AMI approach.

3.2.2 North American vs. European Implementations

The US as well as European countries have developed absolutely independent implementations of the AMI. Nevertheless, the key drivers and business needs are exactly the same.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

The National Institute of Standards and Technology (NIST) and the European Network and Information Security Agency (ENISA) respectively the European Committee for Standardization, the European Committee for Electrotechnical Standardization and the European Telecommunications Standards Institute (CEN/CENELEC/ETSI) mandated by the European Commission drive very similar projects to provide security guidance [31], [32] for smart grid and metering implementations. However, the guidance neither specifically requests for nor does it recommend the use of specific protocols.

If not otherwise stated the remainder of the paper refers to European implementations.

3.3 Architecture and Components

The AMI is typically structured into a bunch of networks and composed of a few major components. Figure 3 provides an overview of all components and most networks. It is made up of the Meter, the Collector and of the server systems at the DSO or metering company side.

Sections 3.3.1 to 3.4.4 sections will briefly introduce the major components and related networks of the AMI.

3.3.1 Head-end System

The head-end system (HES), also known as meter control system, is located within a metering company network. In most cases the metering company is the responsible DSO. The HES is directly communicating with the meters. Therefore, the HES is located in some demilitarised zone (DMZ) since services and functionality

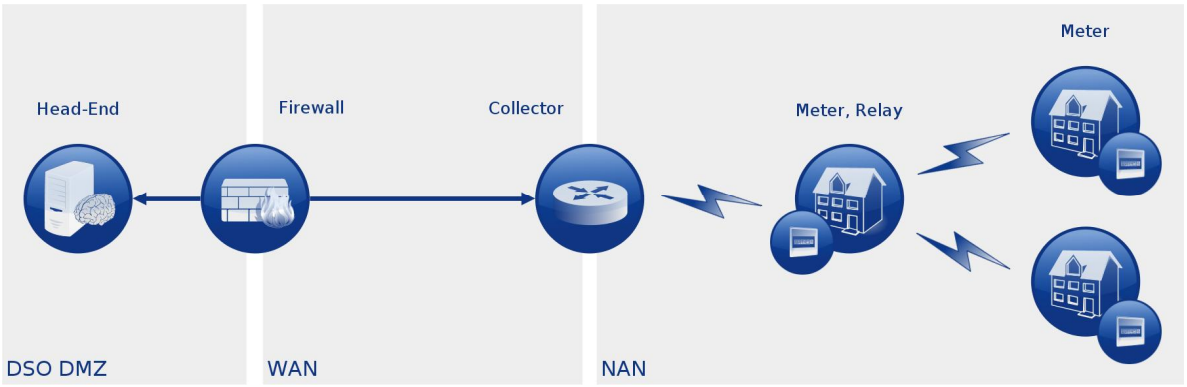


Figure 3: Advanced Metering Infrastructure Networks and Components

will be provided to the outside.

There is much more infrastructure at the DSO or metering company side. The collected data will be managed within a metering data management system (MDM) which also maps data to the relevant consumer. Depending on the automation level, the metering data will have influence on the DSO actions in order to balance the grid.

Exposing the HES to consumers enables some significant threats to the DSO. For example, an adversary getting hold of the HES could read all consumer data. Moreover, one could control meters or could manipulate usage data or generate alerts in order to disturb the DSO operations or at least trigger the computer incident response team (CIRT) and maybe force the DSO to backup to some business continuity plan (BCP) while analysing and recovering the HES.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

3.3.2 Collector

The collector, also known as concentrator or gateway, serves as communication node for the HES. Depending on the infrastructure the collector could be a meter itself. Its primary function is to interface between the HES and the meters and/or other collectors within its neighbourhood – the neighbourhood area network (NAN).

Not only the head-end but also the collector exposes threats. The collector is physically exposed to adversaries, has a trust binding to the HES and the NAN side and is thus privileged to communicate with either end. Adversaries might exploit the fact in order to attack the HES. Additionally, on the NAN side, adversaries might impersonate the collector to setup a man-in-the-middle scenario or to invoke arbitrary commands at the meters.

3.3.3 Meter

The meter is installed at consumer premises. When integrated with a collector, it directly communicates to the HES. As a meter it either communicates with the collector or may serve as a relay in order to route packets between nearby meters and the collector. Some meters provide an interface for appliances. With retail consumer that network is known as the home area network (HAN). Meters do also provide local diagnostic ports for manual readout, installation and maintenance tasks as shown in figure 4.

From an adversaries perspective the meter is the entry point to building automation, DER and usage data. But the meter is also a relevant part of the smart grid and under no circumstances should its manipulation allow critical influence or affect the availability of the grid or parts of it.

3.4 Communication

The infrastructure consists of several networks of which all could rely on absolutely different media and a multitude of protocols. In total, three networks are commonly described when referring to the AMI. The WAN, NAN and HAN.

3.4.1 Wide Area Network

The WAN connects a meter or collector to the HES. The WAN is sometimes also referred to as the backhaul network. Communication on the WAN link is mostly Internet protocol (IP) based and commonly relies on standard information technology (IT) media and technology stacks such as fibre optic cables (FOC), digital subscriber line (DSL), general packet radio service (GPRS), multi-protocol label switching (MPLS), PLC or some sort of private network. A brief overview on PLC for WAN side communication is provided in [33]

An overview on common US standards specifying communication for the WAN segment is provided in appendix 7.1.1. The CEN/CENELEC/ETSI Smart Meter Co-Ordination Group (SMCG) does not identify a specific protocol but proposes to rely on *"secure and non proprietary protocols and communication platforms"* [34] for bulk transmission from collectors that bundle a large number of meters.

3.4.2 Neighbourhood Area Network

The NAN connects meters and collectors. Typical NAN devices are electricity, gas, water or heat meters. Organisations sometimes refer to the NAN as local metrological network (LMS) [35], field area network (FAN) [29] or the metering LAN [36].

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Although standards such as the IEEE 802.15.4 [37], [38] based ZigBee profiles are gaining momentum, the industry and regulators seam to struggle on a common standard. Utilities among the European Union (EU) nations seem to prefer the meter bus standard for NAN communication [35] although the ENISA does not list [29] the meter bus as a NAN protocol.

3.4.3 Home Area Network

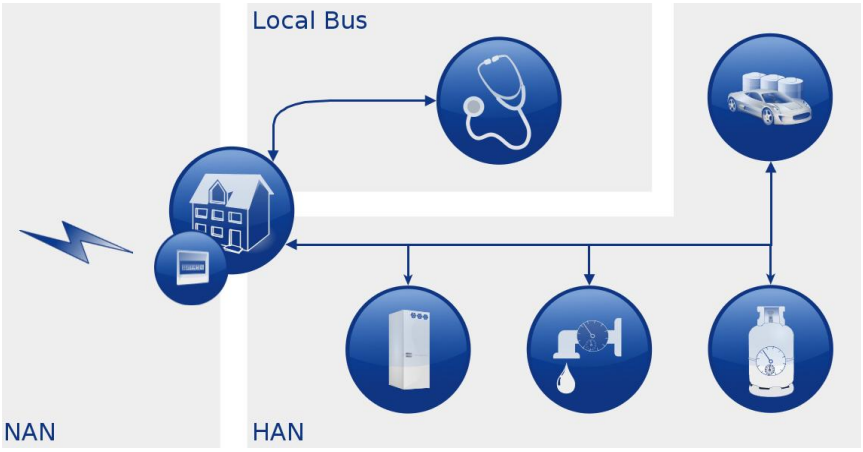


Figure 4: Home Area Network and Local Bus Blueprint

Depending on the consumer type the HAN could also be named as building area network (BAN) or industrial area network (IAN). Whatever its name is, the purpose of the HAN is to integrate additional gas, water or heat meters. The HAN allows for intelligent building automation and also allows the integration of DERs with the smart grid. To optimise consumption during peak hours a utility might for example decide not to entirely turn off but to throttle large heating, ventilation, and air conditioning (HVAC) appliances to balance the grid. For that purpose, consumers will be required to grant utilities or a third-party supplier access to their appliances. However, intelligent control does not necessarily require the intervention of an external part. Therefore, an intelligent HVAC might decide to throttle automatically based on the real-time pricing information provided by the utility.

Meters in the US largely focus on ZigBee for HAN communication [39]. Profiles for home automation and smart energy are specified in [40], [41]. The open metering system (OMS) group is pushing a specification that relies on M-Bus. In addition, the wireless M-Bus stack has been chosen as a foundation for WiMBex [42] and the KNX [43] wireless version. KNX is very popular in home automation among Europe. Unfortunately, KNX does not provide any security measures. Though there are studies which propose security enhancements to KNX [44].

3.4.4 Local Bus

Common interfaces for diagnostic purposes are provided as two or three-wire serial lines, current loop or as an optical interface [45], [46].

3.4.5 Network Protocols

Good overviews on common protocols for WAN, NAN, HAN and the Local Bus are provided in [47], [48].

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

4 Wireless Meter-Bus Analysis

4.1 The M-Bus Standard

The following sections are dedicated to the meter bus standard. Initially, the section will give a short overview of the origin of the M-Bus protocol stack and the standard series structure. Further sections will then discuss the relevant technical details. Specifically, the focus will be laid on the security relevant aspects of the bus system. The standardised bus system is analysed for robustness against common wireless and network communication threats as outlined in well established ISO security architecture standards [49]. The major question to be answered is to what extent the standard bus communication can cope with current requirements for secure networking. Additionally, residual risks will be pointed out and proposed protocol security enhancements will be considered.

4.1.1 History of M-Bus

The M-Bus communication standard has its roots in the water, heat and gas metering industries. Prof. Dr. H. Ziegler †2012, while holding a chair at the physics faculty at the University of Paderborn in Germany, is accredited with the initial concepts of remote meter reading as defined in the M-Bus and OMS standards today. Public documentation that focuses on M-Bus [20] and its standardisation work date back until 1997 [50]. The M-Bus documentation also refers to and bases itself on unpublished work from 1992. The earliest work includes dissertations of University of Paderborn graduates, seminar material of Texas Instruments Germany GmbH and M-Bus slave recognition algorithms by Aquametro AG in Switzerland. At the time of writing, the bus system already exists for twenty years and continues evolving under the OMS umbrella.

In the meantime the M-Bus has become the preferred bus system among several meter vendors and utilities across Europe. According to an Open Meter workshop note [10], 15 million devices were relying on the wireless version of M-Bus in 2010. Above all, the bus became well established among smart electricity meter manufacturers and also made its way into ICS and supervisory control and data acquisition (SCADA) environments.

4.1.2 Overview of the Standard

4.1.2.1 Current Version

The M-Bus standard *"Communication system for meters and remote reading of meters"* specifically the EN 13757 series is made up of six parts. These parts specify data formats, protocol packet structure, physical media access as well as the radio spectrum used for successful interoperability of meters and sensors relying on EN 13757. The following paragraphs will introduce each part.

EN 13757-1 [36]: The "Data exchange" part describes the general data structures and communication for local and remote reading. It further gives an introduction into the protocol stack and the metering architecture which is proposed to be a tree structure. The standard makes use of the term "collector" for devices which serve as an upstream device or as a master node for several other meters.

The standard also proposes the Distribution Line Message Specification (DLMS) and its Companion Specification for Energy Metering (COSEM) as an alternative application layer. Unfortunately, the EN 60056 DLMS/COSEM family and this part share many figures, texts and tables which makes it hard to distinguish between these two.

When it comes to security features and mechanisms the COSEM application layer, EN 60056-53 [51], and the

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Object identification system (OBIS), 62056-61 [52], are being cited.

EN 13757-2 [53]: The "Physical and link layer" part specifies the master-slave concept and foresees an address space of 250 addresses for unique addressing of slave devices. The standard further specifies the binary representation of the current loop (twisted pair, baseband) in the form of electrical signals in voltage and current levels. It further specifies bus powering and discusses slave powering options, collision detection, cable installations and provides protocol examples such as "init" and "readout". Details on the implementation and electronics design of M-Bus devices are provided in [54].

EN 13757-3 [55]: The "Dedicated application layer (DAL)" is proposed to be used in combination with the current loop or wireless interface. It describes the various message types such as baud rate changes, send data, reset application or reporting of alarms. For the latter, signals for tamper detection and voltage drops are defined.

The DAL defines optional encryption for data structures. Unfortunately, the wording is very ambiguous and does not follow common security terminology. The first sentence of section "5.10.1 General" states "The Signature is reserved for optional encryption of the application data". Actually, the data structure defines a "Signature" field which is not used for the signature of the structure but to indicate whether and what type of encryption should be applied.

As an encryption algorithm the Data Encryption Standard (DES [56]) in cipher block chaining mode (CBC [57]) is proposed either using an all-zero initialization vector (IV) or a device dependent IV. However, measures to provide integrity are totally missing. An adversary could simply flip bits in order to manipulate measurement data.

Note, the standard references to the American National Standards Institute (ANSI) specifications of DES and CBC which are technically identical [58] with the here referenced Federal Information Processing Standards (FIPS) publications.

EN 13757-4 [59]: As the title implies the "Wireless meter readout (Radio meter reading for operation in the 868 MHz to 870 MHz SRD band) " part specifies the frequency spectrum, bands and communication types for wireless meter readout. Typically, meters use radio within the NAN which means either between meters and relays, between meters and stationary or drive-by collectors.

The wireless meter readout standard proposes Manchester [60] and "3 out of 6" for bit-coding. For error detection a cyclic redundancy check (CRC) is proposed.

EN 13757-5 [9]: The "Wireless relaying" part specifies meter capabilities to extend the range between meters and collectors. Meters supporting that part of the standard can act in gateway or router mode and forward frames between multiple meters and the collector.

EN 13757-6 [45]: The "Local Bus" part specifies an alternative to the M-Bus and is designed as a 3 wire serial line. The local bus allows for local readout with battery powered Hand-held units (HHU) or mini-master whereby the meter must be self powered. Using the local bus, a minibus of up to 5 devices could be read.

So far the standard series does not take many of the information security relevant core concepts into account. However, the lack of security standardisation has been recognised and changes have been introduced in the latest available draft versions.

4.1.2.2 Draft Version

Currently, three of the six parts of EN 13757 are being revised. Most of the revision work targets DLMS/COSEM interoperability, wireless network improvements and the specification of security mechanisms.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Some interesting and security relevant changes of each part of the draft standards are outlined in the paragraphs below:

prEN 13757-1 [6]: The draft now covers IPv4 [61], IPv6 [62] and well established protocols such as IPsec [63] and TLS version 1.2 [64]. However, IP is only suggested in combination with the COSEM transport layer [65]. Additionally, the draft introduces the concepts of tunnelling and translation for interoperability in mixed COSEM and M-Bus environments.

Finally, section 4.3 of the draft identifies four key aspects for secure metering networks. Furthermore, it introduces some information security terms such as confidentiality, privacy, integrity and authentication as well as the basic concepts of key management and symmetric and asymmetric cryptographic systems. However the section is a bit confusing in terms of confidentiality and privacy, signatures and MACs and does not take availability into account.

The draft mentions pre-shared keys as an example for entity authentication for local connections such as specified in [46]. When relying on High-Level Data Link Control (HDLC) as the data link layer [66] and in the absence of physical access restrictions the draft demands for low-level encryption and signatures as well as for authentication at higher layers.

prEN 13757-3 [7]: The draft on the "Dedicated application layer" specifies additional security relevant aspects. For example, it names consumer privacy-preserving requirements and introduces the Advanced Encryption Standard (AES [67]) in CBC mode [67] with a 128 bit key length with or without an all-zero IV. The draft suggests that manufacturers pre-load devices with a unique key and hand the list of keys and IDs over to the metering company.

Furthermore, it makes suggestions on how to sign billing relevant data and states that the meter display may have precedence to solve disputes, though. Additionally, there is a short mention of authentication and key separation. However, security terms are still used very ambiguously.

prEN 13757-4 [8]: The "Wireless meter readout" draft introduces three additional communication modes that improve efficiency and enable long range communication. Moreover, the extended link layer (ELL) supports AES [67] encryption in CTR mode [68] with a 128 bit key length. The encryption will be applied on the whole payload including a 2 byte CRC. The IV is mainly derived from the frame header. Approximately the first ten bytes of the IV remain static over the lifetime of a meter.

The wireless meter readout draft does not specify any integrity protection or authentication mechanisms.

4.2 Wireless M-Bus Introduction

This section briefly introduces M-Bus communication based on the wM-Bus stack and its related transmission modes as defined in current and draft standards [59], [9], [7], [8]. Tests in a lab environment have shown that all meter vendors do partially support the draft version of the wireless meter readout standard. An example print-screen of devices supporting AES encryption is provided in figure 11. The descriptions within this work are focused on the draft standards.

4.2.1 Protocol Stack

The M-Bus protocol stack is very flexible and the wireless stack is even compatible with various application layers such as COSEM or KNX [43]. A brief overview of the DLMS/COSEM standard series is provided in appendix 7.1.2.The stack does conceptually follow the ISO/OSI layer model but make use of just three respectively four of the seven layers.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

ISO/OSI Layer	Standard	Description
Application	prEN 13757-3 [7]	M-Bus Dedicated Application Layer (DAL)
Network	EN 13757-5 [9]	Wireless relaying (optional for meters supporting the router approach)
Data Link	prEN 13757-4 [8]	Wireless meter readout (Radio meter reading for operation in SRD bands) whereat the data link layer is related to EN 60870-5-1 [69] and EN 60870-5-2 [70]
Physical	prEN 13757-4 [8]	Wireless meter readout (Radio meter reading for operation in SRD bands). The standard proposes Manchester [60], "3 out of 6" and no-return-to-zero (NRZ [71]) for bit-coding, a cyclic redundancy check (CRC) for error detection.

Table 1: wM-Bus Protocol Stack mapped to ISO/OSI Layers

Data transmitted, involving structures of at least the data link and application layer, is referred to as telegrams. The protocol stack shown in table 1 further describes a network layer which only exists with devices that support the M-Bus wireless relaying router approach. According to the specification a device depending on that protocol stack can communicate with its peers in a multitude of transmission modes.

4.2.2 Communication Modes

The wireless meter readout draft standard [8] physical layer defines six main modes in order to allow for optimisation in power consumption supporting different use cases. Additionally, the wireless relaying standard [9] specifies modes for routing and time synchronisation between devices.

- **Stationary Mode (S)** is to be used for communication with battery driven collectors. Specific modes exist for one-way and two-way communication.
- **Frequent Transmit Mode (T)** is optimised for drive-by readout. As with mode S, mode T does provide specific modes for one-way and two-way communication.
- **Frequent Receive Mode (R)** allows for simultaneous readout of multiple meters. Whereby only sub mode R2 is specified. The R2 sub mode is used mainly used for gateways and drive-by meter reading.
- **Compact Mode (C)** is comparable to mode T but allows for increased data throughput. This is achieved by using NRZ for line coding which is more efficient than the Manchester code.
- **Narrowband VHF Mode (N)** is optimised for transmission within a lower frequency narrow band. It is intended for long range repeater use and does specify modes for one-way, two-way and relay communication.
- **Frequent Receive and Transmit Mode (F)** is optimised for long range communication and is also split into one-way and two-way sub modes.
- **Precision Timing Protocol Mode (Q)** provides distribution of time information taking network latency and battery optimised nodes into account. Mode Q is available in simple and relayed environments.
- **Router based Protocol Mode (P)** changes addressing to include source and destination to allow for real routing between collectors and meters in the wM-Bus environment over multiple hops.

There are several wireless M-Bus transmission modes. The laboratory provided access to electricity, gas and water meter devices whereby all of the devices transmit their metering values in frequent transmit mode. Thereby, application data is encapsulated in frames of either type A or B also indicating the vendor of the device. For an introduction into frame types consult section 4.2.3. For a list of vendors and test devices see

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

appendix 7.2.

4.2.3 Frame Description

The wireless meter readout draft standard [8] data link layer defines two slightly different frame formats for application data encapsulation. Wireless frames captured in the lab environment were all of type B – having less redundancy checking resulting in larger block sizes. An example of a captured frame (without CRCs) is provided in figure 7.

4.2.3.1 Frame Format A

Frame format A foresees a 2 byte CRC which is specified by a polynomial. The first block of the frame format is fixed length and contains the sender's address. The second and any following block's length depend on the user data size.

First Block					Second Block			Optional Blocks	
Length	Ctrl	Manuf.	Address	CRC	Ctrl. Info.	Data	CRC	Data	CRC
1 byte	1 byte	2 bytes	6 bytes	2 bytes	1 byte	max. 15 bytes	2 bytes	max. 16 bytes each	2 bytes

Figure 5: wM-Bus Frame Format A [8]

The first block of frame format A, as shown in figure 6, is nearly identical to the first block in frame format B.

4.2.3.2 Frame Format B

As with frame format A, the first block or frame header is fixed length and the length of the subsequent blocks depends on the payload. As mentioned, the first block does not contain a CRC in format B. Within the lab environment mainly frame Format B has been observed.

First Block				Second Block			Optional Block	
Length	Control	Manuf.	Address	Ctrl. Info.	Data	CRC	Data	CRC
1 byte	1 byte	2 bytes	6 bytes	1 byte	max. 115 bytes	2 bytes	max. 126 bytes	2 bytes

Figure 6: wM-Bus Frame Format B [8]

The first block fields do contain the frame length, a control byte to signal message direction and purpose, the manufacturer identification and the device address.

4.2.3.3 First Block Contents Analysis

Analysing the first block of a captured message will provide some insights into the common contents of a real world wM-Bus frame.

```
Timestamp;Frame
06.02.2013 13:40:20:518;1E 44 2D 2C 07 71 94 15 01 02 7A B3 00 10 85 BF 5C 93 72
```


Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
04 76 59 50 24 16 93 27 D3 03 58 C8
```

Figure 7: wM-Bus Frame Capture, Electricity Meter Raw Data, Firs Block Contents

The first ten bytes of the captured frame can be decoded as listed in table 2.

Field	Value (hex)	Interpretation
Length	1E	30 bytes frame length (exclusive length byte)
Control	44	Indicates message from primary station, function send/no reply (SND-NR)
Manufacturer ID	2D 2C	Coded abbreviation for Kamstrup (KAM) calculated as specified in prEN 13757-3 [7]. The manufacturer identification is managed by the flag association and is available online [72].
Address	07 71 94 15 01 02	Most significant bit of the Manufacturer ID indicates a globally unique address. Identification: 15 94 71 07 (low byte first). Device Type: 02 (electricity meter) Version: 01

Table 2: wM-Bus Frame Capture, Electricity Meter Data Decoded First Block

Note, the additional version and type information provided in figure 8 was actually extracted from the first block address field.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

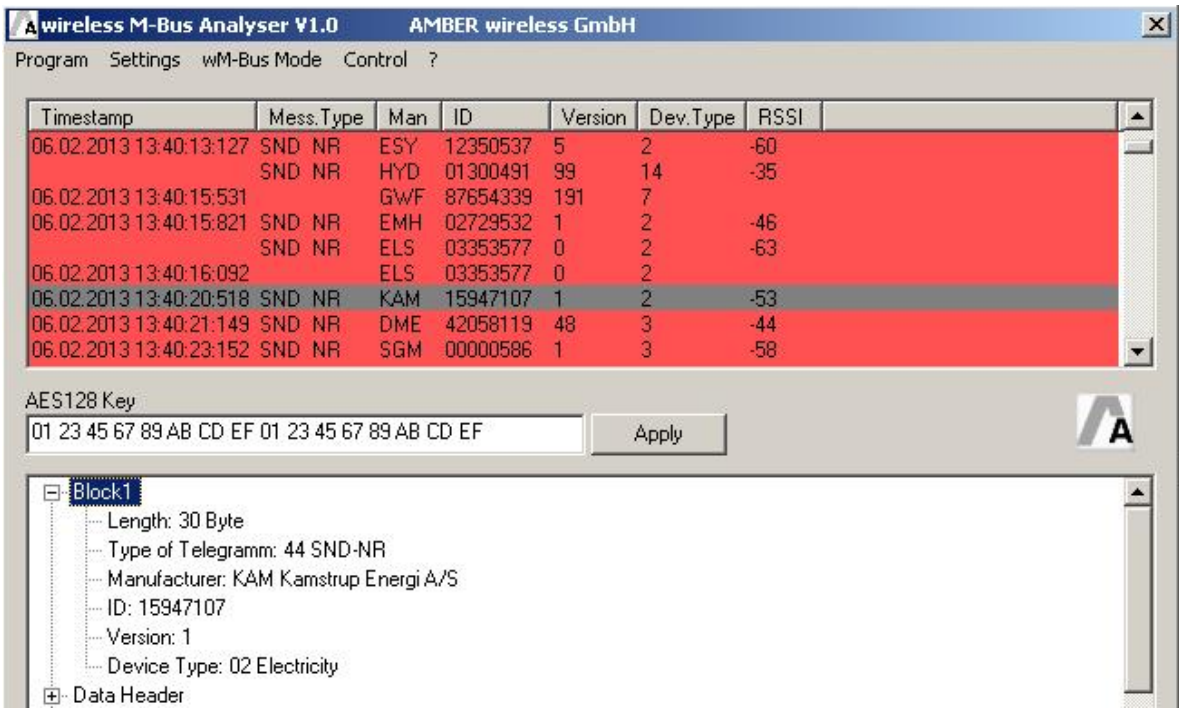


Figure 8: wM-Bus Frame Capture, Electricity Meter Interpreted Data in wM-Bus Analyser [73]

The wireless analyser shown in figure 8 does highlight frames carrying encrypted payload in red colour.

4.2.3.4 Control Information Field

The control information field does specify the upper layer. This could be any application protocol with or without transport layer. In case of the captured frame shown in figure 9 the CI field is $7A_h$ which indicates EN 13757-3 as application layer relying on a short transport layer.

```
RSSI;Timestamp;Frame
-53;06.02.2013 13:40:20:518;1E 44 2D 2C 07 71 94 15 01 02 7A B3 00 10 85 BF 5C 93
72 04 76 59 50 24 16 93 27 D3 03 58 C8
```

Figure 9: wM-Bus Frame Capture, Electricity Meter Raw Data, Control Information Field

The CI field provides values for upper layers such as M-Bus, COSEM, OBIS, time service, alarm service and abstract types such as the network or extended link layer. Some interesting ones are:

- **Response from device** is used to signal data records being submitted. An example for such data is the consumption value.
- **Command to device** could be used to, for example, remotely open or close a valve or breaker.
- **Error from device** is used to signal errors in the application layer to the peer. Errors could be: command unknown, encryption method unsupported, decryption failed, access denied. A full list of errors is provided in the dedicated application layer [7] specification in table 35.
- **Alarm from device** is used to notify the peer about unusual occurrences such as power low or issues that would require a service action such as triggered tamper switches or permanent failure of part of the hardware.
- **Time sync to device** is used in order to update the time service within the device. Time sync to device is also referred to as Clock synchronisation within the standard

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

- **Application reset** does, depending on the implementation, reset application values such as consumption, history, tariff, instantaneous, calibration or load management values.

In the laboratory, responses carrying M-Bus and OBIS with or without short and long transport headers have been observed. Note, there are further special CI fields such as for the extended link layer (ELL) which is briefly outlined in section 4.2.7 and network management for relaying outlined in 4.2.6.

4.2.4 Transport Layer and Data Header

The transport layer is briefly outlined within the "Wireless meter readout" part of the M-Bus standard series. However, since the M-Bus stack does omit the ISO/OSI layers three to six, the "transport layer" structure is defined in the DAL part of the standard whereas the application layer refers to the transport layer as the data header. The data header prepending the data records will be embedded into the frames data section. Actually, there are three different types of data headers whereby all of them have been observed within the lab environment.

4.2.4.1 No Header

If the CI field signals 78_h than there is no data header available. Following that, encryption of data records is not supported.

4.2.4.2 Short Data Header

The short data header defines an access number, status byte and a configuration word as outlined in figure 10. The specification distinguishes between frames originating at the meter or originating from others. Hence, contents of the data header fields slightly differ depending on the communication direction, type and configuration. The below descriptions only provide brief description of each field.

Access	Status	Configuration
1 byte	1 byte	2 bytes

Figure 10: M-Bus Dedicated Application Layer, Short Data Header Format

Access number (ACC) contains a number which is intended to support the detection of repeated frames and should be incremented for each new frame except for responses where the response should reflect the received value. The standard clearly states that this mechanism does not provide sufficient prevention against replay attacks and suggests use of additional measures within the data layer to counter replay.

Status field is included if the frame originated from the meter than this field indicates various alerts and errors. If it originated from any other device then it should provide the receive signal strength indicator (RSSI) of last received meter frame to keep the meter informed about the link quality.

Configuration field is used to set the encryption mode and to define the length of the encrypted user data. The field can be used to choose between DES in CBC mode or AES-128 in CBC mode which both can be used with or without zero IV. The standard clearly states that DES is deprecated and should not be used for new developments any more. None of the devices in the lab supported DES encryption. Depending on the encryption mode, the configuration field provides supplemental information such as the encrypted content length, whether the contained data comes with a signature or the hop count for data that passed a repeater and access control.

All of the described three fields also exist in the long data header format. The long data header defines some

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

additional fields to support wireless to wired bridging respectively to signal addresses of wired devices to a wireless collector.

4.2.4.3 Long Data Header

The long data header inherits all the fields of the short data header. Additionally it provides fields for device identification, a manufacturer ID, a version ID and a device type ID. The four fields correspond to the address and manufacturer fields in the frame format as outlined in section 4.2.3. Wireless devices that serve as a bridge to a wired M-Bus can use these fields to populate the wired device address to allow the wireless receiver to tell multiple wired devices apart.

Identification	Manufacturer	Version	Dev. Type	Access	Status	Configuration
4 bytes	2 bytes	1 byte	1 byte	1 byte	1 byte	2 bytes

Figure 11: M-Bus Dedicated Application Layer, Long Data Header Format [8]

The DAL defines that the identification within the long header shall have precedence over the frame address.

4.2.4.4 Data Header Example

With regard to previous examples, the control information of the captured example in figure 12 indicates a short data header which is four bytes in total.

```
RSSI;Timestamp;Frame
-53;06.02.2013 13:40:20:518;1E 44 2D 2C 07 71 94 15 01 02 7A B3 00 10 85 BF 5C 93
72 04 76 59 50 24 16 93 27 D3 03 58 C8
```

Figure 12: wM-Bus Frame Capture Electricity Meter Raw Data, Data Header Example

Analysing the four bytes provides the information listed in table 3 below.

Field	Value (hex)	Interpretation
Access number	B3	Current access number is 179. The standard mandates to choose a random number on meter start.
Status field	00	The message is meter initiated and there are no alarms or errors.
Configuration	10 85	Encryption mode is 5_h which is AES-128 in CBC mode. The configuration word further indicates (10_h) a single encrypted block containing meter data (without signature). The field further indicates a short window where the meter listens for requests (8_h)

Table 3: wM-Bus Frame Capture, Electricity Meter Decoded Data Header

Decoding the data header allows for a closer look at the data records. However, the records need to be decrypted before analysis according to the M-Bus data records specification.

4.2.4.5 Ciphering

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

This section will focus on encryption and decryption of data and the related padding. The report will stick to the former capture example in order to explain the decryption of the data records defined by the application layer. As shown in former sections, the sample capture has a single encrypted block in M-Bus encryption mode five using AES-128 in CBC mode. The relevant block is highlighted in figure 13.

```
RSSI;Timestamp;Frame
-53;06.02.2013 13:40:20:518;1E 44 2D 2C 07 71 94 15 01 02 7A B3 00 10 85 BF 5C 93
72 04 76 59 50 24 16 93 27 D3 03 58 C8
```

Figure 13: wM-Bus Frame Capture, Electricity Meter Raw Data, Application Layer Ciphering Example

The standard provides further details on the 16 bytes IV required for M-Bus encryption mode five. The IV is composed from frame information as shown in table 3.

Initialization Vector (IV)															
Manufacturer		Address						Padding with Access Number							
2D	2C	07	71	94	15	01	02	B3	B3	B3	B3	B3	B3	B3	B3

Figure 14: wM-Bus Initialization Vector for Encryption Mode Five: AES-128 in CBC Mode

Assumed the IV is derived correctly and assumed being in possession of the correct key k, the encrypted block C highlighted in figure 13 can be decrypted as follows: M = Deck(C) ⊕ IV. Figure 15 provides an example by applying the formula to the referenced block using CrypTool [74]. For a further example consult appendix 7.2.3.

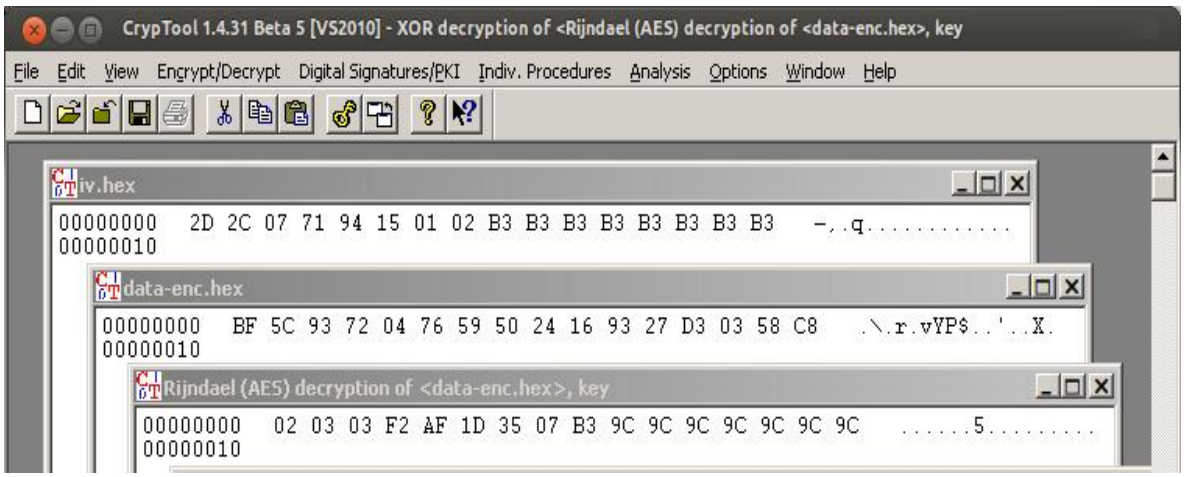


Figure 15: wM-Bus Frame Capture, Electricity Meter Raw Data, Decryption Example using CrypTool [74]

Finally, the plaintext M of the decrypted block represents a padded data record. The standard suggests adding two leading bytes 2Fh 2Fh to detect correct decryption. Moreover, one or multiple 2Fh (filler DIF) are being used as padding byte to create full 16 bytes block. Stripping the leading and trailing bytes leads to the extracted data record shown in figure 16.

```
04 83 3B 08 34 05 00
```

Figure 16: wM-Bus Frame Capture, Electricity Meter Raw Data, Plaintext Data Record

Data records themselves therefore consist of supplement header information and of course, the value itself.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Section 4.2.5 provides a brief introduction into record headers and record data formats.

4.2.5 Data Records

4.2.5.1 General

Data records are the structures transferred at the application layer of M-Bus. This section will outline the structure and provide examples. Throughout the whole section, it is assumed the data records were decrypted and heading and trailing padding was already stripped.

A frame can carry as many records in unordered sequence as the maximum frame length allows for. As with data and data headers each record has a record header which defines the format of the data trailing the header. The record header itself specifies the data information field (DIF) and the value information field (VIF) and related extensions (DIFE, VIFE) of the data. The decrypted data record provided in figure 16 can be decoded as listed in table 7. The full lists of DIFs, VIFs and corresponding extension values are part of the DAL specification [7].

Field	Value (hex)	Interpretation
DIF	04	Instantaneous readout value, no extension fields
VIF	83	Primary VIF, Unit: Energy 10^0 Wh, has extension (VIFE0)
VIFE0	3B	Forward flow contribution only
Data	08 34 05 00	The value is coded LSB first and it represents a value of 341000 respectively: 341 kWh

Table 4: wM-Bus Frame Capture, Electricity Meter Decoded Data Record

A quick cross check with the wireless M-Bus analyser [73] confirms the result of 341 kWh as the consumption value.

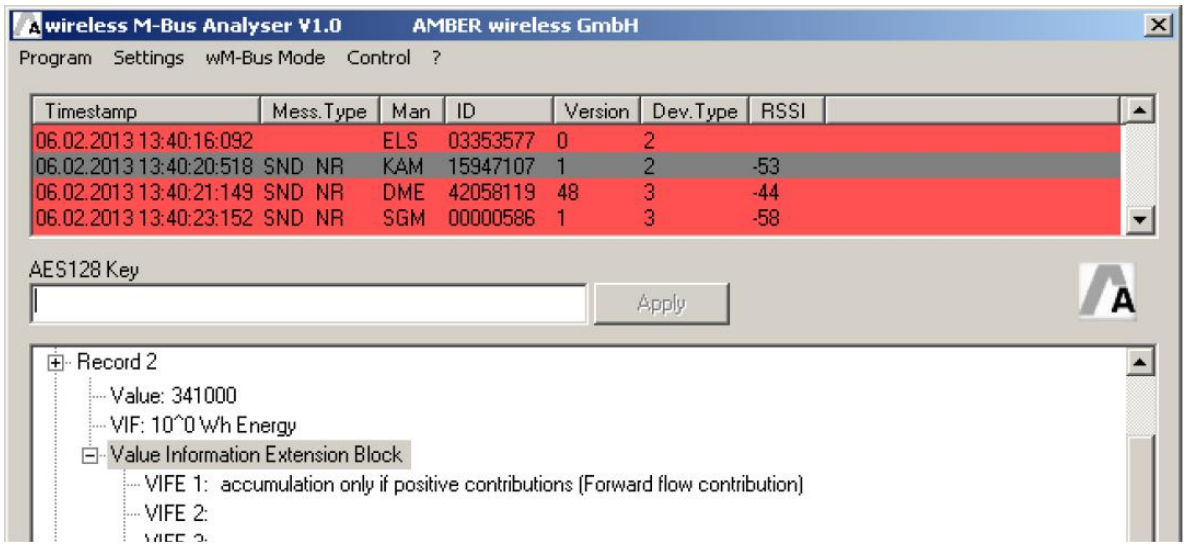


Figure 17: wM-Bus Frame Capture, Electricity Meter Decoded Record using wM-Bus Analyzer [73]

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

4.2.5.2 Optional Formats

Annex K of the draft standard introduces the "M-Bus Compact" and "M-Bus Format" frames which are intended for efficient transmission of data. These are called "frame types", have dedicated CI values to signal these specific types to the receiver but actually, only the record structure differs from the common frame formats. A description of available types of frames is provided in section 4.2.3.

A meter must not necessarily support the compact and format "frames" to comply with the standard. However, the idea of the structures is to transmit the format once and to transmit data of a similar format without the DIF/VIF overhead later on. From a security perspective these optional structures might be interesting because a payload CRC is introduced for the compact frame.

Format Frames do only carry the DIF/VIF structures for the data transmitted within compact frames. Additionally format frames do include a "Format-Signature" which is used to reference the format from within the compact frames. That "Format-Signature" is actually a CRC over the DIF/FIV structures. Therefore, it will be referred to as the "Format CRC" to avoid confusion with digital signatures. Note, that the structure could also contain extensions (DIFE/VIFE). Figure 18 provides an example of the format frame structure.

CI	Long, Short Data Header	Format CRC	DIF1	VIF1	DIF2	VIF2	...
1 byte	header dependent	2 byte	1 byte	1 byte	1 byte	1 byte	

Figure 18: M-Bus Optional Format Frame Structure [7]

Compact Frame: only contains the data specified by a format frame as shown in figure 19. What DIF/VIF structure to use is determined by the "Format CRC" field. The "Payload CRC" is used to verify the full M-Bus frame when combining the format frame DIF/VIF structure with the data delivered in the compact frame. More information on the limitations of CRCs to provide integrity is provided in section 4.3.3.2.

CI	Long, Short Data Header	Format CRC	Payload CRC	Data1	Data2	...
1 byte	header dependent	2 byte	2 byte	x byte	x byte	

Figure 19: M-Bus Optional Compact Frame Structure [7]

The major parts of each M-Bus layer and specifically the dedicated application layer have been introduced. For a completed view on wM-Bus wireless networks the section 4.2.6 does briefly introduce gateways and routers. Afterwards, section 4.3 will the finally focus on the security analysis of the application layer and the extended link layer while also taking relaying into account.

4.2.6 Relaying

Subsequent sections will introduce the major aspects of wireless relaying in wM-Bus. The major goal of this section is to provide sufficient understanding and build a foundation for the security analysis in chapter 4. Relaying in wM-Bus is considered a range extension which is necessary due to devices limited transmission power levels and regulatory requirements. The "Wireless relaying" part five of the standard [9] series foresees a relay device to either work as a router or as a gateway.

4.2.6.1 Routers

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

The *"protocol using routers"*, also known as mode P, enhances frame addressing with source and destination addresses as known from IP and allows for fully routed networks. To allow for a second address, the common frame format A, as described in section 4.2.3.1, needs to be extended. As a result, dual addressing which includes source and destination addresses of the communication peers, cannot be used by EN 13757-5 [9] unaware devices. Additionally, a network layer is being introduced which provides information on hop counts and intermediate devices addresses. Network management functions, as defined in the same specification [9], could be used to maintain routes and detect broken links.

Network management functions (CI 83_h) include the exchange of known node lists and link quality between routers, the deletion of such lists and the signalling of relaying errors as defined in table 8 of the standard. Further details on the protocol using routers are provided in chapter five of [9]. Routers do not need to be authenticated in order to exchange, update and clear information on link nearby devices and the corresponding link quality.

4.2.6.2 Gateways

Using the "protocol using gateways" provides some advantages of the router approach since this type of relaying is compatible with old devices that support the wireless meter readout standard [8] only. As with destination network address translation (DNAT) in IP, the gateway basically hides the upstream network from the meter and masquerades as a collector. An address rewriting technique is used to transport the application data to the collector. Additionally to the known nodes list, lists for trusted gateways and end-nodes need to be managed. The protocol foresees appropriate functions for that purpose.

As with the router approach, network management is not subject to authentication and integrity protection.

4.2.7 Extended Link Layer

The extended link layer (ELL) can provide security services at the link level and is defined in the wireless meter readout part [8]. In contrary, the application layer encryption is defined within the dedicated application layer (DAL [7]) part of the 13757 series.

4.2.7.1 Layer Description

The ELL supporting security services is being signalled with a CI of $8D_h$. The corresponding layer consists 8 bytes structured as provided in figure 20.

CC	ACC	Session Number (SN)			Payload CRC
		Enc.	Time	Session	
1 byte	1 byte	3 bit	25 bits	4 bit	2 bytes

Figure 20: M-Bus Extended Link Layer Structure supporting Security Services [8]

The access number (ACC) as well as the CRC have been discussed earlier on in this chapter. Fields of interest are the communication control field (CC) as well as the session number (SN).

Communication Control Field (CC) provides flags that signal communication direction, type and timings. The field could for example be used to prioritise a frame over other frames.

Session Number is a combination of three parts. The encryption field (Enc.) signals the encryption algorithm mode applied. At the time of writing, there are two options: no encryption or AES-128 in counter mode of

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

operation (CTR). Encryption and decryption in counter mode is visualised in figure 23. The time field represents the time of the meter in minutes and the session field defines a certain bidirectional communication session within the specified minute.

4.2.7.2 Ciphering

Counter mode of operation turns a block cipher into a key stream generator. The IV specified within the ELL partly compares to the IV used for the encryption of the DAL [7]. Within the ELL, the IV is specified as provided in figure 21.

Manuf.	Address	CC	SN	FN	BC
2 bytes	6 bytes	1 byte	4 bytes	2 bytes	1 byte

Figure 21: M-Bus Extended Link Layer Encryption IV [8]

The IV is mainly composed of parameters already discussed. Note, that all parameters except for the frame number (FN) and the block counter (BC) can be read from the frame header and the ELL. Further note, that the router bit (R-bit) of the CC field is always set to 0 for the creation of the IV.

Frame Number (FN) is used to keep track of frames during a session. Therefore, peers will increment the number for each frame. Requests and responses will have subsequent frame numbers. Resent frames will keep their FN.

Block Counter (BC) restarts for every frame at zero and is continuously incremented for each encrypted block.

Finally, encryption is applied to the payload including the payload CRC of the extended link layer.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

4.3 M-Bus Security Analysis

This section aims to identify if the DAL and the ELL do follow common security requirements for network communication. Each subsection provides an analysis and will outline concerns, deficiencies, potential vulnerabilities and attack scenarios regarding the M-Bus standards family. The current versions of the standards do not cover several features proposed in the latest drafts. For that reason, the analysis will focus

- on the draft standard prEN 13757-3 [7] for the DAL,
- on the draft standard prEN 13757-4 [8] for the ELL,
- on the current standard EN 13757-5 [9] for relaying and
- on the draft standard prEN 13757-1 [6] "data exchange" for reference.

4.3.1 Data Confidentiality

This section aims to identify if the M-Bus DAL provides sufficient data confidentiality.

4.3.1.1 Supported Ciphers

Dedicated Application Layer: *"Table11 – Definition of the mode bits (encryption method)"* [7] describes the encryption mode bits of the configuration word, which allows for four encryption modes (modes 2 to 4):

- mode 0) no encryption
- mode 1) reserved
- mode 2) DES/CBC, zero IV
- mode 3) DES/CBC, non-zero IV
- mode 4) AES/CBC, zero IV
- mode 5) AES/CBC, non-zero IV
- mode 6) reserved for future use
- mode 7ff) reserved

The M-Bus DAL allows for partial data record encryption. Thus, the number of encrypted blocks is signalled. The standard even allows for zero encrypted blocks. Note, the encryption mode bits are submitted in plaintext within the data header. See section 4.2.4 for reference.

Extended Link Layer: The ELL [8] provides two different modes. No encryption or encryption mode 1 which is AES in counter mode. Modes 2 to 7 are currently reserved. The wM-Bus ELL does not allow for partial encryption. As with the DAL, the mode bits are being submitted as part of the link layer in plaintext. A brief introduction into the fields of the ELL is provided in section 4.2.7.

General: Note that application resets, alarms, errors, clock synchronisation and network management have been defined as independent protocols (dedicated CI value) and are therefore not subject to application layer or extended link layer encryption.

4.3.1.2 Cipher Strength

Dedicated Application Layer: DES has been withdrawn by NIST in 2005 [56]. Consequently, the M-Bus DAL flags the two DES modes explicitly as deprecated and highlights this fact again in section 5.12.5 paragraph a). Actually, none of the meters in the lab supported or were configured to use DES as an encryption algorithm. Thus, DES is not being considered for the remainder of the analysis. Whether devices allow for fallback to DES or plaintext would need to be verified on a per device basis in practise.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

AES is still considered a secure cipher. At time of writing, the best public known attack on a full-round AES-128 using biclique cryptanalysis [75] which only marginally affects AES-128 [76].

Extended Link Layer: As with the DAL, the ELL is based on AES which is considered secure.

General: Both, the DAL and the ELL allow for unencrypted layers. However, it is left to the implementer whether to accept mixed payloads (encrypted and unencrypted data).

4.3.1.3 Modes of Operation

This section sheds light on the M-Bus encryption modes ciphers and its supported modes of operation.

Dedicated Application Layer: The standard mandates cipher block chaining for all encryption modes. Electronic codebook mode (ECB) would have been an issue since it allows for dictionary attacks [58]. However, meters frequently send a single block only containing the consumption value. For a single block P_1 encryption in CBC mode with an all-zero IV is equivalent to encryption in ECB mode for any algorithm (Enc) under the same key k.

```
CBC:   C1 = Enck(P1 ⊕ IV) = Enck(P1 ⊕ 00 00 … 00 00) = Enck(P1)
ECB:   C1 = Enck(P1)
```

As a consequence, adequate IVs are required to avoid dictionary attacks over multiple ciphertexts having a single block encrypted under the same key. CBC mode requires to be operated with unpredictable IVs and the IVs to be integrity protected [77]. Analysis regarding integrity is provided in section 4.3.3.1.

CBC mode requires plaintexts, that do not fit the block-size of the cipher, to be padded accordingly. In some cases, combinations of padding types and error messages may allow for so-called padding oracle, also known as Vaudenay's attack [78]. The author understands that there are typically three pre-conditions that need to be fulfilled in order to abuse a padding oracle [78], [79] to disclose plaintexts or to re-encrypt (CBC-R [80]) arbitrary plaintexts. These pre-conditions are:

1. The plaintext length is determined by the padding
2. Padding errors must be reported by the receiver before integrity is being checked
3. The oracle must allow for identification of an exact byte value within the influenced plaintext

In case of the M-Bus DAL, the plaintext is prefixed with the values 2Fh 2Fh and padded with 2Fh for the remaining bytes of the block. As the DIF/VIF structure exactly defines the length of the data record, the receiver does not really need to verify the padding. As a result, pre-condition 1 does not really apply.

It is very likely that real-world implementations do not report any padding errors for plaintexts for which the padding does not exclusively consist of one or multiple 2Fh. Thus, pre-condition 2 is unlikely to hold.

Assumed the oracle would report if any of the padding bytes is not 2Fh. Under this assumption, an adversary could determine the exact length of the padding by testing for 2Fh and could conclude the data record total length. However it would not be possible to recover any of the plaintext bytes within the block, since data records basically allow 2Fh as DIF/VIF or data and the padding does not contain any hint on the length. Consequently, it is not possible to identify an exact value for the data record (pre-condition 3).

Following that, the author concludes that padding oracle does not apply and therefore the recovery of plaintexts is not possible by such. As CBC-R relies on a working oracle, CBC-R does not apply either.

Extended Link Layer: The standard mandates to use counter mode for encryption in the ELL. Counter mode turns a block cipher into a key stream generator. Counter mode is *"sensitive to usage errors" [81].* As with

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

stream ciphers or other modes of operation that turn a block cipher into a keystream generator, keys and IVs must be chosen with care since keystream repetition could allow for plaintext recovery. This issue is being discussed in detail in section 4.3.1.6.

General: All analysed M-Bus encryptions modes work with static keys. Therefore, the analysis of the M-Bus encryption modes in sections 4.3.1.4, 4.3.1.5, 4.3.1.6 focus on the IVs only.

4.3.1.4 Initialization Vector for Dedicated Application Layer Encryption Mode 4

This section will discuss whether the dedicated application layer encryption mode 4 is based on adequate initial vectors.

Encryption mode 4 uses an all-zero IV. That means, all 16 bytes will be zeros and do not influence the plaintext block P1 before encryption since the intermediate text (I1) before encryption is $I1 = P1 \oplus IV = P1 \oplus 00\ 00 \ldots 00\ 00 = P1$. Following that, equal plaintext will result in equal ciphertext. Hence, an adversary observing two equal ciphertexts could assume zero consumption due to equal absolute consumption values must have been submitted. Submission of absolute consumption values is the standard behaviour of all meters available within the lab.

In section 5.12.6.1 clause b) the standard [7] mandates to prefix the message M with a date and time record to avoid zero consumption detection. The date and time (record type F) maximum granularity is minutes. For reference consult annex A "Coding of Data Records" of the standard.

Assumed a victim's meter is sending consumption data more than once a minute. If the ciphertext repeats within the same minute and regularly changes each minute then it is extremely likely that zero consumption is being observed.

The lab did not include meters that use encryption mode 4. Most available meters were configured to send consumption data every few seconds. See appendix 7.2.2 for a short capture of a randomly chosen device. For that reason, it is necessary to choose a date and time record type whose granularity is less than the meter nominal transmission interval. For the case above, a granularity of seconds such as specified for the record types I and J in annex A of the dedicated application layer specification, would suffice.

4.3.1.5 Initialization Vector for Dedicated Application Layer Encryption Mode 5

This section will discuss whether the dedicated application layer encryption mode 5 is based on adequate initial vectors.

Encryption mode five specifies a non-zero IV. Still, the requirement for unpredictability holds. The IV is composed as shown in figure 14. The elements used for the IV are:

- Manufacturer ID (2 bytes)
- Device address (6 bytes)
- Access number (8 bytes)

The manufacturer ID and the device address do not change over the life-time of a meter. According to section 5.9.2 of the standard, the access number should be incremented to signal new frames. For meters that support mode S which is outlined in table 2, the standard mandates to increment the access number for synchronous transmissions only. Asynchronous frames in between two synchronous transmissions will have identical access numbers. There are two issues with this protocol specification:

1. IVs repeat

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

2. IVs are predictable

Issue 1 applies to devices that support synchronous transmission only. Since it is mandated to repeat IVs for asynchronous frames in between of synchronous transmissions, the ciphertexts are identical for equal consumption values and would therefore allow to detect zero consumption. To counter that issue, the standard advises in section 5.9.2 to *"add a time stamp or an incremental counter (VIFE "Unique telegram identification") to the telegram content "*. It was already discussed in section 4.3.1.4 that this measure does not counter zero detection for frequent transmitting devices when relying on the time and date record. Moreover, the standard should have noted that the additional record needs to be inserted as first record otherwise ciphertext blocks up to the block that contains the record do not change.

Issue 2 applies to all communication modes but due to the current application layer construction does not seem to be exploitable. Predictable IVs allow for blockwise-adaptive chosen plaintext attacks (blockwise-adaptive CPA) as discussed in [82] and [83]. Regarding M-Bus, this would mean that if one predicts the IV correctly and could choose the first plaintext block (Pg) then one could guess for the correct plaintext (Pi) of of any past frame's ciphertext block (Ci). The test whether the guess (x) was successful works as follows:

```
Calculate the first plaintext block Pg = x ⊕ Ci-1 ⊕ IV.
Test whether Cg = Enc(Pg ⊕ IV) = Enc((x ⊕ Ci-1 ⊕ IV) ⊕ IV) = Enc(x ⊕ Ci-1) = Ci
```

Assumed the adversary guessed the correct value x for the plaintext Pi then ciphertexts Cg and Ci have identical values. When considering the captured plaintext in figure 15 for a guess, one recognises that only four of the bytes are actually variable. After all, the average number of guesses would be 2^{32-1}. The con-

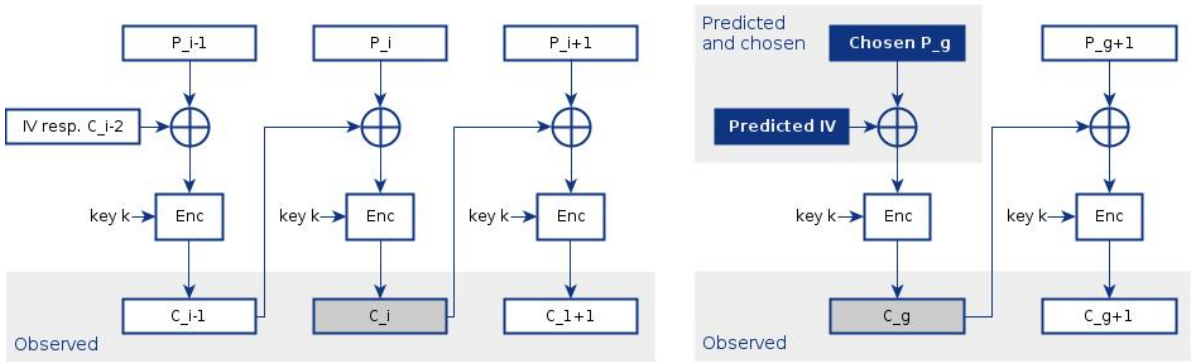


Figure 22: Blockwise-adaptive Chosen Plaintext Attack

sumption value calculated in table 4 is in Wh. In case the meter only counts in thousands of Wh the number of guesses reduces again to $2^{32-1} \cdot 10^{-3} \approx 2'147'484$.

Referring to appendix C.2.3 of the wireless meter readout specification [8] the transmission in communication mode Tx of an 31 byte frame in figure 7 calculates to 4.32 ms. Assuming an adversary will need an equally large frame to choose the plaintext then the total round trip time (RTT) is about 10ms whereby the processing time at the smart meter side has not been taken into account. Accordingly, the approximate time needed for a successful guess is around $2^{32-1} \cdot 10^{-3} \cdot 10^{-2}$ s ≈ 6h.

Research [84], [85] in the fields of the Secure Socket Layer and Transport Layer Security (SSL/TLS) has shown that if an adversary can prepend an arbitrary number of bytes to the plaintext of interest, the number of average guesses for the four bytes can be reduced to approximately $4\ 2^{8-1} \cdot 10^{-2}$ s ≈ 5s due to the fact that each byte can be isolated and guessed on its own.

At the time of writing, the author is not aware of any standardised command or protocol sequence initiated

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

from remote (directed to the meter) that would allow to choose the first block plaintext of the data records (sent by a meter) as needed. Thus, issue 2 remains a theoretical vulnerability due to limitations of the DAL [7].

4.3.1.6 Initialization Vector for Extended Link Layer Encryption Mode 1

This section will discuss whether the extended link layer encryption mode 1 is based on adequate initial vectors.

Encryption mode 1 within the ELL [8] specifies CTR mode of operation. Unlike with CBC mode, the requirement for unpredictability of the IV only partially applies [86] to CTR mode. Specifically, the referred paper identifies predictable IVs allowing for time-memory trade-off (TMTO) attacks. In case of AES-128 in CTR mode, a completely predictable IV lowers the overall security to 85-bits.

Referring to the description in section 4.2.7.2, the IV is created from approximately eight bytes fixed and eight bytes predictable value. Accordingly, the whole 16 bytes significantly lack entropy. Luckily, the eight bytes fixed value are unique to each device and therefore serves as a salt which restrict the TMTO attack to a single device.

As with most stream ciphers, keystream repetition poses severe impact. The repetition of the IV under the same key (k) used to create two ciphertexts (Ca, Cb) would leak information on the plaintexts (Pa, Pb) as follows (remark 7.22 in [58]):

```
Ca = Enck(IV) ⊕ Pa
Cb = Enck(IV) ⊕ Pb
Pa ⊕ Pb = Ca ⊕ Cb
```

Figure 23 provides schematics for the encryption and decryption in counter mode of operation. Note that Pa or Pb denotes a plaintext of one or multiple blocks e.g. Pa_0 … Pa_i.

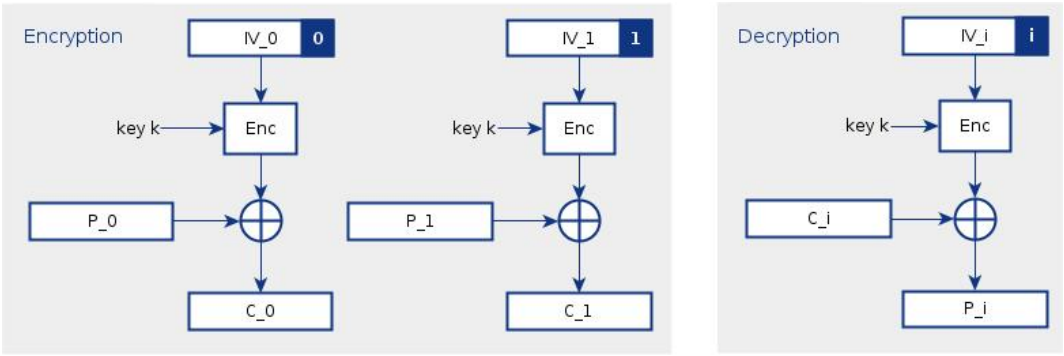


Figure 23: Counter Mode of Encryption

As an example, it is assumed that two application payloads containing consumption values (Pa, Pb), as provided in figure 24, have been encrypted to form Ca and Cb. An adversary observing Ca and Cb in the network may now calculate the difference between the two which is exactly the difference of Pa and Pb

```
Pa =   2F 2F 04 83 3B 08 34 05 00 2F 2F 2F 2F 2F 2F 2F (341'000 Wh)
Pb =   2F 2F 04 83 3B 14 34 05 00 2F 2F 2F 2F 2F 2F 2F (341'012 Wh)
Ca ⊕ Cb =    00 00 00 00 00 1C 00 00 00 00 00 00 00 00 00 00
```

Figure 24: Example of Counter Mode of Encryption with Equal IVs

Having either of the plaintexts would allow the recovery of the other one. Without knowledge of the plain-

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

texts, the difference $1C_h$ basically indicates the difference of the two values. $1C_h$ translates into a difference of three bits in total. Maximum and minimum differences can be calculated from the three bits as provided in figure 25.

```
Max. difference:      0001 1100 = 28
       -0000 0000 =  0
                  = 28
Min. difference:      0001 0000 = 16
       -0000 1100 = 12
                  =  4
```

Figure 25: Example of Consumption Difference Recovery

Following that, the consumption value must have changed for something in between 4 and 28 Wh. Collection of further Cx might help to narrow that difference. Observation of a difference of zero would indicate equal plaintexts which factually indicate zero consumption. Note, that the plaintext has been arbitrarily chosen by the author to construct an example. Such calculation would of course require basic knowledge of the structure of the plaintexts. Obviously, the example effectively visualises the requirement of unique IVs for each encrypted block since a unique IV hinders the cancellation of Enck(IV) and therefore prevents the extraction of the difference.

Providing a general approach for the calculation of the minimum and maximum differences is not straight forward as the order of the plaintext bytes need to be considered. Especially, bit changes over byte boundaries would require additional calculation. However for changes within a single byte boundary the maximum difference is the value of the bits that actually changed. The minuend for the minimum difference is all-zero but the most significant bit (MSBit) that changed will be set to 1. The subtrahend for the minimum difference is 1 for all bits that changed but the MSBit.

The wireless meter readout part [8] of the series specifies the IV for the ELL encryption mode 1 as shown in figure 21. The four byte session number is composed of the meter time in minutes and a four bit (nibble) session number. Whereby the standard restricts the maximum number of sessions to 16 per minute. Following that, the session number field basically guarantees uniqueness of the IV among time and sessions. The frame number ensures uniqueness of the IV among frames during the same session and the block number ensures uniqueness of the IV among blocks of the same frame.

However, depending on the implementation, uniqueness is not entirely guaranteed. In section 11.2.4.3 of the standard it is stated that *"The Time-field describes a relative minute counter " [8].* An absolute minute counter would ensure uniqueness of the IV over the life-time of a meter. A relative minute counter can only guarantee uniqueness back to the relative point in time. The term relative is not further being specified. Thus, devices that start over the minute counter each hour are prone to disclosure of plaintexts. The size of the time field would actually allow for an absolute minute counter. Further concerns regarding potential IV reuse are provided in 4.3.1.7.

4.3.1.7 Initialization Vector and Key Reuse

This section will focus on IV and key reuse for stream ciphers prevented?

Dedicated Application Layer: CBC mode is the only mode of operation supported in the DAL. CBC does not turn the block cipher into a key stream generator. Though, some consider CBC as a stream cipher (remark 7.25 in [58]). Additional mention of the IV used in the DAL exists in sections 4.3.1.3, 4.3.1.4 and 4.3.1.5.

Extended Link Layer: The uniqueness of IVs for the CTR mode such as discussed in section 4.3.1.6 is not entirely guaranteed. In addition, there are some related issues and uncertainties with the specification that could result in IV reuse:

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

- Clock synchronisation
- Frame count for requests and responses
- Asynchronous transmissions

Issue 1 Clock synchronisation: The synchronisation of the clock to a time in the past will cause the IV to repeat. Hence, disclosure of plaintexts is possible for meters that allow unauthenticated updates to the clock. See section 4.3.9 for details on the authenticity of clock synchronisation.

Issue 2 Frame count for requests and responses: In bi-directional communication the frame number must be incremented for each of the sent and received frames to avoid IV reuse. This becomes clear from the timing diagram example, figure E.7 in annex E of the standard [8].

Issue 3 Asynchronous transmission: In section 11.2.4.1 the standard states that *"At least after every bidirectional communication session with the meter, the Session Number Field must be changed." [8].* It can be implied that it is sufficient to change the session field after bi-directional communication which would result in reuse of IVs for one-way submission of data if the frame counter is not being incremented.

4.3.1.8 Encrypt-then-MAC or MAC-then-Encrypt

Actually, there is no MAC at all. Neither for the DAL nor for the ELL. See section 4.3.3ff for further reference.

4.3.1.9 Requirement for Randomness

Dedicated Application Layer: CBC mode requires it to be operated with unpredictable IVs. Cryptographically strong randomness is not necessarily required [77]. Note, additional mention of the IV exists in sections 4.3.1.3, 4.3.1.4, 4.3.1.5 and 4.3.1.7.

Extended Link Layer: As with CBC, CTR mode does not require random IVs. Contrariwise, part of the IV would need to be known when using its random access feature. Moreover, for wireless M-Bus, CTR does not require unpredictable IVs. Additional thoughts on the IV specified in the ELL are provided in sections 4.3.1.6 and 4.3.1.7.

Following that, neither of the specified block cipher modes of operation requires randomness.

4.3.1.10 Supported Key Length

All of the three AES encryption modes specified in the draft standard series are specified for use with 128-bit length keys. According to ECRYPT II [76] and NIST [87] symmetric ciphers that support 112-bit key length are considered adequate for medium term protection (approx. 20 years).

Though, in order to make use of the 128-bit cipher strength it is very much desired that full 128-bit length keys are being chosen. Refer to section 4.3.4.2 for issues with the key lengths suggested in M-Bus specification.

4.3.1.11 Support of New Ciphers

Dedicated Application Layer: The DAL specification [7] encryption mode 6 is explicitly reserved for future use. Following that, the encryption algorithm as well as the construction of the IV have not been specified so far.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Extended Link Layer: The ELL encryption mode field as specified in [8] has 3 bits in total. Currently two states are used for "no encryption" and "AES-128 in CTR mode". Therefore, place for six additional types remains.

Consequently, the possibility to upgrade to another algorithm is given.

4.3.1.12 Relaying

An M-Bus wireless relay such as described in section 4.2.6 does not need to be aware of key material used in either the ELL or the DAL in order to relay and rewrite frames. Thus, the encryption can be considered end-to-end. However, there are some other issues with the confidentiality mechanisms that could allow a relaying or any observing party to recover plaintexts. See sections 4.3.1.4, 4.3.1.5 and 4.3.1.6 for reference.

4.3.1.13 Special Protocols

There are further protocols specified that should be protected from eavesdropping. Commands and services concerned are reset, network management, time protocols, alarms and errors as listed at the bottom of section 4.2.3.4.

Alarms and errors are being signalled within the status byte of the data header which is not subject to encryption. Consequently, an adversary could learn from the errors sent whether the meter detected tampering.

Application resets (CI 50_h) are specified within the DAL but are referred to as a special type of upper layer protocol where security services of the DAL and ELL do not apply. Thus, adversaries can capture reset commands.

Clock synchronisation is also specified as a special upper layer protocol. Annex H of the DAL [7] specifies how clock synchronisation commands need to be formatted. There are actually three types of commands (TC field): set, add, subtract. However, from a confidentiality point of few, they all base on the structure provided in figure 26.

CI	Long Data Header	Check Bytes	TC	Payload	Cmd Verify
1 byte	12 bytes	2F 2Fh	1 byte	9 byte	2F 2F 2F 2Fh

Figure 26: Encryption for Clock synchronisation

Clock updates are being submitted as a single encrypted block including the check and command verify bytes. As the current time is public knowledge, applying confidentiality is worthless. Phillip Rogaway once commented on an IPsec draft: *"it is NEVER useful to encrypt known text. Doing so increases the size of packets and the computational complexity of making them, while it provides no security benefit." [82].*

Commands such as remote control of valves and breakers are submitted as data records. Therefore, these could be encrypted.

Network Management specified in sections 5.6.3 and 6.5.2 of the wireless relaying part [9] do not foresee encryption of information and commands used to organise the network.

Precision Timing (mode Q) also specified within the relaying part [9] does not foresee any encryption.

For integrity issues with special protocols consult chapter 4.3.3.4.

4.3.1.14 Version Information Exposure

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Good practise requires avoiding the disclosure of the type and build of devices to a network. This measure shall complicate detection of known vulnerable devices and software versions. Unfortunately, wireless M-Bus frames disclose the meter manufacturer, the type of meter and its version within the frame header. As a result, adversaries may passively try to identify known vulnerable devices just by listening to the spectrum with a wireless M-Bus analyser.

4.3.2 Data Privacy

This section discusses measures taken in order ensure data privacy. It relies on section 4.3.1 but goes a bit further to verify how M-Bus security measures ensure privacy of consumption data.

As mentioned, data privacy implies proper data confidentiality. Sections 4.3.1.4, 4.3.1.5, 4.3.1.6 and 4.3.1.7 describe under what circumstances confidentiality and therefore privacy can or cannot be guaranteed. There are additional parameters such as frame size or frame transmission timing that could leak information on the consumption. As an example, the frame capture of an arbitrarily chosen device is analysed in the following paragraphs. It will be concluded, that following the M-Bus specification does not lead to leakage of information through frame size and frame timing.

Due to the M-Bus DAL DIF/VIF structure, the size of telegrams does not change with the amount measured. Table 4 provides details on the data record used to transmit instantaneous values. The four byte data value in combination with the exponent specified in the VIF byte allows for sufficient large values for any metering purpose, household or industries, over the lifetime of a meter. For values not taking up the four bytes, leading zero bytes will be inserted. Thus, the data field remains 4 bytes.

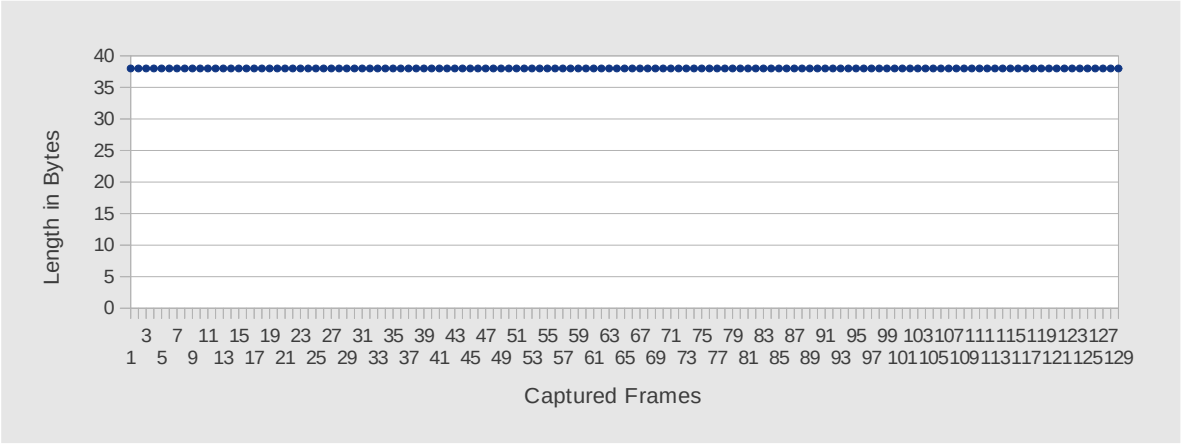


Figure 27: EMH Electricity Meter Steady Frame Size for Consumption

Figure 27 shows a capture of approximately 129 frames which have been recorded during a time span of ninety minutes whereby the metered energy consumption continuously rose. The frame length remained steady with 38 bytes. Actually, all of the EMH meters sent frames with equal size during the measured period. See appendix 7.2.4 for further reference. All of the observed frame sizes and transmission intervals do not seem to be directly related to consumption behaviour. If there are any differences in processing time which relate to the energy flow and would lead to minor derivation of the transmission intervals has not been analysed.

The M-Bus DAL specifies four terms related to the timing of periodic transmission. Whereby, the average transmission interval is termed as the *"nominal transmission interval"*. That interval is not strictly followed to avoid permanent collision with a meter having an equal *"nominal transmission interval"*. To avoid collisions, meters apply *"scatter"* to the nominal value which then results in *"individual transmission intervals"* between frames. Additionally, the term *"average update interval "* is used in the DAL specification [7] to refer to the

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

interval where new consumption data is being submitted.

Figure 28 provides the individual transmission intervals for the same frames as captured in figure 27. It shows that odd transmissions are slightly under 40 seconds and even transmissions are slightly over 40 seconds individual interval. The transmissions at 80, 120 and 160 seconds are not related to consumption behaviour but to frame loss. Due to the large number of devices, the frequency spectrum in the laboratory environment was pretty busy and collisions occurred often. Thus, all frames at 80 seconds actually indicate a single frame loss whereas frames at 160 seconds indicate loss of three subsequent frames.

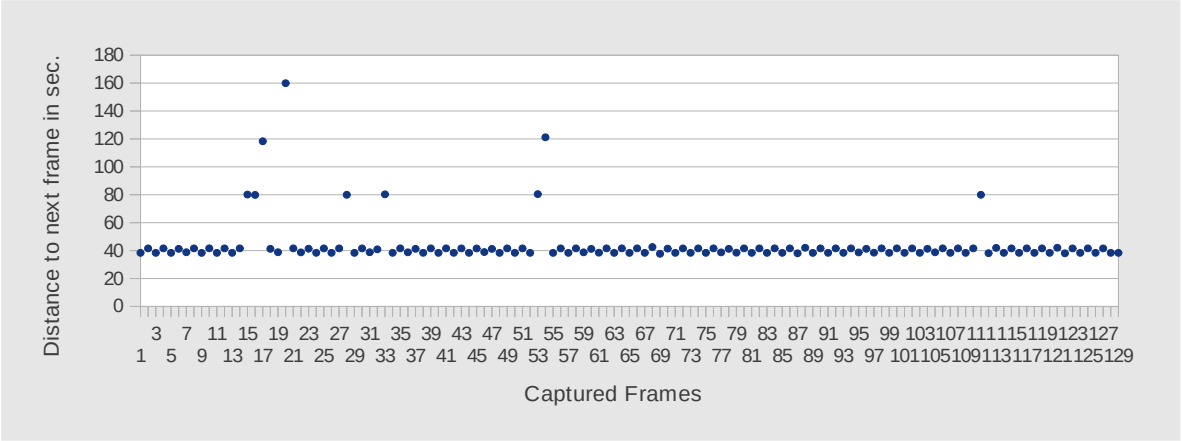


Figure 28: EMH Electricity Meter Individual Transmission Intervals

An obvious approach to avoid collisions towards an efficient use of the frequency spectrum is to keep the spectrum free by just transmitting data when consumption values reach a defined threshold. Apart from M-Bus specific conceptual issues there are privacy concerns that arise from such an approach since an adversary could detect zero consumption and also derive the amount consumed from the individual transmission interval. The shorter the interval the more is being consumed.

Therefore, scientists are researching for more efficient transmission schemes that provide sufficient privacy. An alternative approach for privacy-preserving communication has already been proposed [88].

Consequently, the M-Bus wireless stack in frequent transmit modes is bulky in terms of spectrum use but seems to be privacy-preserving when following the standard. Note, that CPU and application latency issues have not been analysed within this work. Further analysis on privacy issues regarding transmission patterns is provided in [89].

4.3.3 Data Integrity

This section aims to verify whether data in transit is protected from unauthorised manipulation and whether the applied techniques are being considered sufficient measures.

4.3.3.1 Integrity for the Dedicated Application Layer

The M-Bus frames as described in 4.2.3 do incorporate error detection based on a CRC below the application level. However, a CRC cannot protect from manipulation of transmitted information. The DAL does not foresee any other protection mechanism such as a HMAC or a CMAC to ensure integrity of all communication.

Although, in encryption mode 5 and 6 the meter can signal that digitally signed, billing relevant data is contained in by using bits two and three of the configuration word. In annex L.4 of the standard it is suggested to

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

apply *"a legally safe signature. For this method ECC192 is suggested."* [7]. The author assumes the standard refers to elliptic curve digital signature algorithm (ECDSA) as specified in ANSI X9.62 [90] and a popular curve such as P-192 defined in FIPS 186-3 [91]. However, this is not entirely clear from the specification.

None of the devices in the lab did actually apply signatures to billing relevant data. Following that, the DAL is open to attacks that target the manipulation of transmitted data. Specifically, the following issues are present:

1. IV manipulation in order to change the meaning of the first plaintext block [58].
2. Malleable cryptosystems allow the creation of related plaintexts by applying modifications to the ciphertext [92].
3. Arbitrary attachment of plaintext data records

Issue 1, considering the manipulation of the IV, it allows the creation of a meaningful and related first plaintext block. This is due to the nature of the CBC mode of operation which first decrypts the first ciphertext block (C1) and then applies the IV as provided in figure 29. An adversary will chose to alter bits x in the IV in order create a related and meaningful plaintext block P1' such that

$$IV' = IV \oplus x$$
$$P1' = Deck(C1) \oplus IV' = Deck(C1) \oplus IV \oplus x$$

Following that, the chosen bits x will directly influence plaintext P1. Plaintext block P2 will not suffer any changes since the unmodified C1 serves as an IV for the decryption of P2. Hence, the remainder of the blocks will not be altered and decrypt to their correct value Pi.

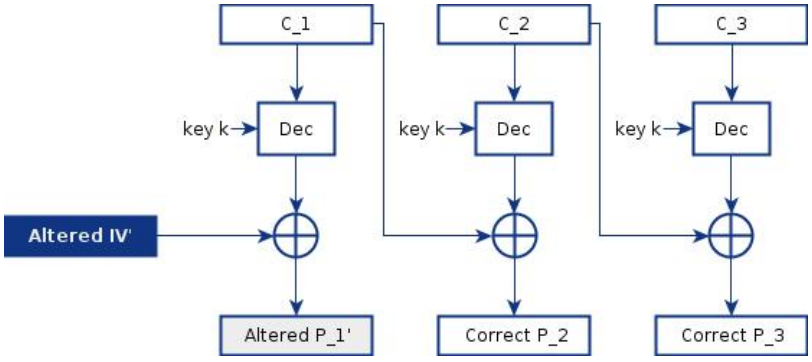


Figure 29: Attack on Decryption in Cipher Block Chaining (CBC) Mode of Operation

Actually, not all of the IV bytes (Bi) can be manipulated to form an altered IV' since the original IV is derived from device dependent properties. Actually, the IV depends on the manufacturer ID field and the device address field which are both used to identify a meter at the receiver side and to lookup corresponding key material. Manipulation of these fields would result in either of the following three scenarios:

a) The receiver is not aware of a device corresponding to the manipulated fields. Thus, a key is not available and data cannot be decrypted.
b) The receiver is aware of a device corresponding to the manipulated fields but decryption results in garbled text because the senders do not share the same key
c) The receiver is aware of a device corresponding to the manipulated fields and the decryption results in meaningful plaintext because the senders share the same key

Thus, in environments where senders do not share the same encryption key an adversary might decide not to manipulate the manufacturer and address fields to avoid scenarios a) and b). Assumed the trans-

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona
T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

mitted data is a plaintext block (P1) containing a consumption value of 341 kWh as decoded in table 4. Additionally, figure 30 provides that the original IV, the key k used for encryption and the corresponding ciphertext block C1.

```
P1      2F 2F 04 83 3B 08 34 05 00 2F 2F 2F 2F 2F 2F 2F
k       AB AD 1D EA AB AD 1D EA AB AD 1D EA AB AD 1D EA
IV      2D 2C 07 71 94 15 01 02 B3 B3 B3 B3 B3 B3 B3 B3
C1      C6 A0 79 B1 66 0B BF 8F 65 BC 4A 43 37 8D DF BE
```

Figure 30: Plaintext P1, IV, key k and Ciphertext C1 for CBC IV Manipulation Example (Original)

The IV and the plaintext P1 for this specific example are composed as outlined in figure 6. Note, that the structure and actual contents of the example are derived from a real world capture. The subsequent paragraphs will consider the possibilities of manipulating the IV in order to influence bits in the data record header (DIF, VIF, VIFE) and the data record (consumption value).

	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15	B16
IV	Manuf. ID		Device Address				Vers.	Type	ACC	ACC	ACC	ACC	ACC	ACC	ACC	ACC
P1	Leading 2Fh		DIF	VIF	VIFE	Consumption Value				Trailing 2F						

Figure 31: Plaintext P1 and IV meaning of bytes

The possibilities for the manipulation of the IV are listed in table 5 for all of the bytes according to the DAL specification. See also section 4.2.4.5 for an example on how the IV is to be constructed.

Bytes	Value (hex)	IV Param	Possibilities
B1-B2	2D 2C	Manuf. ID	The manipulation of the manufacturer ID would cause the leading two 2Fh bytes of the plaintext block P1 to be altered. According to the specification this would be detected as a wrong decryption. Manipulation of these two bytes is not possible without destruction of the plaintext.
B3-B6	07 71 94 15	Device Address	The manipulation of the device address may cause either of three different states at the frame receiver: The address is not recognised as a known meter. As a result, the frame will be dropped. The address is known but has a different key assigned than for the original meter address. Using a different key for decryption would therefore cause data corruption. Assuming a setup with two meters which share the same key with the collector. The manipulated address has been swapped with the address of the second meter. Following that, the collector will be able to properly decrypt the ciphertext C1 since both of the meters share the same key with the collector. However, P1' is only influenced depending on the second device's address. Thus, the adversary must be very lucky to have a second device address that would allow for meaningful changes of the data record header (DIF, VIF, VIFE) or the least significant Byte (LSB, B6) of the consumption value. Hence, manipulation of the device address only makes sense in environments, where devices share the same key.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

B7	01	Version	The manipulation of the version field works for environments, where the meter is only identified by the device address part. In other words, manipulation works if the version is not combined with the address to lookup the decryption key. In such case, an adversary could abuse the version ID in order to modify B7 of P1. Applied to the example P1, an adversary could manipulate the IV B7 to alter the consumption value.
B8	02	Type	The same conditions as for the version byte B7 apply. Thus, for receivers that do not take the type field into account for the lookup of the key material, an adversary can manipulate BB of P1.
B9-B16	B3	Access Number	According to the DAL specification [7] the ACC is used for replay detection. Subsequent frames with identical ACCs are considered duplicates and should be ignored. It is stated that subsequent frames with a different ACC from the previous frame's ACC should be accepted. See section 4.3.5 for further details on replay detection in the DAL. However, an adversary could manipulate the ACC in order to influence the most significant byte (MSB) of the consumption value (B9). Manipulation of the ACC will turn the padding (idle filler, $2F_h$) into another value as well. The standard does not mandate on how a receiver shall handle frames that contain malformed data records. This is something that would need to be verified with specific M-Bus implementations.

Table 5: Possibilities for IV Manipulation

Table 5 also applies for environments which make use of the wireless relaying part [9] of the standard regardless of the relaying approach (gateway or router). Taking the possibilities listed account and applying those to the example values provided in figure 30 an adversary can for example lower the consumption value. Therefore, the adversary needs to create the altered IV' as follows:

```
P1' = Deck(C1) ⊕ IV'
Deck(C1) = P1' ⊕ IV' = P1 ⊕ IV
IV' = P1' ⊕ P1 ⊕ IV
```

An adversary can read the actual consumption value from the meter display and learn that the amount consumed is 341 kWh. Being aware of the plaintext P1 structure the adversary knows that the hex value of it is 08 34 05 00 and starts at byte B6. Let's assume the adversary aims to approximately half the consumption value to 08 34 02 00_h.Thus, for IV'8 = $02_h \oplus 05_h \oplus 02_h = 05_h$.

```
C1     C6 A0 79 B1 66 0B BF 8F 65 BC 4A 43 37 8D DF BE
k      AB AD 1D EA AB AD 1D EA AB AD 1D EA AB AD 1D EA
IV'    2D 2C 07 71 94 15 01 05 B3 B3 B3 B3 B3 B3 B3 B3
P1'    2F 2F 04 83 3B 08 34 02 00 2F 2F 2F 2F 2F 2F 2F
```

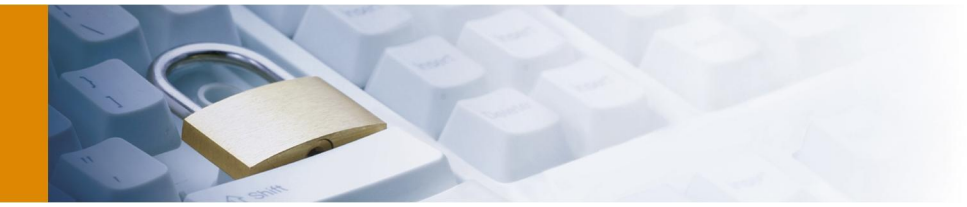
Figure 32: Example of Calculation of Plaintext P1' from Ciphertext C1 using a manipulated IV'

Following that, manipulation of the type byte as highlighted in figure 7 has allowed to adjust the consumption value to 08 34 02 00_h respectively 144'392 Wh. Note, that an adversary would need to actually capture and manipulate two frames with different ACCs to bypass duplication detection at the receiver side. The adversary would then alternately send frames that ACCs differ for each transmitted frame.

Issue 2 "Malleable cryptosystems allow the creation of related plaintexts by applying modifications to the

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch



ciphertext" only applies in very rare cases. Figure 29 provides the schematics of the decryption in CBC mode. As with the manipulation of the IV, the manipulation of a ciphertext block C_i would influence the subsequent plaintext block P_{i+1}. Unfortunately, even minor changes in C_i will completely destroy the plaintext block P_i due to the cipher's diffusion property [93].

An adversary trying to influence the second plaintext block P_2 by manipulation of C_1 will most likely destroy the leading 2F $2F_h$ sequence in P_1 required for detection of proper decryption. The receiver would therefore reject the frame. Manipulation of C_2 will not destroy these flags but will render P_2 unusable.

Following that, for the rare cases where the broken block P_2 is part of a record value, the structure of the data records would remain and an adversary could successfully apply changes to P_3.

Issue 3 "Arbitrary attachment of plaintext data records" is always applicable but the issues impact relies on the meter and how it is handling input data. The M-Bus DAL allows for partially encrypted frames. This means, that plaintext data could follow encrypted data. To attach arbitrary data records, an adversary would need to adjust the total frame length to include the attached plaintext data record. As discussed, the M-Bus does not provide any integrity protection. Neither at the DAL [7] nor at any of the lower layers. Consequently, the length of the frame can be adjusted at will by manipulation of the first byte of the frame which defines the total frame length The frame length byte is highlighted in figure 33. In addition, the encrypted 16 bytes block containing the consumption value is highlighted. The values correspond with those in the example in section 4.2.4.5.

```
1E 44 2D 2C 07 71 94 15 01 02 7A B3 00 10 85 BF 5C 93 72 04 76 59 50 24 16 93 27
D3 03 58 C8
```

Figure 33: wM-Bus Frame Capture Records Encrypted

The encrypted consumption value starts at the third byte of the encrypted block. Its value is 341 kWh encoded LSB first as shown below:

```
Consumption value within encrypted block:      04 83 3B 08 34 05 00 (341'000 Wh)
Consumption value attached as plaintext:       04 83 3B 08 34 02 00 (144'392 Wh)
```

Appending the slightly adjusted plaintext to the encrypted frame provided in figure 33 will result in a modified frame as provided in figure 34 . Changes to the frame have been highlighted accordingly.

```
25 44 2D 2C 07 71 94 15 01 02 7A B3 00 10 85 BF 5C 93 72 04 76 59 50 24 16 93 27
D3 03 58 C8 04 83 3B 08 34 05 00
```

Figure 34: Example wM-Bus Frame having Attached Plaintext Data Records

By the time the receiver parses the frame, it could hold two different values for identical DIF/VIF values. Depending on the receiver software either of the values will have precedence. However, the standard does not define the behaviour in such a scenario. In case the later record has precedence an adversary would be able to arbitrarily override any encrypted record. For the specific example, this means that the adversary can submit arbitrary consumption values.

Of the three issues identified, the third looks the most promising from an adversary's point of view although it heavily depends on the implementation of the collector.

4.3.3.2 Integrity for the Extended Link Layer

As with the dedicated application layer, the M-Bus frames as described in 4.3.2 do incorporate error detection based on a CRC below the extended link layer level. The ELL [8] foresees a 2-byte CRC also being encrypted with the payload. Still, a message authentication code is missing.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

The section will now analyse whether and how the three issues considered for the DAL apply to the ELL. The three issues being considered, in slightly different order, are:

1. IV manipulation in order to change the meaning of the first plaintext block [58].
2. Malleable cryptosystems allow the creation of related plaintexts by applying modifications to the ciphertext [92].
3. Arbitrary attachment of plaintext data records

Issue 1: "IV manipulation in order to change the meaning of the first plaintext block" does not apply in CTR since minor changes with the IV will destroy the plaintext block due to the cipher's diffusion property [93]. CTR encryption and decryption is visualised in figure 23.

Issue 2: "Malleable cryptosystems allow the creation of related plaintexts by applying modifications to the ciphertext" absolutely applies to the ELL. In CTR mode, flipped bits in a block do not affect later blocks since blocks encrypted in CTR are absolutely independent. Referring to figure 23, manipulation of a single bit in ciphertext block C_i exactly influences the same bit in plaintext block P_i and only in P_i.

For some unknown reason, another two byte payload CRC exists at the extended link layer level. The payload CRC is also subject to encryption and actually forms the first two bytes of the first encrypted block within the ELL. Further CRCs are available at the frame level for error detection reasons. Following that, the CRC at the ELL level might have been introduced for integrity reasons. Though, a CRC cannot sufficiently ensure integrity.

CRC		DIF	VIF	VIFE	CMD
CC	22	01	FD	1F	01

Figure 35: Attack against Integrity of ELL Payload: Plaintext Pa

The CRC is computed from the payload using the polynomial specified in [8]. See appendix 7.2.5 for details. Assume the plaintext submitted is a command to close a valve. Therefore, the adversary would know the exact structure and the content of the plaintext P_a as provided in figure 35. It is further assumed that the ciphertext C_a will be intercepted, halted, modified and the modified C_a respectively C_b being released to the valve. Without frame interception, the frame counter would increment and the IVs used for encryption and decryption would not match any more and decryption would fail. However, interception of the frame brings the adversary in an equal state as if observing different ciphertexts C_i that have been encrypted under the same key and IV pair. Therefore, the formula explained in section 4.3.1.6 applies: $P_a \oplus P_b = C_a \oplus C_b$

Meaning, that changes to the plaintext also apply to the ciphertext. In order to open the valve, the adversary would create a valid CRC over the open command (P_b), calculate the difference of P_a and P_b and then apply it to the intercepted ciphertext C_a to form C_b as follows:

```
Pa      = CC 22 01 FD 1F 01
Pb      = F1 47 01 FD 1F 00
Ca      = E7 8E 1B 7B 9D 86
Cb      = Ca ⊕ Pa ⊕ Pb
Cb      = E7 8E 1B 7B 9D 86 ⊕ CC 22 01 FD 1F 01 ⊕ F1 47 01 FD 1F 00
Cb      = DA EB 1B 7B 9D 87
```

Figure 36: Attack against Integrity of ELL Payload: Calculation of Modified Ciphertext Cb

Knowing what the key and the IV were, allows for verification of the result. If the claim holds the plaintext x must be equal to the desired valve open command P_b.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
k      = AB AD ID EA AB AD ID EA AB AD ID EA AB AD ID EA
IV     = 01 23 45 67 89 AB CD EF 01 23 45 67 89 AB CD EF
x      = Enc(IV) ⊕ Pa = 2B AC 1A 86 82 87 0B E2 FE 7A 1D DB C0 38 A4 F6 ⊕ Pa
x      = F1 47 01 FD 1F 00
```

Figure 37: Attack against Integrity of ELL Payload: Cross-check

The value x is the intended value Pb. Valve open. Hence, the ELL cannot not provide adequate integrity protection.

Issue 3: "Arbitrary attachment of plaintext data records" does not apply to the ELL because the ELL does not allow for partial encryption such as the DAL does. Thus, this is not considered an issue.

4.3.3.3 Integrity when Relaying

A relay device does not need to share secrets with its upstream and downstream peers which is an advantage. Unfortunately, missing integrity protection in the DAL and ELL allows for manipulation of the relayed frames. See section 4.3.3.1 and 4.3.3.2 for further issues related to integrity.

4.3.3.4 Special Protocols

The device time is just an example for several commands and services that should be protected from manipulation. The protocols concerned have also been analysed for confidentiality in 4.3.1.13.

Alarms and errors are signalled within the status byte of the data header which are neither encrypted nor integrity protected. Thus an adversary could not only manipulate errors that signal tamper detection but also manipulate remotely initiated alarm and event readouts.

Application resets (CI 50_h) are specified within the DAL but are referred to as a special type of upper layer protocol where security services do not apply. As a result, adversaries can manipulate such commands at will.

Clock synchronisation structure is provided in figure 26. As it does not include measures to ensure integrity, the clock synchronisation is vulnerable to arbitrary changes through adversaries. In combination with the ELL encryption mechanisms, this poses a severe issue since arbitrary clock updates can cause the keystream to repeat. See sections 4.3.1.6 and 4.3.1.7 for reference. Beyond that, meters that make use of time based tariffs can be tricked to allocate consumption to the wrong tariff.

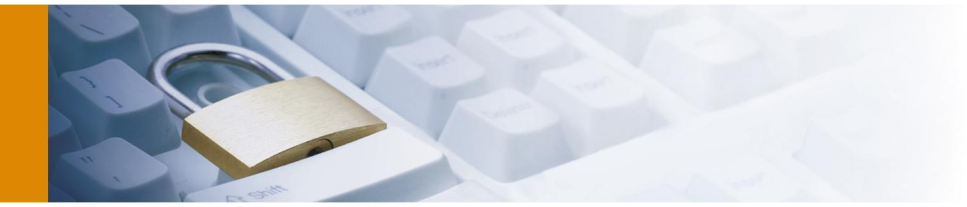
Commands such as remote control of valves and breakers are being submitted as a data record and might therefore be subject to encryption. However, its integrity cannot be guaranteed. See chapter 4.3.3.1 for potential issues.

Network Management as specified in sections 5.6.3 and 6.5.2 of the wireless relaying part [9] do not foresee integrity protection of information and commands used to organise the routes within the network. An adversary could abuse that fact to get into a MitM position, to reroute packets at will or to cause a denial of service condition within the network.

Precision Timing (mode Q) also specified within the relaying part [9] does not foresee any integrity measures. Though, figure 47 of the relying part outlines an optional access control field which is intended to be used for nodes that implement access control. The standard defines: *"Access Control, 4 bytes, optional, shall be present if the node uses access control on this request; the algorithm to use for access control is outside the scope of the current standard" [9].* It is unknown whether that field is just to be understood as a four byte personal identification number (PIN) or whether it does take the payload into account such as with MACs.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch



Implementers would wisely choose to apply some form of MAC. Though, 4 bytes does probably not provide too much of a security margin. Note that similar issues apply as for clock synchronisation.

4.3.3.5 Key length

The subject does not apply as the DAL does not implement any message authentication.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

4.3.4 Key Management

This section will focus on the usage of keys within the DAL [7] and the ELL [8].

4.3.4.1 Hierarchy and Separation

The meter should follow the key separation principle [94]. Therefore, encryption and integrity algorithms should rely on different keys for the same process. Within the data exchange part [6] section 4.3.3 Key Management of the standard, three levels of keys are suggested.

1. Master key (MK)
2. Key encryption key (KEK)
3. Separate keys for encryption and integrity protection per process

The standard foresees that the KEK is distributed under MK and process keys are being derived from the KEK. Though, the standard does not reference any guidance for key generation and distribution such as NIST SP 800-133 [95] and NIST SP 800-57 [94]. In practise, devices are mainly delivered with a pre-configured static key.

Annex L.8.2 of the DAL suggests the introduction of a separate key for the pre-payment functionality of the meter. However, for meters not supporting pre-payment and not supporting any form of MAC or signatures, key separation as suggested is not going to be implemented. Note, that for the meters available in the lab environment, some vendors have delivered unique keys others provide batches of devices that share the same key and some others provide not so wisely chosen keys.

The standard further suggests: *"When keys are being supplied or updated, consideration should be given to using the three pass exchange method. " [6].* As there are no further specification or references on the mentioned method it is assumed that Shamir's no-key protocol [58] is being referred to. The protocol describes the exchange of secret (s) between two parties (A,B) without disclosing their private keys (a,b) under use of a commutative cipher.

```
A => B:       Enca(s)
B => A:       Encb(Enca(s)) = Enca(Encb(s))
A => B:       Deca(Encb(Enca(s))) = Encb(s)
```

There are mainly two issues with that protocol [58]. The cipher chosen and the in-existent authentication. Assume it had been decided not to follow Shamir's proposed algorithm but to use XOR instead. While XOR also fulfils the commutative property, an eavesdropper (E) can disclose the secret (s) and private keys (a,b) from intercepted messages as follows:

```
A => B:       a ⊕ s
B => A:       b ⊕ a ⊕ s
A => B:       b ⊕ s
```

From the three messages E could then compute:

```
s = (a ⊕ s) ⊕ (b ⊕ a ⊕ s) ⊕ (b ⊕ s)
a = (b ⊕ a ⊕ s) ⊕ (b ⊕ s)
b = (a ⊕ s) ⊕ (b ⊕ a ⊕ s)
```

Thus, it is important to use a cipher system such as Shamir's proposed exponentiation in modulo p or a system such as proposed and patented by Massey-Omura [96]. Whatever cipher is being used, the protocol

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

remains vulnerable to man-in-the-middle (MitM) attacks. Therefore, a malicious party (C) with key c would masquerade as A respectively B and learn the secret s as follows

```
A => C:       Enca(s)
C => A:       Encc(Enca(s))
A => C => B:  Deca(Encc(Enca(s)))
B => C:       Encb(Encc(s))
C => B:       Decc(Encb(Encc(s)))
```

In addition, a malicious party (C) could learn the key directly by reflecting the initial message to the initiator (A) of the protocol as follows:

```
A => C:       Enca(s)
C => A:       Enca(s)
A => C:       Deca(Enca(s)) = s
```

Following that, some form of authentication will be need in order to prevent disclosure of s to malicious parties. See section for 4.3.8 for authentication protocols provided in the DAL [7] and the ELL [8]. Alternative approaches for key management in sensor networks are proposed in [97] and [98].

4.3.4.2 Generation and Destruction

In section 5.12.6.2 of the standard in clause e) it is suggested that at least 8 bytes of the key shall be different for each meter. Moreover, clause f) suggests *"The full 16 byte key shall be assigned by the manufacturer together with the meter identification and safely transferred to its customers."* [7]

From a security point of view, it would be desirable to have all bytes of the keys independently chosen for each meter since disclosure of one of the related keys would significantly speed up an exhaustive key search for the remaining 8 bytes. Actually, the recommendation reduces the computational effort to 2^{64} which is severe. The key is actually only half in length but the computational effort has been reduced by factor $2^{64} \approx 1 \cdot 10^{25}$. Additionally, keys should not be related to any device id, version or serial number to avoid reconstruction of keys and to avoid generation of vendor dependent lookup tables through adversaries.

See references in section 4.3.4.1 for guidance on key generation, management and destruction.

4.3.5 Freshness and Replay Prevention

M-Bus should ensure freshness for critical information and actions such as consumption values, authentication or command telegrams.

Freshness of commands and information could by guaranteed by any of the following measures:

a) inclusion of timestamps in messages
b) inclusion of nonces in messages
c) use of one-time pads (OTP) for MAC

To avoid replay and denial of service attacks, the token would need to be protected under use of an appropriate integrity mechanisms otherwise, adversaries might alter the token in order to fit a counter, nonce or to raise a counter to prevent legitimate messages to be accepted.

Dedicated Application Layer: The DAL [7] suggests applying time stamps and unique telegram identifier (UTI) fields for consumption values. Though, this is mainly for the reason of zero consumption detection prevention. In section 5.9 of the standard it is suggested to use a UTI in case it is needed. Appendix C.3 about

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

the remote control of valves and breakers suggest the use of a time stamp or a sequence counter to avoid replay of messages. Furthermore, the standard points out that the ACC is not sufficient to prevent replay in several places of the standard. There are three different attacks that might allow a bypass of the replay detection based on the ACC.

1. Alternate transmission of two messages with different ACCs could defeat detection of replays.
2. An adversary could capture and replay a single telegram, and generate at maximum 254 dummy telegrams in order to replay the captured telegram again.
3. An adversary could capture 255 legitimate frames in order to replay these 255 frames again. Though, this attack would very much depend on the application context and the timing. Thus, this would apply for transmission of basic contents such as consumption values. However, the collection of 255 frames in long transmission interval environments might take some days. Captures of typical transmission intervals are provided in appendix 7.2.4.

Note that the attack outlined in 1) applies to all devices that follow the standard. For more restrictive implementations, attacks as outlined in 2) and 3) might apply.

Extended Link Layer: The ELL does not provide freshness or mechanisms to defeat replay.

General: Replay detection at lower layers can actually not be too restrictive since adversaries could trigger denial of service conditions by injection of maliciously flagged telegrams. In the case of M-Bus, legitimate telegrams would be dropped by receivers if the legitimate telegram and the previously, malicious telegram share the same ACC.

4.3.6 Randomness

This section discusses the use of random number generators for security mechanisms specified in the dedicated application layer. There are a number of services that rely on the use of random number generators. Whether the use of such generators applies to the DAL is discussed

IVs: CBC requires non-predictable IVs. Randomness is not a requirement [77]. See 4.3.1.3 for reference.

Nonces: A random number generator (RNG) could be used to generate nonces in order to provide freshness for messages or entity authentication, though the DAL does not mandate the use of nonces for freshness. Authentication mechanisms which requires nonces are not specified within DAL. See section 4.3.8 for reference.

Keys: As there is currently only a single key for encryption, key derivation using RNGs is not a requirement yet. Though, it would be wise to have a key hierarchy introduced for the generation or distribution of the encryption key. However, none of the devices in the lab actually provides such hierarchy.

Signatures: Computing signatures using the digital signature algorithm (DSA) requires strong random numbers for each signature [91] in order to prevent recovery of the signature key.

Currently, the specified security mechanisms do not require a RNG. Though, improvements to the DAL or extended functionality in a meter would certainly require the implementation of such. NIST FIPS 140-2 provides guidance and introduces security levels for random number generation [99].

4.3.7 Non-Repudiation

Vendors are currently implementing signatures in order to provide non-repudiation service for billing relevant information. The section aims to analyse whether this is achievable although this is not directly related to the DAL. The DAL specifies a flag available in encryption mode 5 to support signed data records as a payload.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

However, non-repudiation is difficult to achieve in a scenario where the metering company has full control over the device that actually ensures the integrity of the data and computes the signature.

"The goal of the Non-repudiation service is to collect, maintain, make available and validate irrefutable evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action." [100].

A meter would need to generate and securely store its own key material. Key material would need to be protected from the metering company to ensure non-repudiation of origin for billing relevant data and to ensure non-repudiation of receipt for pricing information. Additionally, integrity of timestamps, metering and pricing values need to be guaranteed. A trusted platform module (TPM) could provide services to achieve such scenario.

In order to just provide integrity, a MAC might be sufficient.

4.3.8 Entity Authentication

Authentication would provide assurance of the peer's identity and therefore provide the base for access control. The section analyses the extent of authentication available in M-Bus.

4.3.8.1 General

The configuration field in encryption mode 5 of the DAL allows it to signal authenticated commands of type 1 and type 2. However, these two types of authenticated commands are reserved and have not been specified within the DAL [7] so far.

There are two mentions regarding authentication in the 13757 standards series.

Mention 1: Annex L.5 of the DAL states that critical commands might require authentication. From the description provided, the author concludes that controlling a valve is not considered critical and therefore knowledge of a shared secret as used for encryption in the DAL is sufficient. An authentication method or protocol is not being specified.

Mention 2: Annex B.18 of the data exchange part [6] mentions high-level security (HLS) as defined in DLMS/COSEM. DLMS/COSEM specifies client authentication and mutual authentication protocols based on MD5 [101] and SHA-1 [102] or any custom function. However, the analysis of DLMS/COSEM is not part of this work. A brief overview of the DLMS/COSEM standard series is provided in appendix 7.1.2.

The ELL does not mention any authentication protocols.

4.3.8.2 Guidance on Password and Certificate Use

As M-Bus mainly involves communication between devices it does not make use of passwords but rather secrets. Furthermore, the use of certificates is not being explicitly mentioned anywhere in the standard series. Key management respectively key handling is briefly mentioned in the standard and shortly discussed in section 4.3.4 of this report.

4.3.8.3 Authentication Scheme and Session Handling

There is no authentication scheme proposed in the DAL [7] or ELL [8]. The concept of session handling is not

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

considered by the dedicated application layer.

4.3.9 Data Origin Authentication

The data origin authentication section aims to verify whether critical commands such as valve open/close or critical information such as billing relevant data is protected by means of signatures or authentication codes to ensure its origin.

As outlined in previous sections, it is only suggested to apply signatures to billing relevant data. Additionally, there is a single mention of an optional field in the precision timing protocol which could be used for MACs although the algorithm is not specified yet. Any other command or data goes unprotected. See sections 4.3.7 and 4.3.3.4 for reference.

4.3.10 Event Detection

Event detection mainly focuses on the detection of deliberate actions against the M-Bus wireless network or against the meter. Subsections consider error and alarms reporting as well as detection of denial of service conditions.

4.3.10.1 Message Loss

In section 5.9 of the DAL [7] it is mandated that strict increment of the access number (ACC) is to be implemented. The ACC can be used to detect dropped messages. Unfortunately, the number is not part of a MAC and is therefore open for manipulation.

4.3.10.2 Link Availability

With wM-Bus devices that frequently transmit, there is no need to implement a heartbeat since the nominal interval is basically a heartbeat. Though devices that have long intervals might miss an ongoing denial of service attack.

It needs to be considered that environments with lots of frequent transmitting devices have high collision rates. A deliberate attack against the availability of the wireless media might therefore be difficult to tell apart from accidental frame drops.

4.3.10.3 Tamper Evidence

The standard series does not specifically discuss collection and storage of tamper evidence. However, the DAL does specify the error and alerting protocol which provide mechanisms to signal tamper detection and to transmit tamper evidence. More on the confidentiality and integrity of the error and alarm protocol is provided in sections 4.2.3.4, 4.3.1.13 and 4.3.3.4

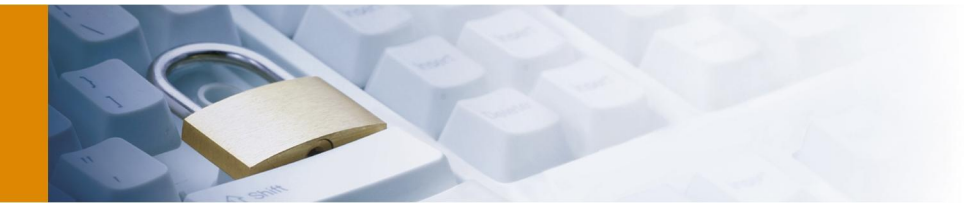
4.3.11 Access Control

This section aims to verify whether M-Bus foresees any access control for assets such as consumption data or commands to open and close valves or breakers.

The data exchange part [6] of the series introduces access control and cites DLMS/COSEM which defines a role based concept including client roles and selective access (read, write) on data. However, the analysis of

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch



DLMS/COSEM is not within scope of this project work. Despite the description of key hierarchy in the data exchange part, the M-Bus devices observed within the lab environment used the same single symmetric key for all security services. Moreover, the standard series mentions in places that knowledge of the key is sufficient to access a meter or control a valve or breaker. See section 4.3.8.1 for reference.

An exception poses precision timing (mode Q) which foresees a 4 byte access code per time change command which basically poses a limitation for few commands. Although, this is more of a data origin authentication than a description of an access control concept. See section 4.3.3.4 for reference.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

4.4 Attack Scenarios

An adversary would need to gain a MitM position or would need to replay messages in order to take advantage of the missing integrity protection described in sections 4.3.3.1, 4.3.3.2, 4.3.3.3 and 4.3.3.4. Applied to wireless environments, this means that adversaries either gain control over relay devices which would allow for delaying, interception and alteration of messages in transit or adversaries alternatively employ some technique to capture, drop and resend messages. Subsections will provide some scenarios on how such attacks could be realised in practise.

4.4.1 Man-in-the-Middle

In wireless M-Bus, a MitM position can be achieved if relays exploit the full capability of network management as specified in the relaying part [9] of the series. Thus, the network should organise itself making use of the network management capabilities. In such scenario, a rogue relay would try to provide better link quality and eventually become the preferred relay. Becoming a rogue relay is feasible as discussed sections 4.3.1.13 and 4.3.3.4.

For environments where peers and hops are configured manually, a MitM position could only be gained through impersonation of a legitimate relay device and complete shielding of such. This will of course require physical access to the legitimate relay or to its surroundings.

The MitM position has the advantage, that messages can be intercepted reliably and the attack is hard to detect.

4.4.2 Jam and Replay

This section will discuss an alternative way that allows to replay messages by applying the technique of jam and replay (JAR). MitM attacks just apply to a small set of devices which use a certain malicious device as a relay.

For the JAR attack, as visualised in figure 3, the adversary identifies the nominal transmission interval of the device during a learning phase. It further records the messages (Mx) during that phase to subsequently modify and replay the messages. During later legitimate transmissions, the adversary is actively jamming the spectrum taking the scatter into account. It then immediately transmits the manipulated message (Mx') right after the original message was jammed. JAR does apply to all wM-Bus devices in range and does not need to get into a MitM position and does not need physical access to the device which is considered an advantage. The downside is clearly that jamming is detectable and that messages are being replayed. More on replay detection and prevention in the M-Bus DAL [7] is provided in section 4.3.5.

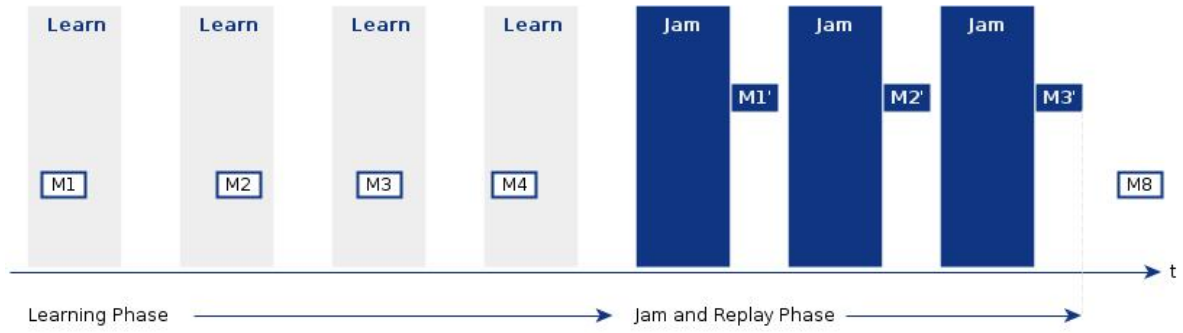


Figure 38: Jam and Replay (JAR) Attack Sequence

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

4.4.3 Shield and Replay

Shield and Replay (SAR) is an alternative version of JAR. As with JAR, an adversary would collect messages for a certain period and replay the messages later on. In the case of SAR, legitimate devices would need to be completely shielded to cancel radiation. Afterwards, altered messages will be replayed.

The advantage of the SAR approach is that the device to replay the messages does not need to jam the spectrum and therefore runs on significant lower energy consumption. Moreover, chances are zero that the jamming sequence runs out of sync over long periods and that jamming is being detected. However, physical access to the legitimate device will be required.

SAR, although slightly related to, should not to be confused with the specific absorption rate.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

5 Conclusion

The major goal of the study was to identify whether the wireless M-Bus as specified within the relevant current and draft ISO specifications [6], [53], [7], [8], [9], [45] can compete with today's challenges and whether known network security issues apply.

The protocol stack has therefore been analysed for services such as confidentiality, integrity, availability, authenticity and non-repudiation. In addition, the specified security mechanisms have been analysed for their effectiveness. Unfortunately, major vulnerabilities have been identified. The discovered issues range from inadequate key length over disclosure and manipulation of encrypted telegram contents to full exposure of key material. It should be recognised that all identified issues rely on theoretical verification and pose conceptual issues under certain assumptions.

As documented in the main chapter, chapter 4, wM-Bus seems to be robust against deduction of consumption behaviour from the wireless network traffic. Consequently, it is considered privacy-preserving against network traffic analysis. Unfortunately, there have been issues identified which obsolete that fact.

The short statements on the major goals are:

- Yes, known network security issues apply.
- No, M-Bus cannot compete with current challenges.

Some specific claims are:

- The standard recommends to choose half of the key unique to each meter which reduces key size to 64 bits
- Inappropriate key and IV use allows for zero consumption detection
- Inappropriate key and IV derivation may disclose plaintexts including consumption values
- Missing integrity protection allows for manipulation of consumption values in transit
- Missing integrity protection allows for manipulation of valve and breaker open/close commands
- Lack of authentication with clock updates may lead to key stream repetition
- Lack of authentication for network management could allow adversaries to become a rogue relay
- Plaintext error and alarm notifications allow an adversary to recognise if tamper switches have been triggered
- Disclosure of device manufacturer, meter type and version ID simplify identification of vulnerable targets
- Loose specified key update mechanism leads to key disclosure

The author is currently not aware of any publicly available security analysis on the wireless M-Bus. Hence, it is very likely that vendors advertising AES support for their wM-Bus devices are not aware of the potential impacts of the outlined conceptual issues. Orchestrating a remote disconnect for a large number of meters could severely affect the reliability of power supply [12]. Even practical analysis of devices in a lab environment has been included in some parts of this study. However, an extensive analysis of meter implementations, has not been conducted.

Future vulnerability analysis in these fields may focus on further real-world implementations and target the evaluation of the effective impact of the claimed findings.

It is worth mentioning that significant efforts of the OMS Group and the German Federal Office for Information Security (BSI Germany) have lead to additional proposals which suggest an integrity-preserving authentication and fragmentation layer (AFL), an additional encryption mode relying on AES-CBC using ephemeral keys and TLS 1.2 support for wM-Bus. An initial draft specification [13] covering these enhancements was released just prior to Christmas 2012 but has not been considered within this study. An analysis of that draft would further contribute to the overview on the wM-Bus stack security and also appreciate the latest devel-

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

opments. Referring to these latest developments the author also can conclude that the security level of wM-Bus has been recognised independently and that the existence of some yet undisclosed studies on the security of wM-Bus is very likely.

The author assumes that smart meters will be required to support the core principles of information security shortly. Support for the core principles will become a standard and will not remain a unique selling proposition. Moreover, devices that provide remote control will be subject to tighter regulation and governance than simple remote reading devices. In that context, it would be interesting to understand whether M-Bus can compete with future challenges but also whether it can compete against other technologies. To know how the wM-Bus stack compares to ZigBee profiles and what advantages DLMS/COSEM could provide over the M-Bus dedicated application layer, if any, would be very valuable.

In the long run it would seem there will be convergence towards IP based communication and more common information technology protocols. For wireless M-Bus, the drafted improvements relying on TLS 1.2 are already a step towards this direction. The Internet of Things (IoT) will be used to reduce emission and to optimise energy consumption in buildings and municipalities. An intermediate step towards a fully IP based network is provided in the Ubiquitous Green Community Control Network Protocol IEEE 1888 standards family [106] which provides monitoring and control, independent of the multitude of sensor networks and protocols. IEEE 1888 aims to add an abstract layer on top of protocols such as ZigBee, WiMax etc. in order to unify authentication, access control and accounting as well as to provide an abstract application programming interface (API) for all major programming languages.

Besides the technical issues and developments with metering, legal aspects need to be clarified. Not only does the frequency of meter readings affect the consumer privacy but also the records management at the metering company. It is not always clear who the owner of the consumption data is. Respectively, it largely depends on local culture and law. Data protection officers and records management specialists will need to provide advice and metering companies will be required to conduct risk assessment and to apply information security management systems. Moreover, it is likely that consumers will be requested to wave data privacy rights to get accurate services.

Finally, vulnerability analysis like this project work and studies on detection mechanisms such as for detection of the manipulation of measurement data [107], all contribute to the overall security awareness and towards more reliable grids and thus to reliable power supply for the next generation.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

6 Bibliography

[1] European Commission. Energy Efficiency Plan. 2011

[2] United States of America. H.R. 6582: American Energy Manufacturing Technical Corrections Act. 2012

[3] B. Cook et al. The smart meter and a smarter consumer:quantifying the benefits of smart meter implementation in the United States. In Chemistry Central Journal. 2012 (DOI 10.1186/1752-153X-6-S1-S5)

[4] CEN-CENELEC eMobility Co-ordination Group. Standardization for road vehicles and associated infrastructure. 2012

[5] W. Galand. Elster REX2 Smart Meter Teardown. iFixit . Jul. 2011. [Online]. Avail-able: http://www.ifixit.com/Teardown/Elster+REX2+Smart+Meter+Teardown/5710/1 [Accessed: 31. Jan. 2013]

[6] prEN 13757-1:2012: Communication system for meters and remote reading of meters - Part 1: Data exchange

[7] prEN 13757-3:2011: Communication system for meters and remote reading of meters - Part 3: Dedicated application layer

[8] prEN 13757-4:2011: Communication system for meters and remote reading of meters - Part 4: Wireless meter readout (Radio meter reading for operation in SRD bands)

[9] EN 13575-5:2008: Communication system for meters and remote reading of meters - Part 5: Wireless relaying

[10] H. Ziegler. CEN TC294 (Meter Communication) and the Mandat M/441. Open Meter Workshop, Brussels, Belgium. 4. Feb. 2010. [Online]. Available: http://www.openmeter.com/documents/Ppt0000012.pdf [Accessed: 11. Feb. 2013]

[11] R.A. Caralli, J.F. Stevens, L.R. Young, W.R. Wilson. The OCTAVE Allegro Guidebook, v1.0. Cert Program, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213. May 2007

[12] M. Costache, V. Tudor, M. Almgren, M. Papatriantafilou and C. Saunders. Remote Control of Smart Meters: Friend or Foe? . In Proceedings of the Seventh European Conference on Computer Network Defense (EC2ND), pp. 49-56. Sep. 2011 (DOI 10.1109/EC2ND.2011.14)

[13] Open Metering System. Technical Report 01 Security. Issue 1.1.0 (Draft). 20. Dec. 2012. [Online]. Available: http://www.oms-group.org/download/OMS-TR01_Security_v110.pdf [Accessed: 31. Jan. 2012]

[14] K. Boutorabi. You Can't Have The Smart Grid Without Smart Meters. Electronic Design. Jun. 2010. [Online]. Avail-able: http://electronicdesign.com/article/power/you_can_t_have_the_smart_grid_without_smart_meters-60529 [Accessed: 31. Jan. 2013]

[15] F.M. Cleveland. Cyber security issues for Advanced Metering Infrastructure (AMI). In Proceedings of IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, pp. 1–5. 2008 (DOI 10.1109/PES.2008.4596535)

[16] S. McLaughlin, D. Podkuiko and P. McDaniel. Energy theft in the advanced metering infrastructure. . 2010 (ISBN 978-3-642-14378-6)

[17] J. Liu, Y. Xiao, S. Li, W. Liang and C.L.P. Chen. Cyber Security and Privacy Issues in Smart Grids. In IEEE Communications Surveys Tutorials, vol. 14, no. 4, pp. 981–997. 2012 (DOI 10.1109/SURV.2011.122111.00145)

[18] A. Hahn and M. Govindarasu. Cyber Attack Exposure Evaluation Framework for the Smart Grid. In Proceedings of IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 835 –843. Dec. 2011 (DOI 10.1109/TSG.2011.2163829)

[19] M.A. Rahman, P. Bera, and E. Al-Shaer. SmartAnalyzer: A noninvasive security threat analyzer for AMI smart grid. In Proceedings of IEEE INFOCOM. Mar. 2012 (DOI 10.1109/INFCOM.2012.6195611)

[20] H. Ziegler. The M-Bus: A Documentation, Rev. 4.8. Fachbereich Physik, Universität-GH Paderborn, 33098 Paderborn, Germany. 1997. [Online]. Available: http://www.m-bus.com/files/MBDOC48.PDF [Ac-cessed: 11. Feb. 2013]

[21] G.N. Ericsson. Cyber security and power system communication essential parts of a smart grid infrastructure. In Proceedings of IEEE Transactions on Power Delivery, Vol. 25, No. 3, pp. 1501–1507. 2010 (DOI 10.1109/TPWRD.2010.2046654)

[22] P. Hasse. Smartmeter: A technological overview of the German roll-out. 29th Chaos Communication Congress "Not my department", Congress Centrum Hamburg, Germany. Dec. 2012. [Online]. Avail-

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

able: http://events.ccc.de/congress/2012/Fahrplan/attachments/2240_smartmeeter.pdf [Accessed: 31. Jan. 2013]
[23] A. Borbely and J.F. Kreider. Distributed Generation: The Power Paradigm for the New Millennium. CRC Press. 2001 (ISBN 0-8493-0074-6)
[24] European Commission for Energy. Financing Renewable Energy in the European Energy Market. 2011
[25] EURELECTRIC. Smart Grids and Networks of the Future. 2011
[26] U.S. Department of Energy. 2009 Smart Grid System Report. 2009
[27] U.S. Department of Energy. 2010 Smart Grid System Report. 2012
[28] G.N. Sorebo and M.C. Echols. Smart Grid Security: An End-to-End View of Security in the New Electrical Grid. CRC Press. 2011 (ISBN 978-1-4398-5587-4)
[29] ENISA. Smart Grid Security: Annex I. General Concepts and Dependencies with ICT. 2012
[30] E.D. Knapp. Industrial Network Protocols, AMI and the Smart Grid. In Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Syn-gress. 2011 (ISBN 978-1-59749-645-2)
[31] NIST. Security Profile for Advanced Metering Infrastructure. v2.0, Jun. 2010
[32] ENISA. Smart Grid Security: Recommendations for Europe and Member States. Jul. 2012
[33] M. Rafiei and S.M. Eftekhari, A practical smart metering using combination of power line communication (PLC) and WiFi protocols, In Proceedings of 17th Conference on Electrical Power Distribution Networks (EPDC), 2012, pp. 1–5, May 2012
[34] Smart Meters Co-Ordination Group. Standardization mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability M/441: Final Report v0.7. Dec. 2009
[35] Federal Office for Information Security (BSI) Germany. Technische Richtlinie BSI-TR-03109-1: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, v0.5. 2012
[36] EN 13575-1:2002: Communication system for meters and remote reading of meters - Part 1: Data exchange
[37] IEEE Std 802.15.4:2011. IEEE Standard for Local and metropolitan area networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)
[38] C. Bennet and D. Highfill. Networking AMI Smart Meters. In Proceedings of Energy 2030 Confer-ence. ENERGY 2008. IEEE. pp 1-8. Nov. 2008 (DOI 10.1109/ENERGY.2008.4781067)
[39] V. Aravinthan, V. Namboodiri, S. Sunku and W. Jewell. Wireless AMI Application and Security for Controlled Home Area Networks. In Proceedings of IEEE Power and Energy Society General Meeting, pp. 1-8. Jul. 2011 (DOI 10.1109/PES.2011.6038996)
[40] ZigBee Alliance. Home Automation Public Application Profile. ZigBee Profile: 0x0104 Revision 26, Version 1.1, Feb. 2010
[41] ZigBee Alliance. Smart Energy Profile Specification. ZigBee Profile: 0x0109, Revision 16, Version 1.1, Mar. 2011
[42] A. Sikora, P. Villalonga, and K. Landwehr. Extensions to wireless M-Bus protocol for smart metering and smart grid application. In Proceedings of the International Conference on Advances in Computing, Com-munications and Informatics, New York, pp. 399-404. Aug. 2012 (DOI 10.1145/2345396.2345462)
[43] EN50090-4-1:2004. Home and Building Electronic Systems (HBES) Part 4-1: Media independent layers - Application layer for HBES Class 1
[44] S. Cavalieri, G. Cutuli and M. Malgeri. A Study on Security Mechanisms in KNX-based Home/Building Automation Networks. In Proceedings of 2010 IEEE Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1-4. Sep. 2010 (DOI 10.1109/ETFA.2010.5641237)
[45] EN 13575-6:2008: Communication system for meters and remote reading of meters - Part 6: Local Bus
[46] EN 62056-21:2002, Electricity metering - Data exchange for meter reading, tariff and load control - Part 21: Direct local data exchange
[47] E. Zountouridou, E. Karfopoulos, S. Papathanassiou and N. Hatziargyriou. Energy-Efficient Computing and Networking. In Review of IEC/EN Standards for Data Exchange between Smart Meters and Devices, pp 95-103. N. Hatziargyriou, A. Dimeas, T. Tomtsi and A. Weidlich, Eds. Springer Berlin Heidelberg (ISBN 978-3-642-19321-7). 2011
[48] K. De Craemer and G. Deconinck, Analysis of state-of-the-art smart metering communication standards, In Proceedings of the 5th Young Researchers Symposium, Mar. 2010

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

[49] ISO-7498-2:1989: Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture

[50] H. Ziegler. FCB and FCV-Bits and addressing. Fachbereich Physik, Universität-GH Paderborn, 33098 Paderborn, Germany. 1997. [Online]. Available: http://www.m-bus.com/files/MUTFCBN5.pdf [Accessed: 11. Feb. 2013]

[51] EN 62056-53:2007: Electricity metering - Data exchange for meter reading, tariff and load control - Part 53: COSEM application layer

[52] EN 62056-61:2007: Electricity metering - Data exchange for meter reading, tariff and load control - Part 61: Object identification system (OBIS)

[53] EN 13575-2:2004: Communication system for meters and remote reading of meters - Part 2: Physical and link layer

[54] L. Zhang, H. Li, Q. Wang and W. Liu. Design of a sensor network based on M-Bus. In Proceedings of International Conference on Fluid Power and Mechatronics (FPM) 2011, pp. 857–860. Aug. 2011 (DOI 10.1109/FPM.2011.6045881)

[55] EN 13575-3:2004: Communication system for meters and remote reading of meters - Part 3: Dedicated application layer

[56] NIST. Data Encryption Standard (DES). FIPS Publication 46-3, Oct. 1999 (withdrawn May 2005)

[57] NIST. DES Modes of Operation. FIPS Publication 81, Dec. 1980

[58] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone. Handbook of Applied Cryptography (Discrete Mathematics and Its Applications). CRC Press. 1996 (ISBN 0-8493-8523-7)

[59] EN 13575-4:2005: Communication system for meters and remote reading of meters - Part 4: Wireless meter readout (Radio meter reading for operation in the 868 MHz to 870 MHz SRD band)

[60] IEEE Std 802.3:2008: IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 3: Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifi-cations - Section One

[61] DARPA. Internet Protocol, DARPA Internet Program Protocol Specification. RFC 791, Sep. 1989

[62] DARPA. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460, Dec. 1998

[63] S. Kent and K. Seo. Security Architecture for the Internet Protocol. RFC 4301, Dec. 2005

[64] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246, Aug. 2008

[65] EN 62056-47:2007: Electricity metering - Data exchange for meter reading, tariff and load control - Part 47: COSEM transport layers for IPv4 networks

[66] EN 62056-46:2002: Electricity metering - Data exchange for meter reading, tariff and load control - Part 46: Data link layer using HDLC protocol

[67] NIST. Advanced Encryption Standard (AES). FIPS 197, Nov. 2001

[68] NIST. Recommendation for Block Cipher Modes of Operation - Methods and Techniques. Special Publication 800-38A, 2001 Edition

[69] EN 60870-5-1:1994: Telecontrol equipment and systems - Part 5: Transmission protocols - Section 5.1 Transmission frame formats

[70] EN 60870-5-2:1994: Telecontrol equipment and systems - Part 5: Transmission protocols - Section 5.2 Link transmission procedure

[71] IEEE Std 802.3:2008: IEEE Standard for Information technology - Telecommunications and informa-tion exchange between systems - Local and metropolitan area networks - Part 3: Carrier sense multiple access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications

[72] FLAG Manufacturers ID. Manufacturers Identification Characters, Issue FA 001, Issue 129. Jan. 2013. [Online]. Available: http://dlms.com/organization/flagmanufacturesids/ [Accessed: 11. Feb. 2013]

[73] Wireless M-Bus Analyser 1.0. Smart metering applications: test and analysis of wireless M-Bus, OMS and NTA8130 radio telegrams or meters, AMBER wireless GmbH, Cologne, Germany. 2010. [Online]. Avail-able: http://amber-wireless.de/415-1-AMB8465-AT.html [Accessed: 22. Feb. 2013]

[74] CrypTool 1.4.3x. Open-source Windows Program for Cryptography and Cryptanalysis. Jul. 2012. [Online]. Available: http://www.cryptool.org/ct1download/SetupCrypTool_1_4_31_beta_05_en.exe [Accessed: 09. Feb. 2013]

[75] A. Bogdanov, D. Khovratovich and C. Rechberger. Biclique cryptanalysis of the full AES. In Advances in Cryptology, ASIACRYPT 2011, Lecture Notes in Computer Science Volume 7073, pp. 344-371. 2011 (DOI 10.1007/978-3-642-25385-0_19)

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

[76] ECRYPT II. Yearly Report on Algorithms and Keysizes (2011-2012), Rev. 1.0. ECRYPT II Network of Excellence(NoE), funded within the Information Societies Technology (IST) Programme of the European Commission's Seventh Framework Programme (FP7). Sep. 2012. [Online]. Avail-able: http://www.ecrypt.eu.org/documents/D.SPA.20.pdf [Accessed: 11. Feb. 2013]

[77] M. Dworkin. Recommendation for BlockCipher Modes of Operation, Methods and Techniques. NIST Special Publication 800-38A, Dec. 2001

[78] S. Vaudenay. Security Flaws Induced by CBC Padding - Applications to SSL, IPSEC, WTLS. Advances in Cryptology - EUROCRYPT'02, pp. 534-546, 2002 (ISBN 3-540-43553-0).

[79] A.K.L. Yau, K.G. Paterson, and C.J. Mitchell. Padding oracle attacks on CBC-Mode encryption with secret and random IVs. In Proceedings of the 12th international conference on Fast Software Encryp-tion, pp. 299-319. 2005 (DOI 10.1007/11502760_20)

[80] J.Rizzo, T. Duong. Practical Padding Oracle Attacks. the 4th USENIX Conference on Offensive Tech-nologies, WOOT 2010, pp. 1-8, USENIX Association, Berkeley. 2010. [Online]. Avail-able: http://www.usenix.org/event/woot10/tech/full_papers/Rizzo.pdf [Accessed: 6. Mar. 2013]

[81] H. Lipmaa, P. Rogaway and D. Wagner. Comments to NIST concerning AES modes of operations: CTR-mode encryption. Sep. 2000

[82] P. Rogaway. Problems with Proposed IP Cryptography. University of California, UC Davis. Apr. 1995. [Online]. Available: http://www.cs.ucdavis.edu/~rogaway/papers/draft-rogaway-ipsec-comments-00.txt [Ac-cessed: 14. Feb. 2013]

[83] A. Joux, G. Martinet and F. Valette. Blockwise-Adaptive Attackers Revisiting the (in)security of some provably secure Encryption Modes: CBC, GEM, IACBC. In Proceedings of Advances in Cryptology - CRYPTO 2002, Lecture Notes in Computer Science 2442. pp. 17-30. 2002 (DOI 10.1007/3-540-45708-9_2)

[84] G.V. Bard. Vulnerability of SSL to Chosen-Plaintext Attack. In International Association for Cryptologic Research (IACR) ePrint Archive 2004. May 2004. [Online]. Available: http://eprint.iacr.org/2004/111.pdf [Accessed: 15. Feb. 2013]

[85] T. Duong, J.Rizzo. Here Come The ? Ninjas. ekoparty Security Conference 2011, Buenos Aires, Argen-tina. Jun. 2011. [Online]. Available: http://blog.tempest.com.br/static/attachments/marco-carnut/driblando-ataque-beast-com-pasme-rc4/ssl_jun21.pdf [Accessed: 14. Feb. 2013]

[86] D.A. McGrew. Counter mode security: Analysis and Recommendations. Cisco Systems. Nov. 2002

[87] NIST. Recommendation for Key Management, Part 1: General. Special Publication 800-57, Vol. 3 , Jul. 2012

[88] P. Deng and Y. Liuqing. A secure and privacy-preserving communication scheme for Advanced Me-tering Infrastructure. In Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES, pp. 1-5. 2012 (DOI 10.1109/ISGT.2012.6175681)

[89] H. Li, S. Gong, L. Lai, Z. Han, R.Q. Qiu, and D. Yang. Efficient and Secure Wireless Communications for Advanced Metering Infrastructure in Smart Grids. In Proceedings of IEEE Transactions on Smart Grid, vol. 3, no. 3, pp. 1540 –1551. Sep. 2012 (DOI 10.1109/TSG.2012.2203156)

[90] ANSI X9.62:2005. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digi-tal Signature Algorithm (ECDSA)

[91] NIST. Digital Signature Standard (DSS). FIPS 186-3, Jun. 2009

[92] D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography. In Proceedings of the twenty-third annual ACM Symposium on Theory of Computing - STOC, New York, NY, USA, pp. 542–552. 1991 (DOI 10.1145/103418.103474)

[93] C.E. Shannon. Communication Theory of Secrecy Systems. In Bell System Technical Journal, Vol. 28-4, pp. 656-715. 1949

[94] E. Barker, William Barker, W. Burr, W. Polk and M. Smid. Recommendation for Key Management – Part 1: General. NIST Special Publication 800-57 Rev. 3, Jul. 2012

[95] E. Barker and A. Roginsky. Recommendation for Cryptographic Key Generation. NIST Special Publi-cation 800-133, Dec. 2012 (DOI 10.6028/NIST.SP.800-133)

[96] J.L. Massey and J.K. Omura. Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission. U.S. Patent 456760028, Jan. 1986

[97] J. Kim, S. Ahn, Y. Kim, K. Lee, and S. Kim. Sensor network-based AMI network security. In Proceed-ings of Transmission and Distribution Conference and Exposition, IEEE PES, pp. 1-5. Apr. 2010 (DOI 10.1109/TDC.2010.5484300)

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

[98] S. Das, Y. Ohba, M. Kanda, D. Famolari, and S.K. Das. A key management framework for AMI networks in smart grid. In Proceedings of IEEE Communications Magazine, vol. 50, no. 8, pp. 30-37. Aug. 2012 (DOI 10.1109/MCOM.2012.6257524)
[99] NIST. Security Requirements for Cryptographic Modules. FIPS Publication 140-2, May 2001
[100] ISO 10181-4:1997. Information technology - Open Systems Interconnection - Security framework for open systems: Non-repudiation framework
[101] R. Rivest. The MD5 Message-Digest Algorithm. RFC 1321, Apr. 1992
[102] NIST. Secure Hash Standard. FIPS 180-1, Apr. 1995
[103] European Commission. Smart Grid Mandate: Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment. Mar. 2011
[104] European Commission. Standardization mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability M/441. Mar. 2009
[105] CEN/CENELEC/ETSI Joint Working Group. Final report Standards for Smart Grids. Jun. 2011
[106] IEEE 1888:2011. IEEE Standard for Ubiquitous Green Community Control Network Protocol
[107] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar and K. Poolla. Smart grid data integrity attacks: characterizations and countermeasures. In Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 232 –237. Oct. 2011 (DOI 10.1109/SmartGridComm.2011.6102324)
[108] A.F. Snyder and M.T. Garrison Stuber. The ANSI C12 protocol suite - updated and now with network capabilities . In Proceedings of Power Systems Conference: Advanced Metering, Protection, Control, Com-munication, and Distributed Resources, PSC 2007, pp. 117-122. Mar. 2007 (DOI 10.1109/PSAMP.2007.4740906)
[109] ANSI C12.18:2006: Protocol Specification for ANSI Type 2 Optical Port
[110] ANSI C12.19:2008: Utility Industry End Device Data Tables
[111] ANSI C12.21:2006: Protocol Specification for Telephone Modem Communication
[112] NIST. FIPS 46-3, Data Encryption Standard. Oct. 1999
[113] ANSI C12.22:2008: Protocol Specification For Interfacing to Data Communication Networks
[114] M. Bellare, P. Rogaway, D. Wagner: The EAX Mode of Operation, Proceedings of the 11th International Workshop on Fast Software Encryption (FSE 2004), Lecture Notes in Computer Science, Vol. 3017, Delhi, India (Feb. 2004), pp. 389-407 (DOI 10.1007/978-3-540-25937-4_25)
[115] A. Moise, E. Beroset, T. Phinney and M. Burns. EAX' Cipher Mode. Computer Security Resource Center (CSRC), NIST. May 2011. [Online]. Avail-able: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/eax-prime/eax-prime-spec.pdf [Accessed: 11. Feb. 2013]
[116] A. Moise and J. Brodkin. ANSI C12.22, IEEE 1703, and MC12.22 Transport Over IP. RFC 6142, Mar. 2011
[117] EN 62056-42:2002: Electricity metering - Data exchange for meter reading, tariff and load control - Part 42: Physical layer services and procedures for connection-oriented asynchronous data exchange
[118] EN 62056-62:2007: Electricity metering - Data exchange for meter reading, tariff and load control - Part 62: Interface classes
[119] S. Keemink and B. Roos. Security analysis of Dutch smart metering systems. University of Amsterdam. 2008
[120] CRC RevEng v1.1.0. An arbitrary-precision CRC calculator and algorithm finder. 09. Feb. 2013. [Online]. Available: https://sourceforge.net/projects/reveng/files/1.1.0/ [Accessed: 27. Feb. 2013]

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

7 Appendix

7.1 Smart Metering Infrastructure

7.1.1 ANSI C12 Series for WAN and Local Communication

The section lists common US ANSI standards and RFCs used for WAN communication. Moreover, the standards listed in table 6 do include the specification for service communication over optical ports. A good overview of the ANSI C12 series is also given in [108]. The author refers to standards from the C12 series that cover accuracy and performance requirements for meters.

Standard	Description
ANSI C12.18 [109]	The *"Protocol Specification for ANSI Type 2 Optical Port "* specifies the communication between the device and a client, a hand-held unit (HHU). It does not mention any confidentiality or integrity controls. Although it proposes some procedure for error detection using a CRC.
ANSI C12.19 [110]	The *"Utility Industry End Device Data Tables "* defines data types and structures as extended markup language (XML) document type descriptors (DTD). These so-called tables could be sent either over optical port (ANSI C12.18), over modem (ANSI C12.21) or could be carried over networks (ANSI C12.22).
ANSI C12.21 [111]	The *"Protocol Specification for Telephone Modem Communication "* defines the client, the device, the lower level protocols as well as electric metering specific protocols. The standard follows the ISO OSI model which is tailored for modem communication in this case. Additionally, it defines the data encryption standard (DES [112]) for confidentiality.
ANSI C12.22 [113]	The *"Protocol Specification For Interfacing to Data Communication Networks "* defines the application layer protocol. This includes services necessary for AMI communication such as logon and logoff. Additionally, it specifies AES in EAX mode [114], [115] to provide confidentiality and integrity of the data. The standard also defines extensions for compatibility with C12.18 and C12.19.
RFC 6142 [116]	The RFC *"ANSI C12.22, IEEE 1703, and MC12.22 Transport Over IP"* describes on how to transport ANSI C12.22 on an IP based network. It specifies port 1153 for both, TCP and UDP related traffic.

Table 6: Common US Protocols for WAN and Local Communication

All of the protocol specifications (C12.18, C12.21 and C12.22) define the same services (e.g. logon, logoff and security). However, only C12.22 foresees state of the art cryptographic algorithms.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

7.1.2 DLMS/COSEM for WAN, NAN and Local Communication

This section gives an overview of the DLMS/COSEM protocol suite. Originally the DLMS specification is grouped into coloured books which made their way into the EN 62056 *"Electricity metering - Data exchange for meter reading, tariff and load control"* standard series. The standard series is following an object oriented approach in order to describe the data objects, methods and the device associations.

The EN 13757 standard series heavily refers to DLMS/COSEM as replacement, as higher-level protocol or for interoperability purposes in mixed environments. Some of the referenced standards are listed and briefly introduced in table 7.

Standard	Description
EN 62056-21 [46]	The "Direct local data exchange" part defines the protocol stack and physical form factors for meter communication with a HHU. Thus, it defines protocols over optical ports, current loop or serial line (RS-232). There are five different protocol modes specified; A to E: **Mode A and B**; allows for data reading and device programming. However, the mode only foresees a password to enter programming mode. **Mode C**; allows for data reading, programming and manufacturer specific modes using "enhanced *security*". For mode C a specific list of access modes is defined. Access Level 1: No Security Access Level 2: Require Password(s) Access Level 3.1: Push sealed button Access Level 3.2: Manipulation with secret algorithm Access Level 4: Physical change within device **Mode D**; permits data reading only. Hereby, reading will be initiated by physical action such as triggering a sensor or pushing a button. **Mode E**; provides support for additional protocols.
EN 62056-42 [117]	The *"Physical layer services and procedures for connection-oriented asynchronous data exchange"* introduces the ISO/OSI reduced 3-layer model and defines the services and protocol data units on the physical layer (PHPDU). These PHPDUs are being exchanged between COSEM enabled servers and client devices.
EN 62056-46 [66]	As usual within the ISO/OSI model the *"Data link layer using HDLC protocol"* is split into two logical layers the logical link control (LLC) and the media access control which purpose it is to provide services for connection-oriented and connection-less protocols.
EN 62056-47 [65]	The *"COSEM transport layers for IPv4 networks"* defines the modifications to UDP and TCP. Whereby COSEM needs some extension to UDP and TCP in order to address the correct logical server device or correct logical client process on a physical device. The standard introduces so-called wPorts. The name *"wPorts"* of the 2 byte value is derived from the words wrapper and port. There is no preferred port number for UDP and TCP communication. However, there are three reserved wPorts for special purposes.
EN 62056-53 [51]	The *"COSEM application layer"* defines how applications on the client and server side can make use of the lower stack services and how to address each other in order

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

	to communicate. It follows the traditional client-server model except for the event notification where a server could send traps to its client out of the classic request and response concept. This is used to indicate issues such as counter overflows or fraud detection. Authentication is defined as levels depending on the entities being authenticated: Lowest level: no authentication Low level security (LLS): client authentication High level security (HLS): mutual authentication custom functions or on the specified functions for which. The functions are specified within the "Interface classes" [118]
EN 62056-61 [52]	The "Object identification system (OBIS) " part of the DLMS/COSEM standard series specifies the addressing of all data elements held in a meter. The IDs used to address the data allows identification of metering values as well as of configuration properties and application parameters of the metering device. For example, the standard describes how to address the security switches to read the current status.
EN 62056-62 [118]	The COSEM *"Interface classes"* are specified in an object oriented manner. Thus, interfaces have attributes and methods that allow for value setting and operations with instances of objects. Since standard revision 2002 the high level security (HLS) mechanisms have been added. Access to COSEM objects could be restricted depending on the client and association. Clients could extract accessible objects and read the permission (read, write) of each object using an internal list. The proposed authentication scheme differs depending on the lower layers security. In case of *"the communication channel offers adequate security to avoid eavesdropping and message (password) replay "* the standard only requires the client to provide a secret in order to get authenticated. In case of the channel cannot provide adequate security a 4-way challenge-response mechanism is specified for authentication. The naming "LLS authentication" and "HLS authentication" is a bit confusing in this context as it does not refer to the strength or number of factors of the authentication but on the ISO/OSI stack layers as levels.

Table 7: Common European Standard for Communication (DLMS/COSEM)

The local data exchange part 21 [46] of the specification introduces some level of access control for local device reading and maintenance. For example, it specifies level 2 and level 3.2 methods which require some form of a secret to be known by the HHU. Additionally, section 6.5 of the standard defines the value portion of the data set to be used for the password as *"32 printable characters maximum with the exception of (,), *, / and ! "* respectively as 128 characters for mode C conversations. The 32 printable characters would provide enough space for adequate algorithms.

Unfortunately, registers are specified for a maximum storage of eight characters for passwords (section C.4.7.2) whereby password policies and key management are not part of the specification. Moreover, the standard does not specify or propose and adequate "secret algorithm" for level 3.1 but leaves the choice of the algorithm entirely to the manufacturer. In any case, an adversary with physical access to the wiring of a current loop setup with multiple slaves could launch significant attacks. Thereby, an adversary could tap into the communication, replay passwords or mount man-in-the-middle attack and masquerade as valid HHU for

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Level 2 and Level 3.2 protected devices. These attacks would not involve any physical manipulation of the slave device apart of rewiring work.

A set of theoretical and practical attacks on the optical port of real-world implementations is given in a security analysis of the Dutch smart metering system [119].

7.2 Lab Setup and Protocol Analysis

7.2.1 Meter Manufacturer List

The lab environment did include wired and wireless devices of the following manufacturers. For a full list manufacturer shorts consult the DLMS website [72].

Short	Hex	Company
AMB	A205	Amber wireless GmbH, Hawstrasse 2a, 54290 Trier, Germany
AMT	B405	Aquametro, Ringstrasse 75, 4106 Therwil, Switzerland
DME	A511	DIEHL Metering, Industriestrasse 13, 91522 Ansbach, Germany
ELS	9315	Elster GmbH, 55252 Mainz-Kastell, Germany
EMH	A815	EMH metering GmbH & Co. KG, Neu-Galliner Weg 1, 19258 Gallin, Germany
ESY	7916	EasyMeter GmbH, Piderits Bleiche 9, 33689 Bielefeld, Germany
GWF	E61E	GWF MessSysteme AG, Obergrundstrasse 119, 6002 Luzern, Switzerland
HYD	2423	Hydrometer GmbH (Diehl Metering), Industriestrasse 13, 91522 Ansbach, Germany
ITR	9226	Itron Inc., 2111 North Molter Road, Liberty Lake, WA 99019-9469, USA
KAM	2D2C	Kamstrup Energi A/S, Industrivej 28, 8660 Skanderborg, Denmark
SGM	ED4C	Swiss Gas Metering AG, Reichenauerstrasse, 7013 Domat/Ems, Switzerland
SON	EE4D	Sontex SA, Rue de la Gare 27, 2605 Sonceboz, Switzerland
TCH	6850	Techem Service AG & Co. KG, Hauptstraße 89, 65760 Eschborn, Germany
WZG	475F	Neumann & Co. Wasserzähler Glaubitz GmbH, Industriestraße A7, 01612 Glaubitz, Germany

Table 8: List of Manufacturers of involved Test Devices

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

7.2.2 Wireless Device List

Within the lab environment and its surroundings the devices listed in table 9 were in receiving range. Some of the devices were actually productive devices installed with the company that provide the lab space. Productive devices have not been subject to any active attacks.

Manuf. Short	Manuf. Hex	Address	Version	Type	Type Description
DME	A511	19810542	30	03	Gas
ELS	9315	77353503	00	02	Electricity
EMH	A815	32957202	01	02	Electricity
EMH	A815	34957202	01	02	Electricity
EMH	A815	35957202	01	02	Electricity
EMH	A815	73957202	01	02	Electricity
ESY	7916	37053512	05	02	Electricity
GWF	E61E	BF070520	15	00	Other
HYD	2423	03024010	64	0E	Bus/System component
HYD	2423	34019011	63	0E	Bus/System component
HYD	2423	76034010	64	0E	Bus/System component
HYD	2423	85043001	63	0E	Bus/System component
HYD	2423	91043001	63	0E	Bus/System component
ITR	9226	92030011	1E	03	Gas
KAM	2D2C	07719415	01	02	Electricity
SGM	ED4C	86050000	01	03	Gas
TCH	6850	32992223	69	80	Reserved

Table 9: List of wM-Bus Devices in Laboratory Environment Range

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

7.2.3 M-Bus Encryption Mode Five Example

The following example provides the step-by-step decryption of an M-Bus encryption mode 5 encrypted block using CrypTool [74]. The values correspond to Annex P "Telegram examples for the M-Bus and the wireless M-Bus" of the draft DAL specification [7].

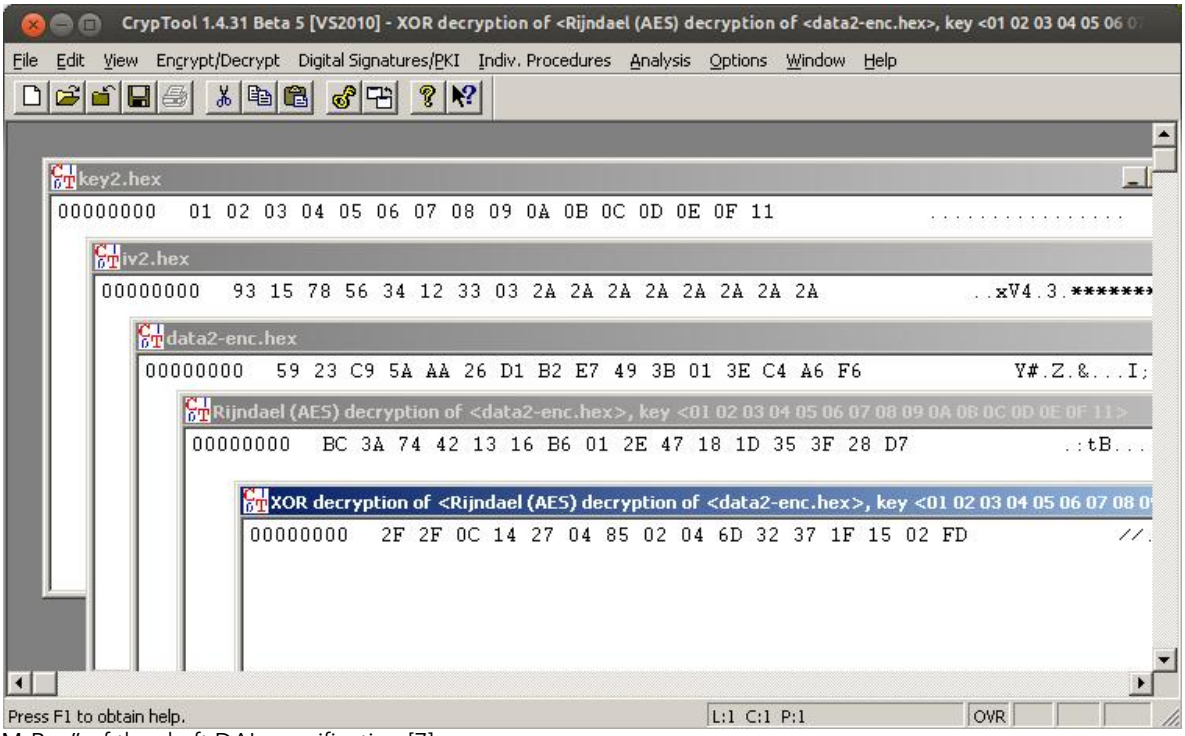


Figure 39: M-Bus Encryption Mode Five, Decryption Example using CrypTool [74]

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

7.2.4 Consumption Data Transmission Intervals and Frame Size

The devices in the lab are configured for high transmission rates. Table 5 provides an example of the transmitted packets of a randomly chosen meter device. The listed records have been captured in a three minutes time span. Each record provides evidence on the meter address, the timestamp when the record was captured and the signal strength of the received frame.

RSSI	Timestamp	L	C	MANUF.		ADDRESS				T	V
-43	06.02.2013 13:39:39:519	00	44	00	11	19	81	05	42	30	03
-43	06.02.2013 13:39:50:315	00	44	00	11	19	81	05	42	30	03
-44	06.02.2013 13:40:01:270	00	44	00	11	19	81	05	42	30	03
-44	06.02.2013 13:40:11:465	00	44	00	11	19	81	05	42	30	03
-44	06.02.2013 13:40:21:149	00	44	00	11	19	81	05	42	30	03
-47	06.02.2013 13:40:30:913	00	44	00	11	19	81	05	42	30	03
-45	06.02.2013 13:40:41:708	00	44	00	11	19	81	05	42	30	03
-46	06.02.2013 13:40:51:452	00	44	00	11	19	81	05	42	30	03
-45	06.02.2013 13:41:02:068	00	44	00	11	19	81	05	42	30	03
-45	06.02.2013 13:41:12:863	00	44	00	11	19	81	05	42	30	03
-45	06.02.2013 13:41:23:809	00	44	00	11	19	81	05	42	30	03
-47	06.02.2013 13:41:34:024	00	44	00	11	19	81	05	42	30	03
-45	06.02.2013 13:41:43:708	00	44	00	11	19	81	05	42	30	03
-45	06.02.2013 13:41:53:462	00	44	00	11	19	81	05	42	30	03

Table 10: Consumption Data Transmission Rate of a Randomly Chosen Meter

Thus, for that specific device, values are being sent every ten seconds in average. The deviation is approximately +/- a single second.

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

7.2.5 CRC Computation using RevEng

```
cbrunsch@tortuga: ~/Documents/rhul/thesis/software/reveng-1.1.0
$ ./reveng -h
CRC RevEng, an arbitrary-precision CRC calculator and algorithm finder
Usage:  ./reveng        -cdDesvhu? [-bBfFlLMrStVXy]
                [-a BITS] [-A OBITS] [-i INIT] [-k KPOLY] [-m MODEL]
                [-p POLY] [-P RPOLY] [-q QPOLY] [-w WIDTH] [-x XOROUT]
                [STRING...]
Options:
        -a BITS         bits per character (1 to 64)
        -A OBITS        bits per output character (1 to 64)
        -i INIT         initial register value
        -k KPOLY        generator in Koopman notation (implies WIDTH)
        -m MODEL        preset CRC algorithm
        -p POLY         generator or search range start polynomial
        -P RPOLY        reversed generator polynomial
        -q QPOLY        search range end polynomial
        -w WIDTH        register size, in bits
        -x XOROUT       final register XOR value
Modifier switches:
        -b big-endian CRC               -B big-endian CRC output
        -f read files named in STRINGs  -F find presets less quickly
        -l little-endian CRC            -L little-endian CRC output
        -M non-augmenting algorithm     -r right-justified output
        -S print spaces between chars   -t left-justified output
        -V reverse algorithm only       -X print uppercase hex
        -y low bytes first in files
Mode switches:
        -c calculate CRCs               -d dump algorithm parameters
        -D list preset algorithms       -e echo (and reformat) input
        -s search for algorithm         -v calculate reversed CRCs
        -h | -u | -? show this help

Copyright (C) 2010, 2011, 2012, 2013  Gregory Cook
This is free software; see the source for copying conditions.  There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
Version 1.1.0                           <http://reveng.sourceforge.net/>
$
$ ./reveng -D | grep 13757
width=16  poly=0x3d65  init=0x0000  refin=false  refout=false  xorout=0xffff  check
=0xc2b7  name="CRC-16/EN-13757"
$
$ ./reveng -m CRC-16/EN-13757 -c 01FD1F01
cc22
$ ./reveng -m CRC-16/EN-13757 -c 01FD1F00
f147
$
```

Figure 40: CRC Computation using RevEng v1.1.0 [120]

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch