Device monitoring and device management for smart meters

Kaushik Bettagere
Student ID : 448831

St Catherine's College
University of Oxford



A dissertation submitted in partial fulfilment of the requirements for the degree of MSc in Software Engineering
16th November 2012

Abstract

The utility industries across the world are trying to address challenges such as energy conservation, greenhouse gas emission, demand response management, diversified energy generation and so on. The next generation grid referred to as "Smart Grid" and "Smart Metering" are expected to provide solution to majority of these challenges. Smart metering is simply a culmination of information and communication technologies with traditional utility components – which will deliver intelligent and automated, remote utility meter monitoring and management capabilities [1]. The two main components of Smart metering are, the smart meters and the communications network which will provide the two way communication capability between the utility suppliers and the consumers (Smart meters).

The key aspect of smart metering network is its ability to manage events generated by end devices namely smart meters. An event is any notable condition that happens in the smart metering environment. These events must be reported to both the communication service provider and the utility supplier. An event in general could be a fault in the system such as a device failure or business event such as detection of a threshold condition, over or under voltage detection etc. Both system faults and business related events will occur frequently and it is important that both kinds of events are quickly detected and reported. A fault management system will provide a centralized event monitoring and management capabilities to the network service provider. Like any other larger scale communications network, a smart meter network will also be built with multi vendor devices and technology. Therefore it is essential to build an event monitoring system that is scalable and can support diverse network equipment. The objective of this dissertation is to propose a fault monitoring system model for smart meters.

Acknowledgements & Declaration

I would like to thank my supervisor Dr. Niki Trigoni for her guidance and support throughout the duration of this dissertation. In addition I would like to extend my appreciation to my wife Bhavana and to our 1year old boy for their co-operation. And lastly I would like to thank my parents for their extended support and encouragement throughout the duration of the dissertation.

The author confirms that this dissertation has not been previously submitted for another degree or academic award. The work presented here is author's own, except where otherwise stated.

Abbreviations

6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
ADSL	Asymmetric Digital Subscriber Line
ANSI	American National Standards Institute
CENELEC	Comité Européen de Normalisation Électrotechnique - European Committee for Electrotechnical Standardization - responsible for European standardization in the area of electrical engineering
CMIP	Common Management Information Protocol
CORBA	Common Object Request Broker Architecture
COSEM	Companion Specification for Energy Metering
COSEM IC	COSEM Interface Class
DCC	Data Communications Co
DCF	Data Communication Function
DECC	Department of Energy and Climate Change
DHCP	Dynamic Host Configuration Protocol
DLMS	Device Language Message Specification
DLMS UA	DLMS User association
DRLC	Demand Response and Load Control
EML	Element Management Layer
ERDF	Electricite Reseau Distribution France
ETSI	European Telecommunications Standards Institute
FCAPS	Fault Configuration Accounting Provisioning Security
FCC	Federal Communications Commission - independent agency of the United States government
GD	Gateway Device
GDMO	Guideline for Definition of Managed Object
GPRS	General packet radio service
GSM	Global System for Mobile Communications
HTTP	Hypertext Transfer Protocol
IC	Integrated Circuit
IEC	International Electrotechnical Commission, an international standards organisation dealing with electrical, electronic and related technologies
IEEE	Institute of Electrical and Electronics Engineers
IHD	In house display
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ITU	International Telecommunication Union
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector
LLA	Logical Layered Architecture
MAC	Media Access Control
M-BUS	Metering Bus
MF	Mediation Function

MIB	Management Information Base
NE	Network Element
NEF	Network Element Function
NML	Network Management Layer
NMS	Network Management System
OBIS	Object Identification System
OFDM	Orthogonal frequency division multiplexing
Ofgem	Office of Gas and Electricity Markets
OSF	Operations Systems Function
OSGP	Open Smart Grid Protocol
OSI	Open Systems Interconnection
OTA	Over The Air
PAN	Personal Area Network
PHY	Physical Layer
PLC	Power Line Communication
PRIME	Powerline Intelligent Metering Evolution
QoS	Quality of Service
REST	Representational State Transfer
RF	Radio Frequency
RFC	Requirement for Change
SAP	Service Access Point
SCE	Southern California Edison
SM	Smart Meter
SM-HAN	Smart Metering Home Area Network
SML	Service Management Layer
SMS	Smart Metering System
SNMP	Simple Network Management Protocol
SSCS	Service Specific Convergence Sublayer
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TMN	Telecommunication Management Network
UDP	User Datagram Protocol
UK	United Kingdom
URI	Universal Resource Identifier
WAN	Wide area network
WSF	Workstation Function
xDLMS	Extended Device Language Message Specification
XML	Extensible Markup Language
ZCL	ZigBee Cluster Library
ZigBee SE	ZigBee Smart Energy
ZigBee SEP	ZigBee Smart Energy Profile

Contents

1. INTRODUCTION....8
1.1. EVENT DRIVEN ARCHITECTURE....8
1.2. UK SMART METERING....8
1.3. SMART METERING INFRASTRUCTURE....9
1.4. EXISTING COMMUNICATION STANDARDS....10
1.5. FAULT MANAGEMENT....11
1.6. OBJECTIVES AND OVERVIEW OF THE DISSERTATION....11
1.6.1. Objectives of the dissertation....12
1.6.2. Structure of the document....12
2. SMART METERING INFRASTRUCTURE....13
2.1. SMART METERS....13
2.2. SMART METERING SYSTEM (SMS)....14
2.2.1. UK Smart meter deployment....14
2.3. SMART METER VARIATIONS....15
2.4. CANDIDATE TECHNOLOGIES FOR SMART METERS....15
2.5. WIRELESS TECHNOLOGIES....16
2.5.1. ZigBee....16
2.6. WIRED TECHNOLOGIES....17
2.6.1. PRIME PLC....17
2.6.2. G3 PLC....18
2.6.3. LonWorks/LonTalk/OSGP (Open Smart Grid Protocol)....19
2.6.4. KNX smart metering specification....19
2.6.5. M-BUS....20
2.7. APPLICATION LAYER PROTOCOLS....21
2.7.1. DLMS/COSEM....21
2.8. CONCLUSION....21
3. FAULT MANAGEMENT ARCHITECTURE....23
3.1. COMPONENTS OF SMART METERING INFRASTRUCTURE....24
3.1.1. Smart meters (end devices)....24
3.1.2. SM-HAN Gateway Device (GD)....24
3.1.3. Network management system (NMS)....25
3.2. CHARACTERISTICS OF SMART METERING NETWORK....25
3.3. NETWORK MANAGEMENT FRAMEWORK....25
3.3.1. TMN viewpoints....26
3.3.2. TMN functional blocks....26
3.3.2.1. Network Element Function (NEF)....26
3.3.2.2. Operations Systems Function (OSF)....27
3.3.2.3. Data Communication Function (DCF)....27
3.3.2.4. Mediation Function (MF)....27
3.3.2.5. Workstation Function (WSF)....27
3.3.3. TMN Logical Layered Architecture (LLA)....27
3.3.3.1. Element Management Layer....28
3.3.3.2. Network Management Layer....28
3.3.3.3. Service Management layer....29
3.3.3.4. Business Management layer....29
3.4. SMART METERING NETWORK MANAGEMENT ARCHITECTURE....30
3.4.1. Use of TMN service management in smart metering....31

3.5. FAULT MANAGEMENT 33
3.6. FAULT MANAGEMENT ACTIVITIES (DEVICE MONITORING AND MANAGEMENT) 34
3.7. FAULT MANAGEMENT - FUNCTIONAL REQUIREMENTS 34
3.7.1. Alarm Surveillance 35
3.7.2. Fault Localization 36
3.7.3. Fault Correction 36
3.7.4. Testing/Diagnostics 37
3.8. SUMMARY 37
4. FAULT MONITORING 38
4.1. DEPENDENCIES 38
4.2. ASSUMPTIONS AND LIMITATIONS 38
4.3. SUMMARY OF REQUIREMENTS FOR FAULT MONITORING 39
4.4. ZIGBEE NETWORK ARCHITECTURE FOR FAULT MANAGEMENT 39
4.4.1. ZigBee smart meters 40
4.4.2. ZigBee-HAN gateway device (GD) 40
4.4.3. ZigBee range extender 40
4.4.4. ZigBee node addressing 40
4.4.5. Endpoints, device discovery, service discovery and binding 40
4.4.6. Binding 40
4.4.7. ZigBee components for fault monitoring 40
4.4.7.1. ZigBee Application Profile 41
4.4.7.2. Devices 41
4.4.7.3. Attributes 41
4.4.7.4. Clusters 41
4.4.7.5. ZigBee Cluster Library (ZCL) 42
4.4.7.6. ZigBee Smart Energy Profile (SEP) 42
4.4.7.7. ZigBee SEP clusters 43
4.4.7.8. ZigBee SEP devices 44
4.4.8. ZigBee event configuration and notification capabilities 45
4.4.8.1. Attribute reporting 45
4.4.8.2. Attribute report configuration 45
4.4.8.3. Alarms cluster and alarm attribute set 47
4.4.8.4. Alarm mask 47
4.4.9. ZigBee event storage and retrieval capabilities 48
4.4.10. ZigBee device testing capabilities 48
4.5. ZIGBEE SUMMARY 48
4.6. DLMS/COSEM 49
4.6.1. COSEM Data Model 49
4.6.2. Logical device and Application Process (AP) 49
4.6.3. COSEM Interface Class (IC) & COSEM interface objects 49
4.6.4. Client/Server model 50
4.6.5. Object Identification System (OBIS) 50
4.6.6. COSEM management logical device 50
4.6.7. COSEM association object 50
4.6.8. Connection oriented service 51
4.6.9. Logical Name (LN) and Short Name (SN) 51
4.6.10. COSEM_on_IP Profile 51
4.6.11. Node addressing 51
4.6.12. DLMS/COSEM device management data collection system 51
4.6.13. Data communication services 52

4.7. DLMS/COSEM SUMMARY 52
4.8. CONCLUSION 53
5. INTEGRATION WITH IP NETWORKS 54
5.1. SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) 54
5.2. REPRESENTATIONAL STATE TRANSFER (REST) 55
5.2.1. Resource Identifier 56
5.2.2. Functions and event handlers 56
5.2.3. Callback handlers 57
5.2.4. Resource manipulation commands 57
5.3. SEQUENCE OF EVENTS 59
5.4. SUMMARY 61
6. CONCLUSION 62
7. REFERENCES 63

List of figures

Figure 1 - Smart metering fixed infrastructure architecture 9
Figure 2 - Smart meter functional components 13
Figure 3 - Smart Metering System 14
Figure 4 - Smart meter deployment scenarios 15
Figure 5 - Zigbee Protocol Stack 16
Figure 6 - PRIME PLC Protocol stack 17
Figure 7 - G3 PLC Protocol Stack 18
Figure 8 - M-BUS Protocol Stack 20
Figure 9 - Smart metering infrastructure components 24
Figure 10 - TMN Logical Layered Architecture 28
Figure 11 - Smart metering component placement on TMN architecture 30
Figure 12- TMN Value added Services 32
Figure 13 - TMN Layered Services 32
Figure 14 - ZigBee Clusters 42
Figure 15 - ZigBee Attribute reporting 46
Figure 16 - Sequence of events for setting up attribute reporting from NMS 60

List of tables

Table 1 - ZigBee General commands 42
Table 2 - ZigBee SEP Clusters 43
Table 3 - ZigBee Smart Meter Clusters 44
Table 4 - ZigBee Gateway Device Clusters 44
Table 5 - ZigBee Alarm Masks 47

1. Introduction

A smart meter at its heart is an electronic device which has two basic functionalities. First, it measures and records utility consumed or produced as well as other measurable quantities. Secondly it acts as a communications hub connecting utility providers to households. The term Smart meter often refers to an electricity meter, but it can also mean a device measuring natural gas or water consumption. Smart meters will be deployed at the consumer's premises to collect the consumption / generation data (potentially control the consumption as well, for load management). As a communications hub, smart meters may also incorporate additional processing capabilities, memory and communications means for storage and transmission of data. However, the main purpose of a smart meter is to facilitate correct and efficient data transfer and communication between the utility providers and households.

As more and more utility suppliers shift towards smart metering, multiple smart meters might be deployed at the consumer's premises. Due to safety concerns some of these meters might be battery operated, such as gas and water meter. The communication link to these battery operated device may be provided wirelessly by an external communications hub which are mains operated or the communications hub might be included within the electricity meter. These communications hub (electricity meters) could also provide the gateway functionality between the households and utility supplier's communications network. In order to maintain a reliable communication between the utility suppliers and households, it is essential that these devices are properly monitored and managed on the network.

1.1. Event driven architecture

Smart meters are well known for their ability to provide automated meter readings at regular intervals, as well as bi-directional communication and remote operating capabilities. In addition to these features, smart meters also generate hundreds of events, events relating to smart meter status, such as "smart meter malfunction", "Last gasp" (Last gasp is an alert generated by the smart meter just before its battery is fully depleted). Power quality events, such as voltage sag, swell and high/low voltage alarms etc. All of these events generated by smart meters provide a very powerful source of information to improve utilities' and the communication service provider's business processes. It is important all of these events generated by smart meters are quickly detected and reported. To manage these requirements both the utilities and the communications service provider will need systems to identify the right events and provide a centralized system for managing them.

1.2. UK Smart metering

The UK Government is planning to roll out smart meters to every home, business and public sector offices in Great Britain by 2020. It is expected that the rollout of smart meters will play an important role in Britain's transition to a low-carbon economy. To implement this vision, the Government has established a central change programme - the Smart Metering Implementation Programme. The programme is responsible for overseeing the development and implementation of the policy design, including establishing the commercial and regulatory framework to facilitate the rollout. The Group is jointly chaired by the Department of Energy and Climate Change (DECC) and Office of Gas and Electricity Markets (Ofgem). A range of proposals on the policy design for the implementation of electricity and gas smart metering were published in July 2010. The key objectives outlined in this proposal include - open, flexible, secure and mature communication standards for smart meters. The UK

government has also confirmed its commitment to adapt to a central communications model for the delivery of smart metering. Under this approach, the communications between smart meters in domestic consumer's, homes and authorised smart meter data users (utility suppliers) will be co-ordinated by a UK-wide data and communications function called Data Communications Co (DCC), which will be provided by a communications service provider. DECC advocates the use of DCC (Data Communication Co) for WAN connectivity and a home area network called SM-HAN (Smart Metering Home Area Network) for local connectivity.

1.3. Smart metering infrastructure

The proposed network architecture for smart metering is based on a fixed network infrastructure. Fixed network infrastructure consists of permanently installed infrastructure to collect smart meter reading/data, events/alarms generated by smart meters and to transfer these data to the central data and management centre. Smart meters can be located at various geographic locations stretching from congested urban centers to sparsely populated rural areas, inside buildings, offices, homes and in remote areas with limited accessibility. The network will also contain energy constrained devices such as gas and water meters. As illustrated in Figure 1 - Smart metering fixed infrastructure architectureFigure 1, combination of both short and long range communication technologies will be required to establish the end-to-end communication between the utilities and the smart meters. The main components of this network infrastructure are, SM-HAN for local connectivity and the WAN connectivity between households and the utilities central data and management centre. The WAN connectivity can be subdivided into an access network and a backhaul network as shown in the Figure 1 [2].

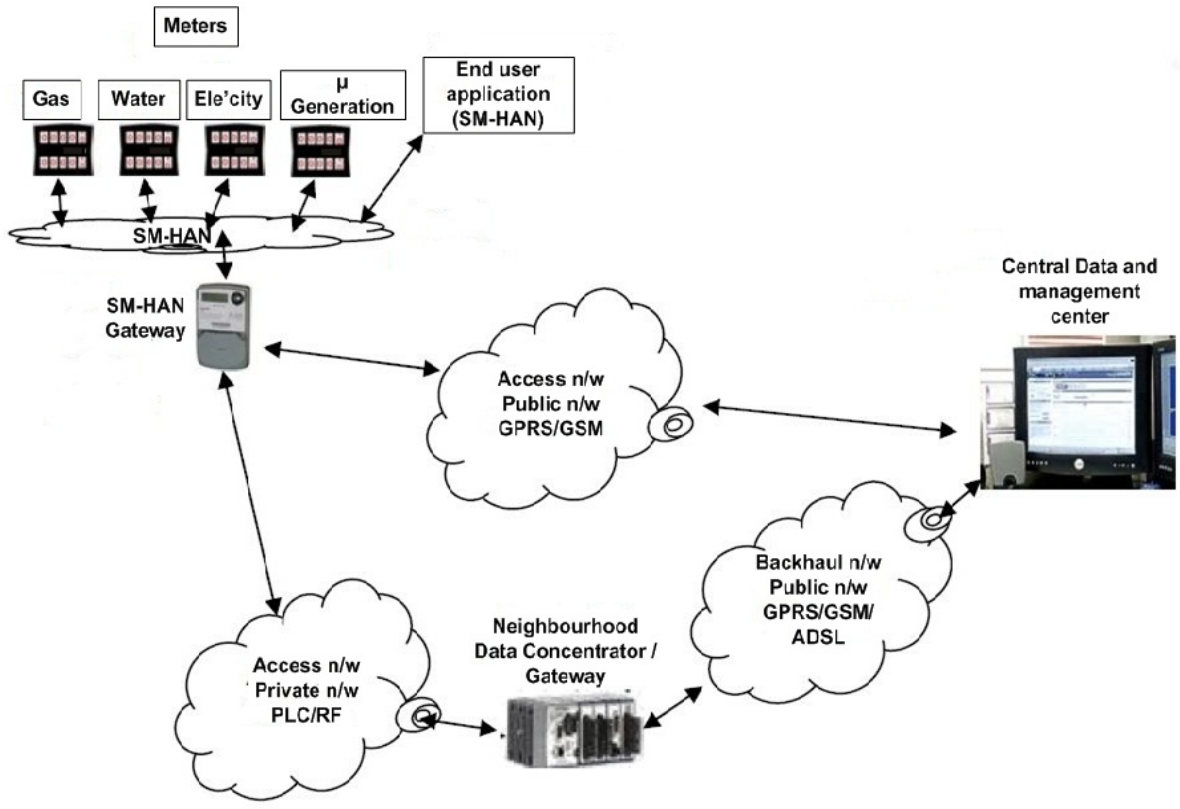


Figure 1 - Smart metering fixed infrastructure architecture

The local network which provides connectivity between the SM-HAN gateway and other devices in the premises could use short range RF communication technologies based on IEEE 802.15.4 example ZigBee or wired technologies such as Power Line Communication (PLC) or Metering Bus (M-BUS). The WAN connectivity between the home gateway and the central data and management center could be provided 100% by a public network for example mobile data networks or it could be provided by a heterogeneous network such as a private network for access and a public network for backhaul, for example PLC for access and GPRS for backhaul connectivity. It is the responsibility of the DCC to integrate, support, manage and monitor these diverse set of resources and technologies on their network and provide reliable data transmission.

Note: The access network comprises the networks between house gateway and a data concentrator or the data management centre in case there is no data concentrator.
The term backhaul network is used to designate the final segment between data concentrator and the data & management centre for utility services and customer-related services

1.4. Existing communication standards

Several utility companies in different parts of the world are deploying smart meters to their customers. Enel Spa Italy's largest utility supplier was the first utility supplier to deploy smart electricity meters to its 30 million customers. It was then followed by Sweden, Denmark, Finland and other European countries. Utility companies in North America are also deploying smart meters to their customers. However majority of these deployments are based on proprietary RF mesh technology for SM-HAN connectivity combined with public communication networks such as GPRS/GSM/Fibre/ADSL for WAN connectivity. Utility companies in Europe however are predominantly using narrow band PLC to connect meters to a neighborhood data concentrator which then connects over the public network back to the utilities data and management center. Most of these deployments only include electricity meters and smart meters for gas and water are only being deployed on a trial basis.

Irrespective of the choice of technologies, all these deployments are adopting a common infrastructure model - devices in a premises or neighborhood are interconnected on a local network and a data concentrator or a gateway device on this network provides the WAN connectivity over a public communications network. The choice of technology for WAN communication namely GPRS/GSM/ADSL/Fibre is not a major concern. These technologies have existed for at least a couple of decades and the standards, flexibility and security of these technologies are not debated. However the choice of communication for local connectivity i.e. SM-HAN is the main concern.

As seen earlier, several smart meter deployments use a proprietary communication technology and these technologies do not conform to open or international standards. In addition to the proprietary data transmission technology, these deployments also use proprietary application layer device management protocols. There are several technologies, both proprietary and open standards, for both data transmission and device management that may be suitable for SM-HAN. However, these are not universally agreed standards. Some of these technologies are currently in use in other smart meter deployments or have gained recognition over the last few years. These technologies include both wired and wireless communication. For example wireless technologies such as ZigBee (an open standard based on IEEE 802.15.4 standards provides a complete protocol stack including application layer protocol for device management) and Zwave (a proprietary wireless solution which also

provides a complete protocol stack with its own device management protocol). Wired technologies such as M-BUS, broadband/narrowband PLC etc have all made it to the smart meter market. As a consequence major equipment manufacturers supply devices which are based on more than one technology, and potentially the smart meter deployment in the UK will also include equipment based on multiple technologies [3][4][5].

1.5. Fault management

Broadly speaking network fault management refers to the activities associated with monitoring and managing the network resources to understand what is going on, and troubleshooting and remedying aspects that could lead to service degradation or even network outages.

Though smart metering is an emerging technology, it can be expected to grow in scale and complexity over the coming years. It is expected that the utility companies could use the smart metering infrastructure not only for automated meter reading but also for load management functions. This infrastructure in future could also be used by other service providers for services such as remote patient monitoring, home surveillance and so on. As seen in the previous sections, the smart metering infrastructure is a resource constrained infrastructure which includes both mains operated and battery operated devices. And these devices could be based on a multitude of technologies and potentially supplied by multiple vendors. Additionally the device vendors may also provide device management applications specifically to manage their devices. In such a diverse infrastructure faults and events will occur frequently. Faults are nothing but notifications generated by the network equipment to notify events such as low battery, transmission errors or failures in the equipment or interface. Business related notifications include events such as leak detection, voltage fluctuation, power outage, intrusion alert etc. It is important that both kinds of events are properly identified and reported. Typically a network fault management system is used for identifying and reporting system faults generated on a communications network. Since the business related events are nothing but events generated by the devices in the smart metering infrastructure, a network fault management system could also be used for managing business events generated on the network. Therefore a fault management system is an essential requirement for not just the network service provider but also for other services dependent on the smart metering infrastructure.

1.6. Objectives and overview of the dissertation

There are several matured and popular fault management applications available in the market which provides a comprehensive set of fault management services for a traditional voice/data communication network. However, these services are built on top of the basic device management capabilities provided by the underlying network resources. For ex: the network resources in a TCP/IP network predominantly uses SNMP for device management. Fault management tools such as HP Openview TeMIP integrates with SNMP for southbound management (Integration of fault management tools with the network devices for managing these devices is referred to as southbound management) and provides various fault management services to its users which are built on top of the SNMP capabilities [41].
As illustrated in Figure 1, the smart metering networks connect over the traditional voice/data communication network for backhaul connectivity. Therefore it may be possible to integrate the existing fault management tools with the smart metering infrastructure to provide a fault

monitoring system for smart meters as well. As discussed earlier, several technologies could be used for smart meter communications and there is no universally agreed technology. Irrespective of the choice of technology used, all these technologies must also provide some device management capabilities. In order to integrate the existing fault management tools with the smart metering infrastructure, it is essential to understand the device management capabilities provided by these smart metering communication technologies.

1.6.1. Objectives of the dissertation

The main objectives of this dissertation are

- To understand the components of a smart metering network and variations.
- To understand the various scenarios that would impact the deployment of smart meters in the UK.
- To provide a survey of candidate smart meter technologies for smart meter deployment in UK.
- To propose a fault monitoring architecture for smart metering infrastructure in the UK.
- Identify and classify events generated by smart meters.
- Identify the requirements of the fault monitoring system for smart meters.
- Review the fault management capabilities of the candidate technologies.
- Propose a model for integrating the candidate technologies with an existing fault management system.

1.6.2. Structure of the document

The reminder of the dissertation is organized as follows

- Chapter 2 provides an overview of smart meters, components of a smart metering system, smart meter variations, and smart metering architecture from a GBs perspective and a survey of the candidate technologies for smart meters.
- Chapter 3 identifies the characteristics of the smart metering network and based on these characteristics a fault management architecture for smart metering infrastructure is proposed. The events generated by smart meters are identified and classified based on the events category. And finally the functional requirements for the proposed fault monitoring system are identified.
- Based on the requirements identified in Chapter 3, Chapter 4 evaluates the fault monitoring capabilities of the candidate smart meter technologies
- Chapter 5 proposes a model for integrating smart metering technologies with traditional fault management system.

2. Smart metering infrastructure

The main components of the smart metering infrastructure are the smart meters, the communication infrastructure and the technology that enables meaningful exchange of data and information between the resources on the network.

2.1. Smart meters

Several sources define a smart meter as one that can communicate in both directions, i.e. the meter can transmit information to the utility providers and the utility providers can also send information to the smart meter. All this occurs without any personnel having to actually visit the meter. The term Smart meter often refers to an electricity meter, but it can also mean a device measuring natural gas or water consumption.

A smart meter at its heart is an electronic device which has two basic functionalities. First, it measures and records utility (electricity, gas, water etc) consumed or produced (micro generation using solar panels or wind), and other measurable quantities (Peak/off-peak usage etc). Secondly it provides the interconnection between the utility company and households. Figure 2 shows a schematic overview of the functional components of a smart meter. The intelligence for the smart meter is incorporated within the meter. Typically a smart meter communicates with the utility providers using an internal or external communications hub. This communications hub could also be used for connecting smart meters to other in house smart appliances such as the in house display for providing current usage information, latest tariff details and so on. They could also be used to connect utilities to smart appliances in the house for load management capabilities. Based on these factors a communications hub not only enables two way communications but also acts as a gateway between the utilities and the households. Several components are required to provide the two way communication capability between the utilities and households. All these components along with the smart meter are grouped together and are referred to as a "Smart Metering System" (SMS).

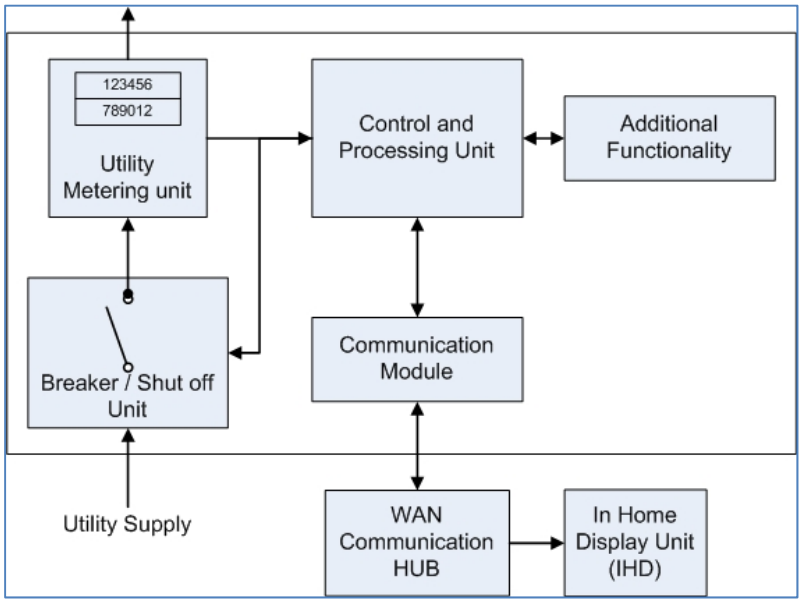


Figure 2 - Smart meter functional components

2.2. Smart Metering System (SMS)

The smart metering system includes the key Smart Metering equipment – the smart meters, the communications hub, In Home Display (IHD) and other control devices. All these devices are interconnected by the Smart Metering Home Area Network (SM-HAN) which is denoted by the blue rectangle shown Figure 3. The baseline smart metering architecture for UK assumes one WAN module per home or premise, which will provide the WAN access to SM-HAN and a single network layer based on IP for WAN connectivity [7] [6]. However, the choice of SM-HAN communication is yet to be determined by the market, subject to compliance with the relevant specifications.

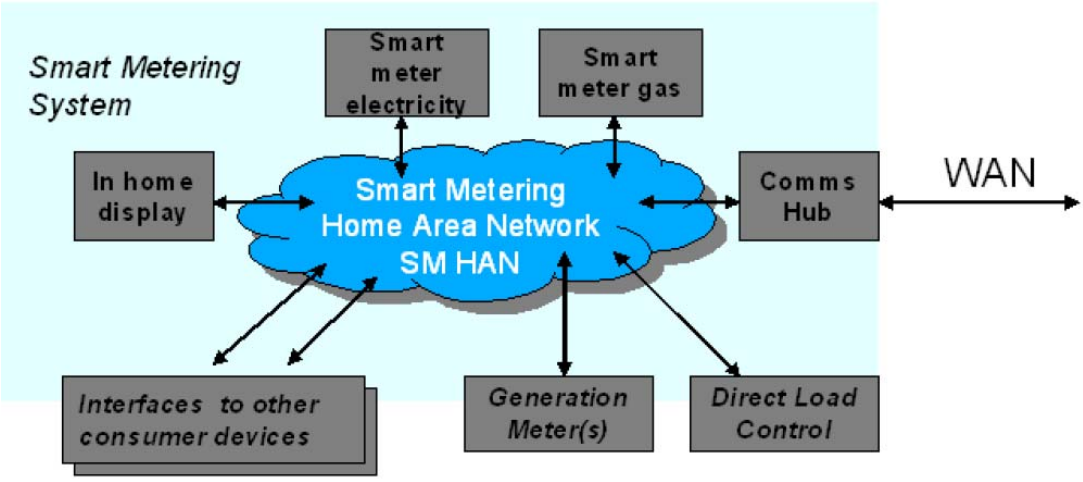


Figure 3 - Smart Metering System

2.2.1. UK Smart meter deployment

The UK government's vision is to roll out smart meters to every home, business and public sector users in Great Britain. It is estimated that nearly 53 million gas and electricity meters, will be deployed to nearly 30 million homes and small businesses in the UK by end of 2019. Various factors could have an impact on the deployment of smart meters.
Factors such as -

- The geographic location of metering points, smart meter deployment logistics, physical, environmental and sociological factors
- Smart meters could be deployed in densely populated urban areas and in sparsely populated rural areas and also in areas with limited accessibility.
- In a multi utility environment, the smart meters for different utilities might be deployed at different stages.

All of these factors will have an impact on the delivery of the smart metering functionality. In order to address these various scenarios, DECC has proposed about half a dozen smart meter deployment architectures [7]. These architectures include scenarios varying from a standard installation of gas and electricity meters wherein all the metering components are installed at a single metering point and scenarios which requires a standalone installation of electric and gas meters. In addition to these scenarios certain special scenarios where the metering components might have to use additional equipment to extend the communication

range of the smart meters (or the communications hub) and scenarios to support micro generation are also addressed. These different scenarios are illustrated in Figure 4 [8].

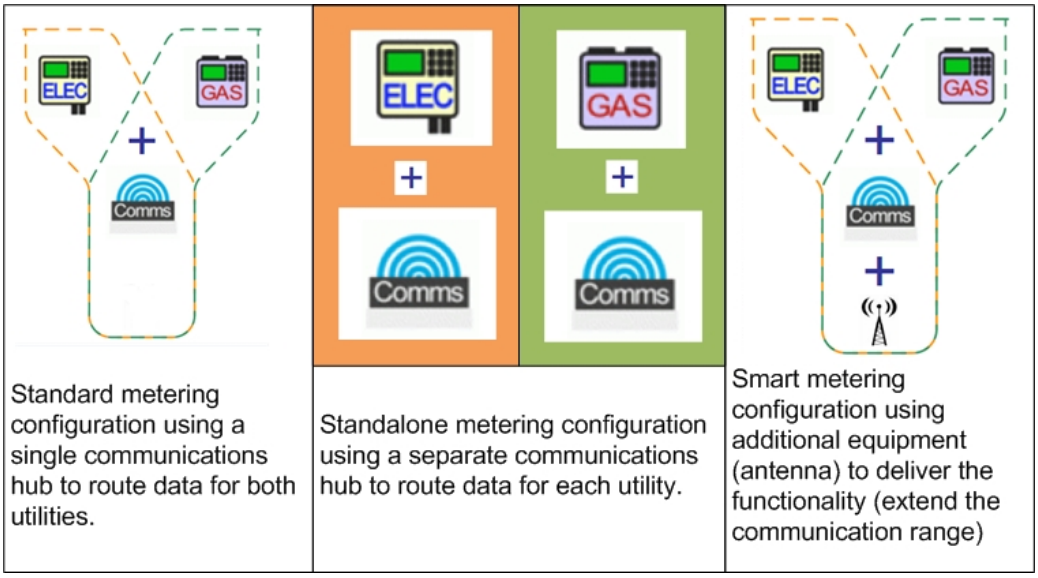


Figure 4 - Smart meter deployment scenarios

2.3. Smart meter variations

'One size fits all' solution may not apply to the smart meter roll out. Based on the different smart metering architecture variations, the smart metering system could be comprised of a number of physical devices (external communications hub, range extenders etc) to deliver the smart metering functionality. Both wired and wireless technologies will be required to address different smart metering scenarios identified. The availability, suitability and maturity of technology will all have an impact on the choice of communication for smart meters. It is neither a good practice nor practical for all the smart meters deployed to be of the same kind and supplied by a single manufacturer. Even with all these constraints, there are still several technologies that may be suitable for SM-HAN. Therefore in reality when these meters are rolled out into production, there is a possibility that different kinds of meters based on different technologies and supplied by multiple manufacturers will coexist. A survey of these technologies is provided in the following section.

2.4. Candidate technologies for smart meters

The choice of communication technology used in smart meters is an important aspect of smart meters. 'Communication technology' does not just mean the physical medium that is used for data transfer it also includes the application layer communication protocols and data exchange format used between devices. The DECC in their proposal have expressed their intention to adopt an existing solution for SM-HAN rather than develop an entirely new one [7]. As seen in previous discussions there are several open and proprietary technologies (both wired and wireless) that are currently available and are being used for SM-HAN communication in different parts of the world. However, DECC has mandated that the technology must be based on open, flexible, secure and matured communication standards. Based on those criteria the following is a survey of some of the candidate technologies for SM-HAN.

Some of these technologies specify the complete communication protocol stack i.e. the physical, MAC, network and the application layers are all included in the specification. Some technologies only specify the physical and the network layers and a separate application layer protocol is used for data exchange between devices. The technologies are mainly classified based on the communication medium used i.e. wireless and wired technologies. An overview of the application layer protocol used by these technologies is provided at the end of the discussion.

2.5. Wireless technologies

2.5.1. ZigBee

ZigBee is a low-power wireless communications technology designed for monitoring and control of devices, and is maintained and published by the ZigBee Alliance. ZigBee works on top of the IEEE 802.15.4 standard, in the unlicensed 2.4 GHz or 915/868 MHz ISM bands. The IEEE 802.15.4 standard defines the physical layer (PHY) and the media access layer (MAC). ZigBee alliance defines a stack profile which includes the network, security and application layers as illustrated in Figure 5. UK government recently announced its support for ZigBee operation in the 2.4 GHz band.

IC makers and equipment manufacturers in the Smart Grid sector namely Landis+Gyr, Computime Limited, Comverge, Energate, Greenbox Technology, Itron, LS Industrial Systems, Co. Ltd., PRI, Tendril and Trilliant etc supply ZigBee compliant equipment. The ZigBee Smart energy profile 1.0 defined in cooperation with the Homeplug Alliance is a public application profile that is used in Smart Grid applications such as metering and home area networks. The Swedish energy company, Gothenburg Energy installed ZigBee-based communications infrastructure for 270,000 homes in Gothenburg and is referred to as the world's first ZigBee city [9].

ZigBee supports star, tree and mesh topologies. A ZigBee network has 3 kinds of nodes namely coordinator, router and end device. A ZigBee gateway device which acts as a network coordinator provides a central configuration and management function to a ZigBee network. Network repeaters provide the range extension and message routing functions. ZigBee devices use ZigBee application profile and ZigBee clusters as the application layer protocol for data exchange and device management [10].

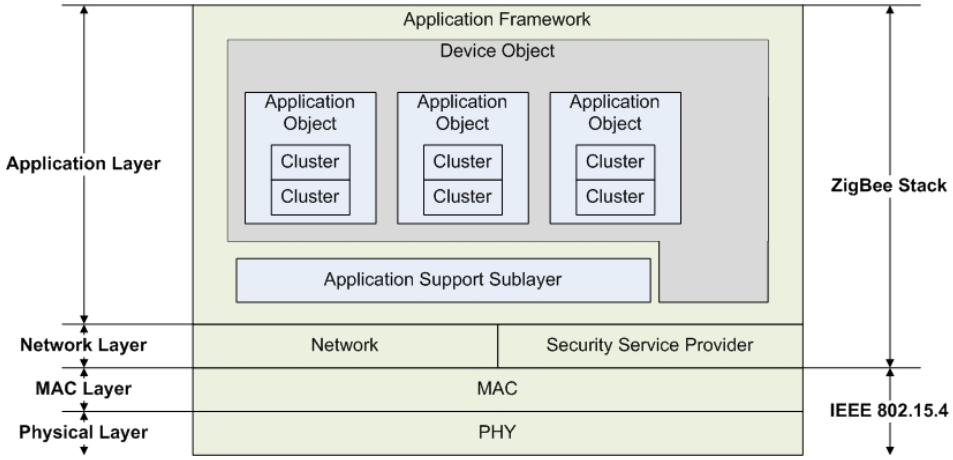


Figure 5 - Zigbee Protocol Stack

2.6. Wired technologies

2.6.1. PRIME PLC

PRIME is an acronym for Powerline Intelligent Metering Evolution for an industry alliance focused on the development of a new open, public and non proprietary powerline telecommunication solution for smart grid. PRIME is a narrow band wired communication technology based on OFDM multiplexing which operates in CENELEC-A band and in FCC band up to 500 kHz in the US. It defines the physical and MAC layer standard and several convergence sub layer on top of the MAC layer including an IPv4 convergence sub layer which allows efficient transfer of TCP/IP traffic over PRIME network as illustrated in Figure 6. However, PRIME does not specify any application layer protocols. DLMS/COSEM on top of IPv4 (COSEM_ip_profile) is used for device management and data transmission between devices in a PRIME network.

IC makers and equipment manufacturers in the Smart Grid sector namely STMicroelectronics, Texas Instruments, ITRON, Landis & Gyr, Iberdrola, Current, ADD, ZIV and GE supply PRIME PLC compliant equipment. Spanish utility Iberdrola is currently deploying PRIME PLC based meters with DLMS/COSEM application layer protocol to link its 18 million customers.

PRIME system is composed of sub networks. A sub network is a tree with two types of nodes, the Base Node and the Service Nodes. A Base node is at the root of the tree and acts as a master node that provides connectivity to the subnetwork. It manages the subnetwork resources and connections. The base node is also the data concentrator for the subnetwork. Any other node of the subnetwork is a Service Node which is responsible for connecting themselves to the sub network and switching the data of their neighbours in order to propagate connectivity. It is also possible to use SNMP over the IPv4 convergence sublayer for device management [11][12][13][14].

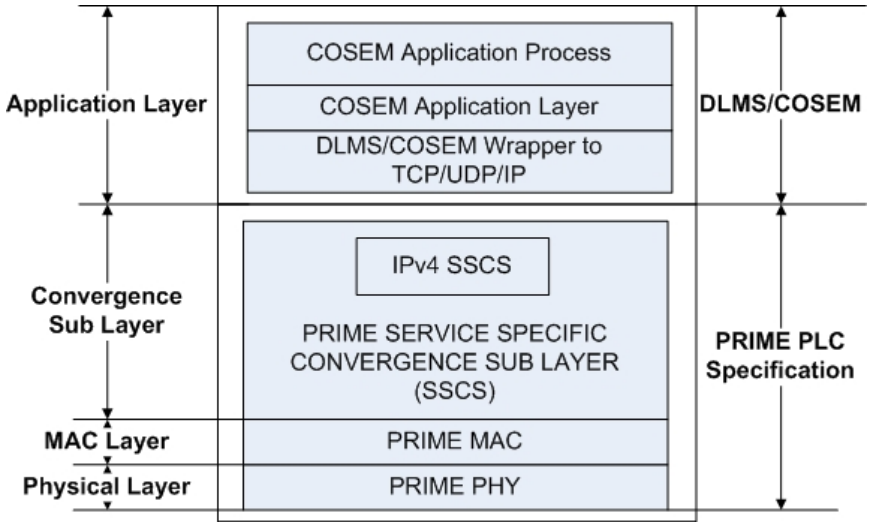


Figure 6 - PRIME PLC Protocol stack

2.6.2. G3 PLC

G3 PLC is a narrow band power line communications specification promoted by maxim and Electricite Reseau Distribution France (ERDF). G3-PLC is a non-proprietary specification conforming to IEEE P1901.2, ITU Ghnem/G.9955, and IEC/CENELEC T13 standards. It is based on OFDM multiplexing in CENELEC-A band, and operates in FCC band up to 500 kHz in the US. PRIME PLC and G3 PLC are non interoperable technologies. The G3 PLC data link layer specification comprises two sublayers the MAC layer based on IEEE 802.15.4 and the 6LoWPAN Adaptation sublayer based on RFC 4944 for transmission of IPv6 packets over 802.15.4 MAC layer. G3 PLC also does not specify any application layer protocols. COSEM_ip_profile is used for device management and data transmission between devices in a G3 network.

Several major IC makers and equipment manufacturers in the Smart Grid sector namely Enexis, ERDF, Maxim Integrated Products, STMicroelectronics, Texas Instruments, Cisco, Itron, Landis & Gyr, Nexans, Sagemcom, and Trialog supply G3 compliant equipment. Currently G3 PLC meters based on COSEM_ip_profile are being deployed in France.

G3 network supports mesh topology and has two kinds of nodes, a network concentrator and a terminal node. G3 supports either a decentralized architecture where the concentrator acts as an application relay or a centralized architecture in which the concentrator simply acts as a network gateway. It is also possible to use SNMP top of IPv6 can be used for device management [14][15].

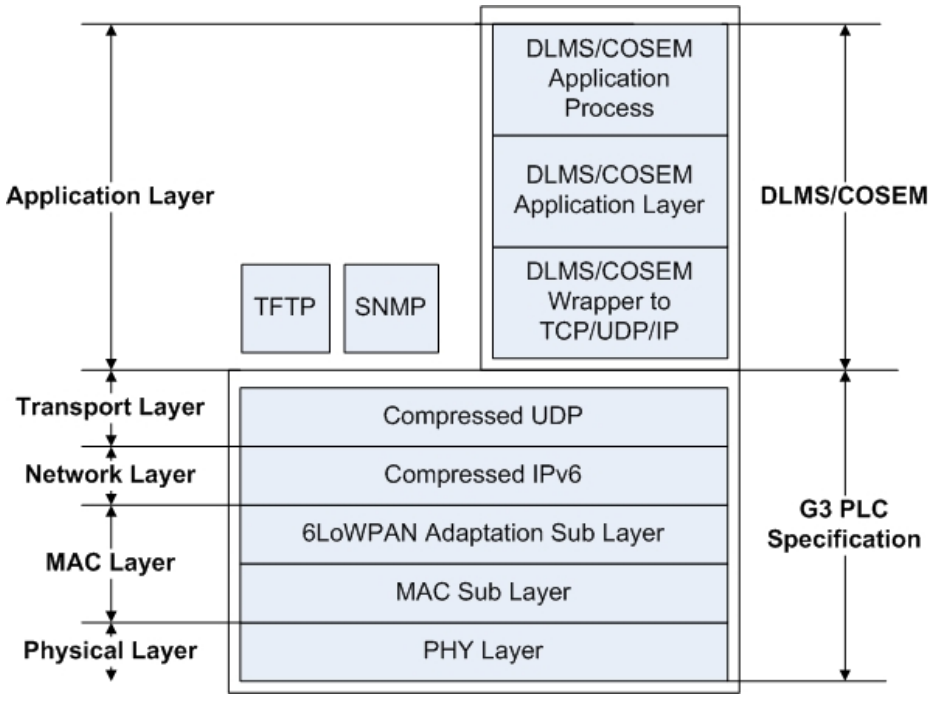


Figure 7 - G3 PLC Protocol Stack

2.6.3. LonWorks/LonTalk/OSGP (Open Smart Grid Protocol)

The heart of the LonWorks technology (Local Operating Network) is the LonTalk protocol, developed by Echelon. Echelon created LonWorks as a whole platform by offering the hardware (Neuron chips), firmware and tools (Neuron ANSI C) as well. The LonTalk protocol a layered, packet-based, peer-to-peer communications protocol designed to be medium-independent but some widely used channels are twisted pair and PLC. Echelon is the main manufacturer of Neuron chips and smart meters based on Lonworks. Enel SpA of Italy has installed Echelon smart meters based on Lonworks to its 30 million customers [16].

LONworks is capable of providing support for a variety of topologies including bus, star, ring, tree or hybrid on a large scale. LONworks devices are intended to work in a peer to peer way on a "flat" network, so each node holds information about the other nodes it is associated with. Creating these associations is known as "binding". The network configuration and management is done by the network management software known as LNS (Lonworks Control Network Software) Network Operating System. The LNS Network operating system includes a LNS sever which installs all devices and it hosts a database which holds all the binding data relating to a LON network, that ensures interoperability of devices, apps, and tools on the LON network. A LNS server can support upto 32,385 devices. Optionally a LNS controller device can be used to provide the controller and gateway functionality for local control with built-in apps for scheduling, alarming, logging, trending, monitoring, and system control. The LNS controller can be integrated with the LNS server [40].

At the end of 2008, ISO and IEC made LonTalk technology into standard ISO/IEC 14908, which now forms the basis for OSGP specification. The OSGP specification also covers all OSI 7 layers. The lower 6 layers are based on ISO/IEC 14908 and the application layer is based on IEEE 1377 standard. OSGP specification was only released in January 2012 only supports narrow band PLC based on CENELEC-A band [17][18].

Note: Although Lonworks is an open standard, the documentation is maintained by Echelon. Echelon provides the documents only for Echelon partners and is not available publically.

2.6.4. KNX smart metering specification

The Konnex (or KNX) Association was setup in 1999 on the merger between three former European associations namely Batibus, EIB and EHS. KNX provides application models for distributed automation, configuration and management schemes, device profiles and a communication system (media and protocol stack). Possible communication media are twisted pair cabling, RF, IP/Ethernet or sometimes PLC, however the KNX smart metering specification uses the KNX RF medium. The KNX RF specification for smart metering is based on the wireless M-Bus standard (EN13757-4) for physical and datalink layer specification. The KNX smart metering specification has specified a KNX Metering M-Bus Data Collector, which allows the collection of metering data from M-Bus meters. The data collector act as the master and can receive, filter and interpret M-Bus Data of up to eight meters, each represented by a KNX Interface Object. The KNX interface object holds static data of the meter, such as manufacturer, identification number, version, medium etc as well as variable data, like operating time, dates and values for minimal and maximal metering data, information on errors etc. The KNX M-Bus Data Collector acts as a server, holding the data of these 8 meters available for any client to read from remotely [19].

Data exchange between KNX and M-Bus devices are possible only at the physical level, however the rules for data exchange at the application level is still in preparation [19].

Note: Although KNX is an open standard, and the documentation is maintained by KNX user group. KNX user group provide the documents only for the participating members and is not available publically

2.6.5. M-BUS

M-Bus (Meter-Bus) is a European standard (EN 13757-2 physical and link layer, EN 13757-3 application layer) for the remote reading of gas or electricity meters, it can also be used for other types of consumption meters. The M-Bus interface is made for communication on two wires, where all nodes on the network are remotely powered by the bus making it very cost effective. A wireless variant of M-Bus (Wireless M-Bus) is also specified in EN 13757-4. Since the M-Bus is not a network, only the physical, the data link, and the application layers are defined as illustrated in Figure 8. An additional Management Layer beside and above the other layers is defined for changing of parameters like baud rate and device address etc.

Wired M-Bus only supports half-duplex asynchronous serial data transmission. Although M-Bus supports bus, ring, star, tree and mesh topologies, only the bus topology is considered reliable and cost-effective networking for consumer utility meters. The M-Bus is a hierarchical system, with communication controlled by a master (Central Allocation Logic). The M-Bus network consists of a master, a number of slaves (smart meters) and a two-wire connecting cable. The application layer transmits data using variable length binary telegrams. The application layer telegram uses a control filed to distinguish between application layer communication and management commands for lower layers. Slave devices use dedicated control fields to report application error and alarms to their master. A master can manage up to 250 end-devices (smart meters). A master also provides the gateway functionality. M-Bus can alternatively be used with DLMS/COSEM. The COSEM Application layer provides the application layer protocol for data exchange and device management.

The Wireless M-BUS standard (EN13757-4) specifies the physical and datalink layers for wireless communication, operating at 868MHz. The wireless M-Bus application layer specification shares the wired M-Bus specification EN 13757-3 i.e. the wireless network also consists of a master and a number of slaves. Like wired M-Bus, wireless M-BUS can also be used with DLMS/COSEM application layer protocol. DLMS/COSEM on M-BUS is the preferred M-BUS technology for smart meters [20].

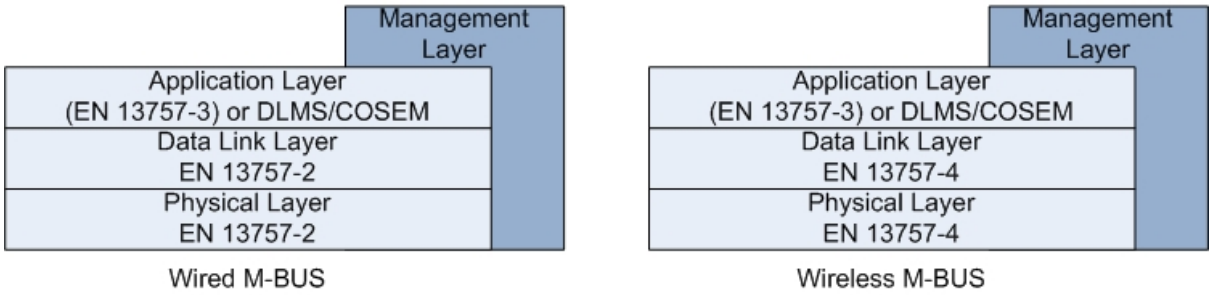


Figure 8 - M-BUS Protocol Stack

2.7. Application layer protocols

2.7.1. DLMS/COSEM

DLMS (integrated in IEC 62056) stands for Device Language Message Specification and is an application layer communication protocol. It specifies general concepts for - modelling a device related services, communication entities and protocols. COSEM is the Companion Specification for Energy Metering. COSEM models metering equipment as a set of logical devices, hosted in a single physical device. Each logical device models a subset of the functionality of the metering equipment as these are seen through its communication interfaces. The various functions are modelled using COSEM interface objects. A COSEM interface object is a collection of attributes and methods. Attributes represent the characteristics of an object. The value of an attribute may affect the behaviour of an object. An object may offer a number of methods to either examine or modify the values of the attributes. Objects that share common characteristics are generalized as COSEM Interface Class. Data exchange between data collection systems and metering equipment using the COSEM interface object model is based on a client/server paradigm. The metering equipment plays the role of the server and the data collection device plays the role of a client. Servers can notify clients about events and unsolicited services are also available. DLMS/COSEM is positioning itself as the all round contender for smart grid communication. It supports several communication standards such as M-Bus, PRIME PLC, G3 PLC etc. Recently a collaborative effort between the ZigBee Alliance and the DLMS UA was announced to define a method to tunnel standard DLMS/COSEM messages with metering data through ZigBee Smart Energy networks. This is yet to be released but when released ZigBee devices could also use DLMS/COSEM for device management and data exchange [21].

2.8. Conclusion

This section provided an overview of the various smart metering communication technologies that are currently available and are being used for smart meter deployments in different parts of the world. Of course there are several other technologies that are available in the market namely Zwave from z-wavealliance a wireless communication technology, Modbus a wired communication technology, PLC technologies namely G.hnen, G.hn etc. These are either proprietary technologies or not widely used for smart meter deployments.

In terms of wireless technologies ZigBee is a leading contender and is well placed in the market with large scale deployments and many device manufacturers and vendors supplying ZigBee compliant devices.

In terms of wired technologies PLC technologies are at the forefront compared to M-BUS and KNX. PRIME PLC, G3 PLC and Lonworks have all been deployed on a large scale (or have been chosen for large scale deployment) and are equally strong contenders competing in the smart metering market. It is hard to tell which PLC technology will lead the market, but it is very likely that all 3 PLC technologies (PRIME PLC, G3 PLC and Lonworks (OSGP)) may co exist.

In terms of the application layer protocol for meter data exchange DLMS/COSEM is a leading standard and many commercial applications are available today. However, since ZigBee devices can only communicate using ZigBee clusters, DLMS/COSEM have not yet entered the ZigBee communication networks. The recent alliance between ZigBee and DLMS

UA to tunnel DLMS/COSEM messages into ZigBee communication network will open up this technology as well for DLMS/COSEM. As a consequence both ZigBee clusters and DLMS/COSEM will coexist.

3. Fault management architecture

Broadly speaking network management refers to the activities associated with running a network, along with the technology required to support those activities. A significant part of running a network is simply monitoring it to understand what is going on, and troubleshooting and remedying aspects that could lead to service degradation or even network outages.

Fault management/monitoring is the component of network management whose main function is to detect report and isolate faults in the network.

A fault management system must take into consideration the following two main aspects of the network to be monitored.

1. A good understanding of the network architecture, topology, devices, connections, services, dependencies and relationships among them. Specifically, an understanding of the aspects that are unique about the network and services that need to be monitored is required, along with an understanding of the aspects that are fairly generic and might be common to other managed technologies.
2. A good understanding of the communication protocols, since the management systems use communication protocols to communicate with the devices they manage and possibly other management applications.

As seen here and in earlier discussions, communication protocols are used by the management systems to communicate with devices they manage. The fault monitoring system is also dependent on these communication protocols for detection, reporting and isolation of faults. Understanding the types of events generated on the network and the functional requirements for the fault monitoring system helps to define the relationship between the fault monitoring system and the underlying communication protocol.

This chapter is mainly concerned with understanding the network architecture, topology, devices, connections, services and the various dependencies and relationships among them.

The reminder of the chapter is organised as follows.

- On overview of the smart metering infrastructure is provided and the characteristics of the smart metering infrastructure are identified.
- A Network management system reference model serves as a conceptual framework for organizing different devices, connections, services, dependencies, relationships, tasks and functions that are part of a network management system. Since fault monitoring is a component of the overall network management system, this framework also helps in organising various tasks and functions required for fault monitoring. Based on the characteristics identified for a smart metering infrastructure, suitable network/fault management architecture is proposed.
- Different types of events generated by smart meters are identified and classified.
- The functional requirements for the fault monitoring system are identified.

3.1. Components of smart metering infrastructure

As seen in earlier discussions majority of the smart metering deployments follow the same network infrastructure model. Figure 9 illustrates the network management hierarchy based on the network infrastructure model illustrated in Figure 1.

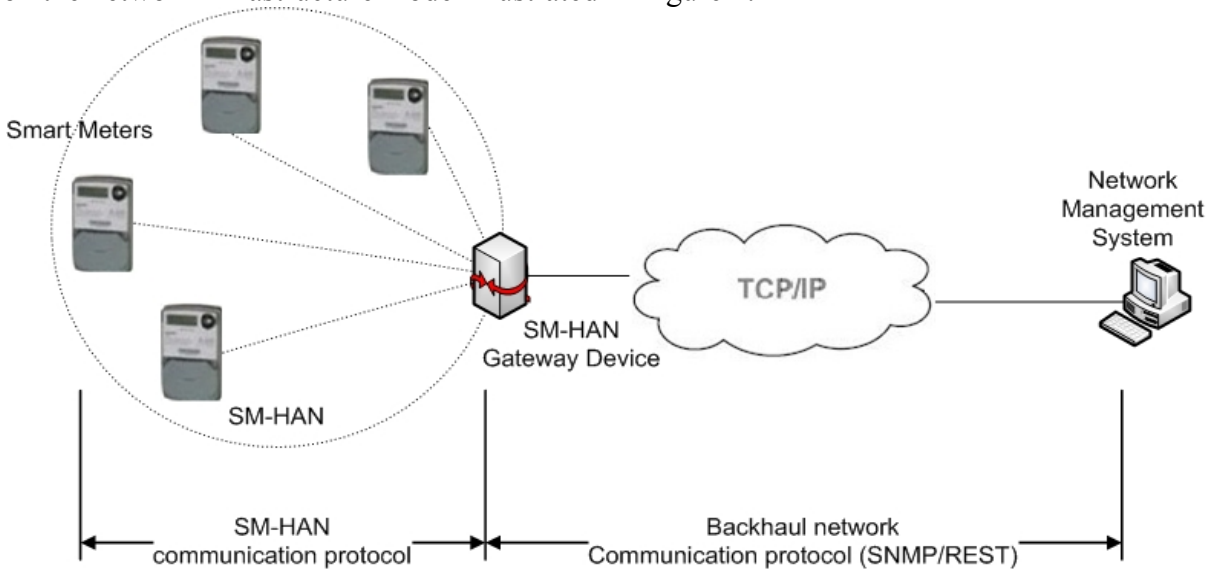


Figure 9 - Smart metering infrastructure components

As illustrated in Figure 9, the main components in the smart metering network architecture are the end devices (smart meters), the gateway (master device or the data concentrator), the network management system and the communication protocol(s).

3.1.1. Smart meters (end devices)

Smart meters are the end devices on SM-HAN whose main functionality is to measure and record energy consumption. These devices also generate and record system related and consumption related events. It also allows this data to be remotely read by and/or periodically reported to the utility company.

3.1.2. SM-HAN Gateway Device (GD)

Every SM-HAN must have a SM-HAN gateway device. The SM-HAN gateway provides an exit/entry point between the NMS and the smart meters on the SM-HAN; a mechanism whereby external applications can interact with individual end devices on SM-HAN to exert control over or to obtain data from those end devices or conversely a mechanism whereby the end devices can communicate some information to the external applications. As illustrated in Figure 9, the end devices (smart meters) connected over a SM-HAN are locally managed by a GD. Typically GDs are capable of managing only those end devices that are based on a common technology. The GD may be housed within a meter or may be a standalone device.

The GD connects the SM-HAN to the communication service provider's backhaul network and routes messages, responses and smart meter data into and out of SM-HAN. Since the smart meter data is routed through the GD, it also acts as a data concentrator. As illustrated in Figure 9, SM-HAN provides an interface between two different networks therefore it also includes protocol conversion functionality.

3.1.3. Network management system (NMS)

A NMS is responsible for managing several smart meters operating in a specific geographic location or a sub network. In a large scale network such as the smart metering network, there may be several NMS's managing smart meters, each responsible for a specific geographic location or a sub network. It is likely that these NMS's interact with each other to provide an overall network management service for the entire network.

However, at the individual NMS level they interact with the GD's for managing the smart meters. They hide the complexity of the multitude of technologies used by various smart meter installations and provide a uniform view of the faults and business events generated by smart meters by formatting these alerts and events into a uniform format. They also provide a uniform interface to the users or other network management services to send commands to the smart meters and present the responses generated in a uniform format, enabling a common management model for managing heterogeneous smart meters in the network.

3.2. Characteristics of smart metering network

As seen here and in earlier discussions, the smart metering network infrastructure is a large scale infrastructure dependent on both existing public networks as well as private dedicated networks belonging different administrative domains. The infrastructure is also dependant on a multitude of technologies and equipment to provide the two way communication capability. All of these factors characterize a smart metering infrastructure as a large scale, distributed and a heterogeneous network. The complexity and heterogeneity characteristics of the communications network for smart meters will be similar to that of other large scale access networks supporting voice / data services. However, stakeholder expectations, QoS requirements and load patterns will be significantly different from those of a typical voice/data network because of the nature of the applications and services supported. Both networks will share, at least partially, problems related to managing and operating a complex and heterogeneous network [22]. Because of these similarities between a large scale voice/data access network and smart meter network, the network management framework for voice/data networks could provide the basis for a fault monitoring system for smart meters.

In order to manage a heterogeneous, complex and a distributed network, the network management system must be generic in nature, scalable and must be able to manage heterogeneous network devices on the network.

3.3. Network management framework

Telecommunication Management Network (TMN) model is a framework defined by the ITU-T (International Telecommunications Union - Telecommunication Standardization Sector) for managing heterogeneous equipment and operations system in a communications network. The TMN model is widely established and is embraced by several other standards bodies for the management of heterogeneous distributed network environments. The use of TMN framework for managing smart grids has also been proposed in the "Smart Grid Reference Architecture" document produced by a team of architects from Southern California Edison (SCE), Cisco Systems, and IBM. [23] [24] [25].

The TMN specification provides a generic network management framework for managing heterogeneous networks by introducing the concept of generic network models. It provides

specifications for performing the general management of diverse equipment, network and services using a generic information model and standard interfaces [26]. The TMN specification also includes but is not limited to, the data communication protocol, information models and data representation specifications.

The TMN framework defines a layered logical architecture which is designed in the same spirit as the layered OSI network model. Each layer above builds on the functions of the layer below and is considered an abstraction of the lower layer [27]. This architecture clearly distinguishes between element, network, service and business management and provides a framework through which the appropriate management services support the telecommunication service provider's business processes. The functional categorizations of the management tasks are based on the OSI Recommendation X.700, which is also known as FCAPS – Fault management, Configuration management, Account management, Performance management and Security management. The TMN framework also allows processing to be distributed to appropriate levels for scalability, performance, and communication efficiency.

3.3.1. TMN viewpoints

TMN describes the telecommunication network management from several viewpoints - The Physical architecture, the information architecture and the functional architecture.

The information architecture provides the principles and guidelines for modelling the network management information using CMIP (Common Management Information Protocol) and GDMO (Guideline for Definition of Managed Object) which provides the template for defining managed resources. As seen in earlier discussions the communication protocols for exchange of management information and modelling used in smart meters are based on the choice of underlying communication technology used.

The physical architecture provides the principles and guidelines for the implementation TMN functionalities at the device level.

Therefore the TMN information architecture and physical architecture are out of scope for this dissertation.

However, the concepts presented in the TMN functional architecture, provides the inspiration for the proposed fault monitoring system for smart meters. The TMN functional architecture is a structural and generic framework for the telecommunication management functionality that describes the TNM principles. The functional architecture identifies the functional modules or blocks in the TMN environment. It also defines the TMN layered logical architecture for structuring the management functionality.

3.3.2. TMN functional blocks

The TMN functional blocks provide an overall embodiment of management functions in deployable units called function blocks. TMN defines the following function blocks for deploying management functionality.

3.3.2.1. Network Element Function (NEF)

The NEF is concerned with the managed network elements. Network elements themselves are not part of the TMN functional architecture specification, but NEF is required for

providing the management information relating to the managed network elements. Network elements would include hardware, software, systems and processes. NEF includes the management agent and the associated information database in the managed network element, for example MIB [25].

3.3.2.2. Operations Systems Function (OSF)

The operations systems function block are implemented in the operations systems. OSF includes functions namely monitor, manage, and control telecommunication networks and services. Network management services, both as a manager and an agent, are also considered operations systems which includes OSF blocks for providing network management services [25].

3.3.2.3. Data Communication Function (DCF)

The communication between the function blocks itself is a function within a function block, but not a function block on its own, defined as the data communication function (DCF). DCF supports the standard transport protocols [25]. Some notable applications that could provide the DCF functionality include SNMP, CORBA etc [25].

3.3.2.4. Mediation Function (MF)

The MF block addresses the operations performed on the information content passing between the network elements and operations systems. Such operations include filtering, store and forward, protocol conversion etc. A physical entity in which the MF is implemented can be shared between multiple operations systems and network elements [25].

3.3.2.5. Workstation Function (WSF)

The WSF provides the means to interpret TMN information for the human user, and vice versa. The responsibility of the WSF is to translate between TMN information to and non-TMN information [25].

3.3.3. TMN Logical Layered Architecture (LLA)

To deal with the complexity of telecommunications management, the management functionality may be considered to be partitioned into logical layers. The Logical Layered Architecture (LLA) is a concept for structuring the management functionality which organizes the functions into groupings called "logical layers" and describes the relationship between layers. A logical layer reflects particular aspects of management arranged by different levels of abstraction [26]. The different layers of abstraction are illustrated in Figure 10. Although these layers are widely accepted, it should not be regarded as the only possible solution. Additional or alternative layers may be used to specialise functionality [26].

- Business Management
- Service Management
- Network Management
- Element Management
- Managed Network Element

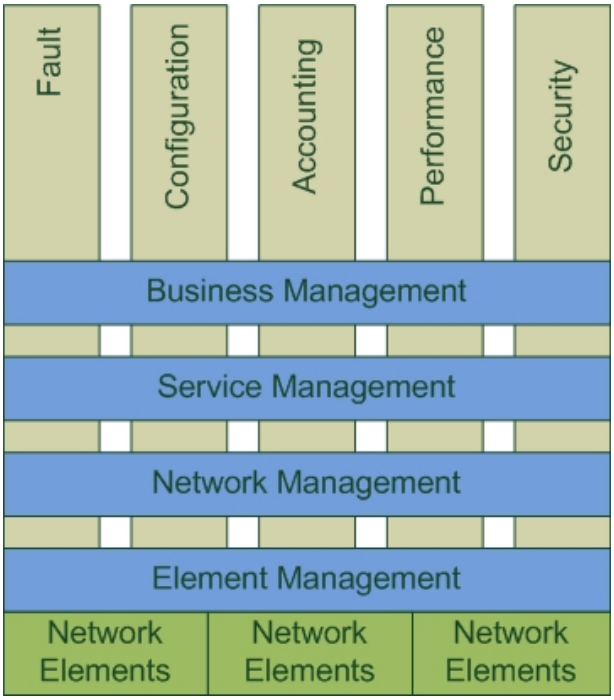


Figure 10 - TMN Logical Layered Architecture

3.3.3.1. Element Management Layer

The functions of individual Network Elements are managed by Operations Systems Functions (OSF) in the Element Management layer. This layer deals with device specific management functions and hides these functions from the layer above, the Network Management layer [28].

Examples of functions performed at the Element Management layer are:

- Detection of equipment errors.
- Measuring power consumption.
- Logging of statistical data.
- Updating firmware.

Note that an OSF in the Element Management Layer and a NEF may be implemented within the same piece of equipment, or in different pieces of equipment. For ex, the SM-HAN gateway may be included within the electricity meter or it might be standalone equipment. In this interaction the end devices act in an agent role and the element manager in a manager's role.

3.3.3.2. Network Management Layer

The traditional fault management systems and tools (HP Openview TeMIP) operate at this level. The responsibility of the Element Management layer is to manage NEFs implemented within single pieces of equipment, whereas the responsibility of the Network Management layer is to manage multiple pieces of equipment. At network management level the internal structure of the network elements is not visible; this implies that alarm filtration capabilities at the smart meter level, buffer space within routers etc cannot be directly managed at this level [28].

Examples of functions performed at this layer are:

- Provide a uniform interface for heterogeneous network equipment,
- Creation of a uniform view of the events and faults generated by different equipment
- Fault detection and propagation to appropriate end users etc

The OSFs at the Network Management layer use device independent management information provided by the OSFs in the Element Management layer. In this interaction the OSFs at the Network Management layer act in a manager role and the OSFs in the Element Management layer in an agent role.

3.3.3.3. Service Management layer

The Service Management layer is concerned with management of those aspects that may directly be observed by the users of the telecommunication network. These users may be end users (customers) but also other service providers (administrations). Service Management builds upon the management information that is provided by the Network Management layer, but does not 'see' the internal structure of the network [28].

Examples of functions performed at the Service Management layer are:

- Network management for the entire network.
- Business event management.
- Accounting.

3.3.3.4. Business Management layer

The Business Management layer is responsible for the management of the whole enterprise. This layer has a broad scope; communications management is just a part of it. Business management can be seen as goal setting, rather than goal achieving. For this reason business Management can better be related to strategical and tactical management, instead of operational management, like the other management layers of TMN [28].

3.4. Smart metering network management architecture

The various components in the smart metering network management hierarchy can be logically partitioned into different TMN layers based on their functionality as illustrated in Figure 11.

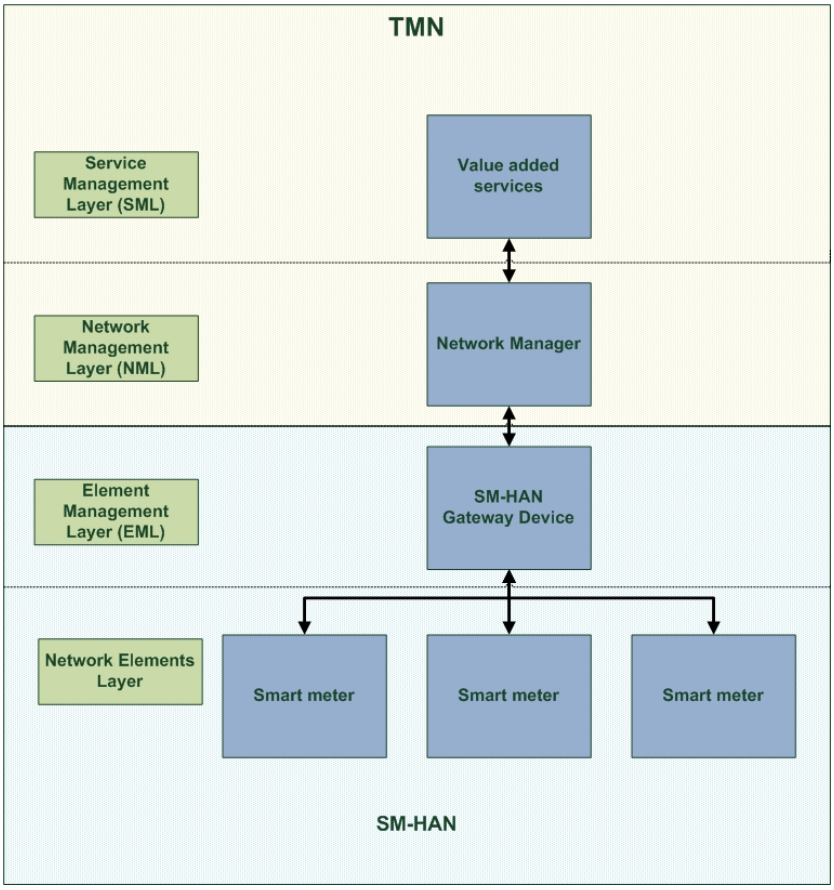


Figure 11 - Smart metering component placement on TMN architecture

Also the various fault monitoring functions required for detection, identification and reporting events in the proposed fault monitoring system can be logically classified into TMN functional blocks as follows.

- NEF - The device firmware, the device management interface provided by the devices i.e. smart meters, routers etc at the network element layer provide the network element functionality (NEF).
- MF - The GD which is responsible for converting the information from one network management protocol to another must include mediation function (MF) blocks for performing the protocol conversion.
- OSF -The relationship between the GD and the network elements, the relationship between the network manager and the element manager, the relationship between the network managers at the network management level are all manager/agent relationship. The manager process issues directives and receives responses, events and alarms, and an agent process carries out directives and sends responses, and emits events and alarms. The network management services provided by both managers and agents must include OSF blocks for these services.

- DCF - As illustrated in Figure 9, events generated by meters are propagated to the network managers via the GD using network management protocols. Network management protocols also provide a mechanism for interaction between various network managers at the network management level. As seen in earlier discussion the choice of network management protocol at the network element layer is dependent on the choice of technology used in smart meters. However, for scalability and uniformity a single network management protocol must be used at the network management level. The network management protocol used provides the Data Communication Functions (DCF) for the fault monitoring system.

3.4.1. Use of TMN service management in smart metering

The notion of TMN Service Management can be regarded as the most valuable contribution of TMN. The proposed fault monitoring system is a good example for the use of service management layer services. The fault monitoring system could provide services which allow the utility suppliers to retrieve, manage events generated by smart meters. Assuming the end devices are managed by the DCC, the utility suppliers need not worry about managing these devices on the network and hence need not receive the device faults generated by the smart meters. Therefore the DCC hides away these details from the utility suppliers only exposing the business events generated by smart meters. Although the DCC might allow certain end device management services such as meter data retrieval from the meters, control or shutoff supply etc.

A second example would be when a consumer switches utility suppliers, the previous utility suppliers' access to the consumers' smart meter must be disabled and access must be provided to the new utility supplier. These are typically value added services offered at the service management layer which is illustrated in Figure 12.

A third example would be as illustrated in Figure 13. DCC provides the end-to-end link between the utilities data and management centre and the various smart metering subnetworks in a specific geographic location. However, the DCC would not allow the utility company to view or modify the configuration of this link, but it provides services which allow the utility company to view or modify the configuration parameters of the smart metering subnetwork or end devices. From the point of view of the utility company these smart metering subnetworks are managed entities on its network. Therefore the utility company utilises the management services offered by the DCC to manage these smart metering subnetworks. Hence the reference point between the element management layer on the utility provider's network, to the service management layer on the DCCs network. In case the utility company has the option to choose alternative links to a specific smart metering subnetwork, there will also be a reference point between the network management level on the utility's network to the service management level on the DCCs network. Finally the DCC transport services might be affecting the suppliers' entire utility network for a specific geographic location. In this case there may be also a reference point at the service management level.

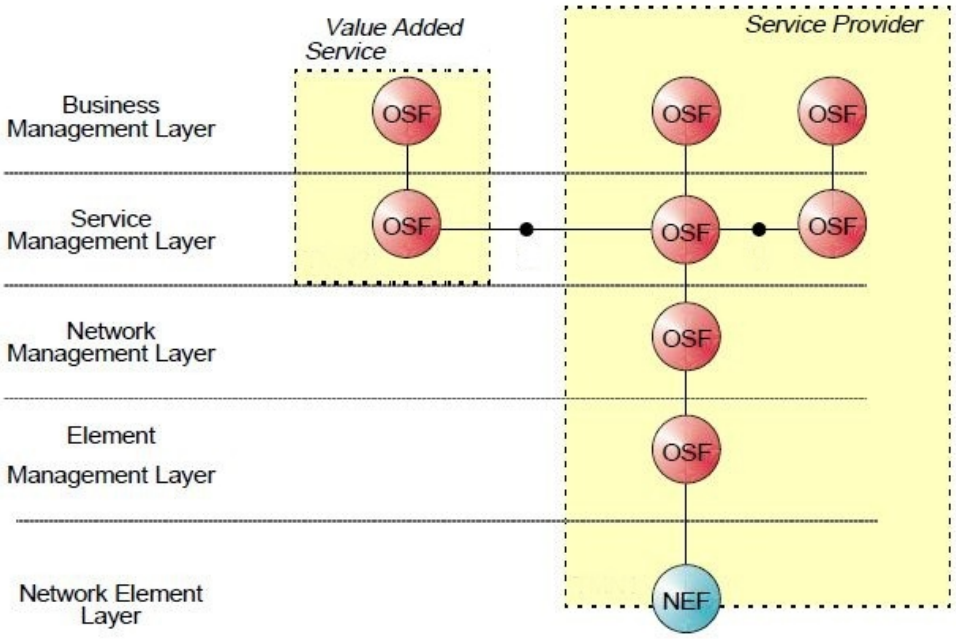


Figure 12- TMN Value added Services

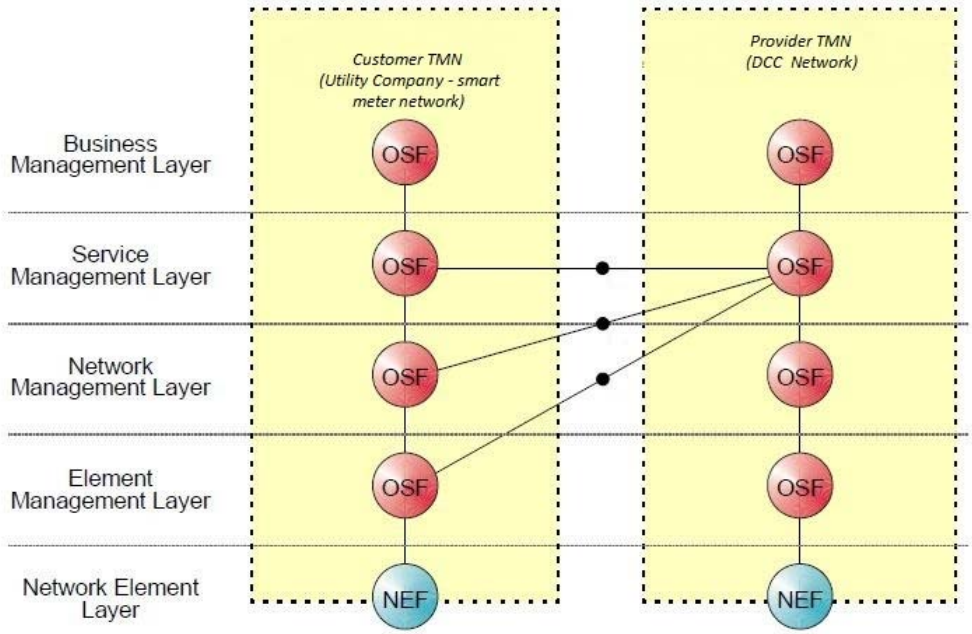


Figure 13 - TMN Layered Services

3.5. Fault management

Next step of the modelling process is to identify and classify the different types of events generated by smart meters and to identify the functional requirements for fault monitoring.

An event is any notification generated by the managed object in a communications network. An error is an event which notifies the deviation of a managed object from its normal behaviour. A fault is the physical or algorithmic cause of a malfunction which manifests itself as an error of the corresponding managed object. An alarm is a notification of a specific event in a communications network.

As discussed earlier, the main functionality of smart meter is to report the utility usage data to the utility supplier at regular intervals and the bi directional communication and remote operating capabilities. In addition to these features smart meters also generate events relating to power quality, leak detection or events related to other potential future services.

These events include several attributes namely source of the event, severity level and the event category. Event category provides the information about the process to which the event is related. Based on the event category, events can be broadly classified as system events and business events.

System related events provide information about a fault in the communication network or the devices on the communications network. These faults must be reported to the network administrators managing the network.

Business events generated could be used to provide enhanced level of customer services which could be a revenue generator for the utility suppliers, the communication service provider and also for other service providers.

System Events include [29]

- Alerts about smart meter not reachable or no communication from a smart meter or meters for more than a specified amount of time (in case of repeater or a parent of sub tree failure).
- Low battery and battery critical alerts for battery operated devices.
- Device last gasp alerts.
- Alerts relating to malfunctions with the smart meter.

Business events include [29]

- Alerts relating to remaining credit on prepayment meters. These alerts must be sent to both the utility supplier and also to the customers IHD.
- Load limiting Alerts for example an event is generated which must be delivered to the utility supplier when the amount of power drawn at a given metering point exceeds a threshold value for more than a specified amount of time.
- Over or under voltage detection alert.
- Supply outage alert.
- Device tamper detection alert.
- Reverse flow alert or leak detection etc.

From here on SM-HAN system faults are referred to as "Faults" and Business related Events as "B-Alert".

3.6. Fault management activities (device monitoring and management)

In general fault Management activities are concerned with detection, isolation and notification of abnormal behaviour i.e. faults encountered in a telecommunication network. In addition to detection of faults, the proposed system should also be able to manage business events generated by smart meters.

The fault management activities are performed by an application or a user (network administrator), using the services of the fault management system. Based on that criterion the following four activities are identified for the proposed system.

- Alarm Surveillance
- Testing
- Fault localization
- Fault correction

Alarm surveillance:
Alarm surveillance is mainly concerned with monitoring, notification and management of system faults generated in the smart metering network. However, the proposed model would also include monitoring, notification and management of business events generated by smart meters.

Testing:
Testing functions provides the tools necessary for running diagnostics on faulty network resources.

Fault Localization:
Fault Localization is concerned with identifying the specific network resource that is responsible for improper behaviour in the network. Fault localization makes use of the testing functions for identification and localization of faulty network resources.

Fault Correction:
Fault correction refers to the activities performed by the fault management system or the network administrator to restore the functions of a faulty network resource

3.7. Fault management - functional requirements

As discussed in Section 3.3.2.1, the TMN model although is device independent, but it is dependent on the NEF (Network element functions) offered by the network resources. This section describes the requirements for fault management services at different levels in the TMN model. However, the main objective is to identify the fault management capabilities offered by the candidate technologies. Therefore the main focus remains at the network element and the element management level.

3.7.1. Alarm Surveillance

Overall requirements for alarm surveillance functions -

- Must monitor the network resources and upon receiving alarms from the managed objects in the network, it should be able to identify faults and B-Alerts generated within the network.
- Must record alarms and B-Alerts which can be used for other activities such as B-event and fault reporting, fault localization and fault correction.
- Must be able to filter the detected events, and report the events to the fault/service management user.

Requirements for alarm surveillance functions at the NE (smart meter) level

- Alarm reporting: Smart meters must provide functions to control and support alarm reporting and related information.
- Alarm summary: Smart meters must provide functions to control and report current alarms summary. Scheduled and on demand reporting must be supported. This may be optional for reduced function devices due to their limited memory and processing capabilities.
- Alarm event criteria: Smart meters must provide functions to manage the criteria used for determining when a certain condition is to be considered an alarm.
- Log control: Managed objects must provide functions for controlling logging and the retrieval of alarm history. This may be optional for reduced function devices.

Requirements for alarm surveillance functions at EML

- Alarm reporting: The element manager must control and support alarm reporting and related information.
- Alarm summary: The element manager should provide functions for controlling and reporting of current alarms summary for a specified resource. Typically scheduled and on demand reporting must be supported.
- Alarm event criteria: The element manager should provide functions the element manager must provide functions which can be used by the network administrator to configure the alarm criteria.
- Log control: The element manager should provide functions for controlling alarm logging and the retrieval of alarm history for a given NE.
- Alarm filtering: The element manager should provide functions for filtering redundant alarm notifications within the scope of an NE or group of NEs. However, this may be an optional requirement since the alarm filtering capability may not be included in all element management systems.

Requirements for alarm surveillance functions at NML

- Network fault event correlation and filtering: The fault management functions must remove redundant alarms and narrow the range of possible root causes by performing alarm correlation and filtering. These functions make use of the network topology information etc to perform these tasks.
- B-event forwarding: B-Alerts generated by the managed objects must be forwarded to service management functions.

Requirements for alarm surveillance functions in SML

- The B-event management functions must handle the B-Alerts i.e. log events and forward B-Alerts to service management users.

3.7.2. Fault Localization

Overall Requirements

- A fault within a network may result in multiple alarms from MOs directly or indirectly related to the fault. The fault management functions must include fault localization capabilities, which determines the root cause of the alarms received.

No requirements identified at the network element (smart meter) level

Requirements for Fault Localization functions at EML

- NE(s) fault localization: Element manager must support scheduling of tests and diagnostics to identify the root cause. If a root cause is found within an NE or group of NEs, that fact must be reported.

Requirements for Fault Localization functions at NML

- Network fault localization: Fault management functions must analyze filtered alarms and perform testing and diagnostics to identify the root cause. Based on these results the function must determine if the fault is affecting any network services. If service has been affected, then the service status information must be updated.

3.7.3. Fault Correction

Overall Requirements

- Fault correction is responsible for the repair of a fault and also for the control of procedures that use redundant resources to replace equipment or facilities that have failed.

Requirements for Fault Correction functions at NE level

- None identified

Requirements for Fault Correction functions at EML

- The fault management function must carry out automatic restoration process within an NE or groups of NEs and must report the outcome of the restoration process (successful or unsuccessful).

Requirements for Fault Correction functions at NML

- Scheduling and dispatch administration of repair force: Fault management functions determine what analysis, testing, or repair activity has to be performed and must assign it to the repair engineers.

3.7.4. Testing/Diagnostics

Testing is an activity or tool in the fault management system to verify the functionality of a managed resource. Diagnostics is an algorithm / procedure applied by the fault management system to analyse the root cause of a fault and to report the findings of its tests.

Overall requirements

- The fault management functions must include capabilities for testing/diagnosing one or more managed objects in the network not only for identifying faults but also for routine management tasks.

Requirements for Testing/Diagnostics at the NE level

- Testing functions: Managed objects must support device testing functions. Device testing functions could include but not limited to connectivity tests. Identify how devices can be tested, if the ne provides any mechanism to test the devices.

Requirements for Testing/Diagnostics functions at EML

- The element manager must manage access to testing capabilities, manage test configuration, and control the performance of tests or test suites, report test results and the status information of tests.

Requirements for Testing/Diagnostics functions at NML

- Connection selection, test correlation and fault location: The diagnostics function must systematically test various connection segments to determine the faulty segment or a faulty component.
- Selection of test suite: The fault management function must support requests from a requestor, to test specific part of the connection or to run appropriate test suite. The results of the requested test must be returned to the requestor.

3.8. Summary

To summarize what was discussed in this chapter, an overview of the various components of the smart metering infrastructure was discussed. This provided an understanding of the characteristics of the smart metering network. Based on these characteristics identified, a fault management model for smart metering network was proposed. The different category of events generated by smart meters were identified and classified and the functional requirements for the fault monitoring system were also identified.

As mentioned at the beginning of this chapter, the fault monitoring systems must take into consideration two main aspects of the network to be monitored. The topics discussed in this chapter helped in understanding the first aspect which is the smart metering network architecture, topology, devices, connections, services, dependencies and relationships among them. The next stage in the modelling of the fault monitoring system is to understand the communication protocols used for managing the network. The functional requirements provided in this chapter forms the basis for evaluating the fault monitoring capabilities of the candidate communication protocols identified in section 2.4.

4. Fault monitoring

As illustrated in Figure 9 the main components of the smart metering infrastructure are the smart meters, the SM-HAN gateway, the NMS and the communication protocols. The only component that was not included for discussion in Chapter 3 was the communication protocol. However, Chapter 3 provided the requirements for evaluating the fault monitoring capabilities of the candidate communication protocols. Therefore the main objective of this chapter is to evaluate the fault management capabilities of the candidate communication protocols based on the requirements presented in Chapter 3.

The Communication Protocol is an application layer protocol which describes a standardized method of communication for managing devices in a communications network. As illustrated in Figure 9, devices on SM-HAN use a communication protocol which is specific to that network segment for exchanging messages, responses, and events. As seen in earlier discussions the communication protocol is dependent on the underlying data transmission technology, for ex: Devices on SM-HAN may be connected over a ZigBee network, therefore these devices use ZigBee clusters as their communication protocol. Similarly devices connected over a PRIME PLC network would use DLMS/COSEM as their communication protocol. As seen in earlier discussions, several candidate technologies may be used in smart meters. Therefore the communication protocol used in SM-HAN will be specific to the chosen smart meter technology.

4.1. Dependencies

The storage requirements and the amount of storage available in devices in the smart metering system is device specific. The smart metering equipment specification document published by DECC requires the devices to able to retain device configuration information at all times and meter data and events for a specified amount of time. The storage requirements are classified based on the kind of data to be retained. This includes device specific data, configuration specific data and operational data. The device specific data registers holds information about the current firmware version, device type, device identifier etc. The configuration data registers holds information related device configuration information such as how the device establishes WAN link (i.e. device network identification), pricing information (i.e. tariff details) etc. The operational data registers holds information about meter readings, events generated by meters etc. The communication protocols provide a mechanism for manipulating and accessing the information from these devices [29].

4.2. Assumptions and limitations

The study carried out did not involve any hardware component. The facts presented are purely based on literature review.

ZigBee alliance maintains the specifications and documentation for ZigBee standards and the documentation are available publically. Since ZigBee is a leading contender and is well placed in the market with large scale deployments and many device manufacturers and vendors supplying ZigBee compliant devices, capabilities of ZigBee is evaluated.

The application layer protocol for meter data exchange DLMS/COSEM is a leading application layer communication protocol used by many commercial applications namely PRIME PLC, G3 PLC, M-BUS etc, which are currently in use for meter data exchange. Therefore the capabilities of DLMS/COSEM are also evaluated.

Although DLMS/COSEM is an open standard, the documentation for DLMS/COSEM is maintained by the DLMS UA. The DLMS/COSEM specification is fully described in the DLMS UA coloured books, however, only excerpts from these books are available publically. The DLMS/COSEM full documentation is available from the DLMS website only for members of the DLMS UA. Therefore the study carried out on DLMS/COSEM was limited due to the unavailability of full documentation.

Lonworks and KNX are also open standards, and the documentation is maintained by Echelon and KNX respectively. Echelon and KNX also provide the documents only for the participating members and is not available publically.

4.3. Summary of requirements for fault monitoring

The various functional requirements for fault management services presented in the previous chapter can be grouped under the following 3 categories.

- Event configuration and Reporting: This is concerned with the configuration, detection, notification and control of the events.
- Event storage and retrieval: This is concerned with the storage and retrieval of events (both scheduled and on demand)
- Device configuration and testing: This is concerned with device configuration and testing.

4.4. ZigBee network architecture for fault management

A ZigBee network known as a personal area network (PAN)[1], consists of 3 types of nodes, a ZigBee end device, ZigBee router and a ZigBee coordinator. ZigBee end devices are nodes with a low duty cycle (i.e. usually in a sleep state and not permanently listening), designed for battery operation. ZigBee routers are nodes that are permanently listening devices and they act as packet routers, once they have joined an existing PAN. ZigBee coordinators are also permanently listening devices and they are responsible for establishing the PAN and allocation of addresses to the new nodes joining the PAN. Coordinators are also aggregators through which all the PAN data is routed into and out of the ZigBee PAN to other networks or devices outside the ZigBee PAN. Therefore coordinators are also routers.

Typically the SM-HAN is installed by the utility supplier. As seen in the previous discussion irrespective of the communication technology a SM-HAN contains several devices which are required to provide the smart metering functionality. A mapping of various SM-HAN devices to ZigBee devices is provided here.

[1] A ZigBee based HAN is a ZigBee PAN.

4.4.1. ZigBee smart meters

These are the ZigBee end devices which are battery operated, the gas and the water meters. An electricity meter can also be an end device, but, since electricity meters have direct access to power additional functionality could be included in these devices.

4.4.2. ZigBee-HAN gateway device (GD)

In a ZigBee PAN the GD is a ZigBee coordinator, these devices must have direct access to power therefore the GD could be housed within an electricity meter or it could be a standalone device which must have direct access to power.

4.4.3. ZigBee range extender

ZigBee routers act as range extenders they are also responsible for routing packets. A range extender could be housed within an electricity meter or it could be a standalone device which must have direct access to power.

4.4.4. ZigBee node addressing

ZigBee nodes have two kinds of address a 64 bit MAC address and a 16 bit network address assigned by the network coordinator when a node joins the network. Node addresses are stored in routing table on routers and the network coordinator. Both the MAC address and the network node addresses are stored in the routing tables.

4.4.5. Endpoints, device discovery, service discovery and binding

ZigBee uses a concept of Enpoints to address the applications running on ZigBee nodes in a PAN. A ZigBee node in a PAN may have several applications running on it. These application instances on a node are said to be endpoints, where messages can originate and terminate. There can be upto 240 endpoints (applications) on a ZigBee node. Each application on the node is uniquely identified by its endpoint address. Endpoint addresses for user applications are numbered from 1 to 240.

Device Discovery is the process whereby ZigBee nodes can discover other ZigBee nodes on the network by initiating queries that are broadcast to all nodes on the network.

Service Discovery is the process whereby services available on endpoints of a device are discovered by other devices in the PAN.

4.4.6. Binding

Binding is the process of associating source address, source endpoint, cluster id to a list of destination address and destination endpoint. The network coordinators and routers maintain the binding tables which has the binding information of all devices on the PAN. ZigBee end nodes can directly send messages to the network coordinator without binding.

4.4.7. ZigBee components for fault monitoring

ZigBee provides a complete protocol stack for implementing a wireless PAN. The following section identifies and gives an overview of the ZigBee components that are required for modelling the fault management system.

4.4.7.1. ZigBee Application Profile

ZigBee is designed as an industry-standard protocol for the implementation of wireless networks by different manufacturers. One of its aims is to allow wireless network devices from multiple manufacturers to operate together in the same network. With this aim in mind, the ZigBee Alliance introduced the concept of an Application Profile.

An Application Profile provides a design framework for a specific market sector by defining a set of devices that can be coherently used together in implementing an application for that market sector. For example, the ZigBee Alliance has defined the Home Automation (HA) profile for use in controlling appliances and systems in the home, such as a lighting system. It defines a number of 'devices' and functions that are needed or useful in controlling domestic systems, e.g. switches, dimmers, occupancy sensors and load controllers for a lighting system. The ZigBee smart energy profile addresses the smart metering market.
ZigBee public profiles are those specified by the ZigBee Alliance as opposed to private profiles specified by individual device manufacturers.

4.4.7.2. Devices

In ZigBee, a 'device' is a software entity comprising the set of properties and functionality of an application that runs on a network node.

4.4.7.3. Attributes

An attribute is a data entity, such as a device configuration parameter. An application has a set of attributes that it uses in its communications - attribute values are exchanged in the messages sent from one application to another in a ZigBee network.

4.4.7.4. Clusters

ZigBee applications use the concept of a 'cluster' for communicating attribute values. A cluster comprises a set of related attributes together with a set of commands. A cluster has two aspects, which are respectively concerned with receiving and sending commands. One or both aspects may be used by a ZigBee application device. This is illustrated in Figure 14.

Server or Input Cluster: This side of a cluster is used to store attributes and receive commands to manipulate the stored attributes (to which the cluster may return responses) - for example, a server cluster on a Metering Device may store an "energy consumed" attribute and associated attributes, and respond to commands which request readings of these attributes.

Client or Output Cluster: This side of a cluster is used to manipulate attributes in the corresponding server cluster by sending commands to it (and receiving the responses). Normally, these are read commands to obtain attribute values (the read values being returned in the responses) – for example, to read the "energy consumed" attribute (and associated attributes) on a remote Metering Device. There may also be write commands to remotely set attribute values.

Clusters are defined in a ZigBee Application profile, and the ZigBee devices are defined by the clusters they use.

Clusters in an application profile are uniquely identified by a cluster identifier. Attributes within a cluster are uniquely identified by an attribute identifier.

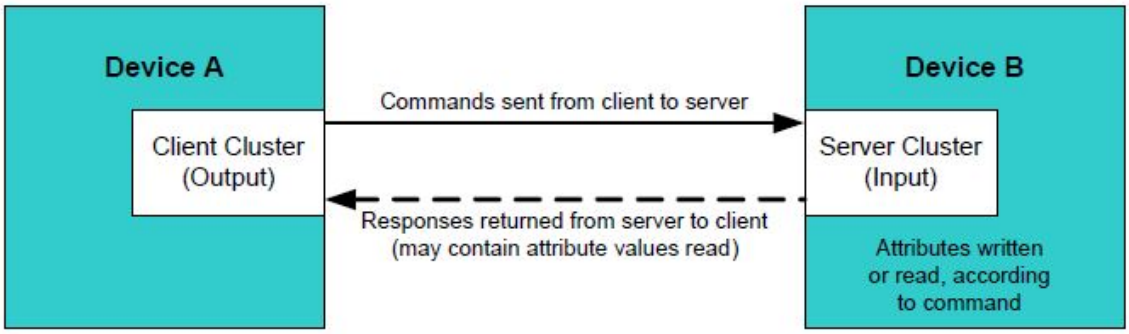


Figure 14 - ZigBee Clusters

4.4.7.5. ZigBee Cluster Library (ZCL)

Although clusters may be defined in an Application Profile, certain clusters are useful across all Application Profiles. Therefore, the ZigBee Alliance has defined a number of standard clusters for different functional areas. These are collected together in the ZigBee Cluster Library (ZCL). For example, the Smart Energy profile uses the Alarm cluster from the ZCL (for configuring alarm conditions on nodes of a smart metering network). A list of clusters from ZCL is provided in the appendix.

The ZCL defines a set of general commands that are used for manipulating attributes and other general tasks that are not specific to an individual cluster. The general cluster commands are listed Table 1.

Table 1 - ZigBee General commands

Command	Description
Read attributes	Read one or more attributes
Read attributes response	Return value of one or more attributes
Write attributes	Write one or more attributes
Write attributes undivided	Write one or more attributes as a set
Write attributes response	Return success status of write attributes
Configure reporting	Configure attributes for reporting
Configure reporting response	Status of configure attributes
Read reporting configuration	Read current reporting configuration
Read reporting configuration response	Return current reporting configuration
Report attributes	Attribute report, depends on configuration
Default response	Unsupported command response
Discover attributes	Determine supported attributes on remote node
Discover attributes response	Results of discover attributes command

4.4.7.6. ZigBee Smart Energy Profile (SEP)

The ZigBee Alliance has published a public Application Profile for Smart Energy called Smart Energy Profile, which specifies a set of clusters and possible devices that use these clusters. Manufacturers who wish to develop Smart Energy products for ZigBee networks could use this specification for designing their products.

4.4.7.7. ZigBee SEP clusters

The ZigBee SEP uses certain clusters from the ZCL and also defines some of its own clusters. All the clusters used by the SE profile are outlined in Table 2. The clusters from the ZCL are listed as “General” and the clusters defined by the SE profile are listed as “Smart Energy”.

Table 2 - ZigBee SEP Clusters

Category	Cluster	Description
General	Basic	The Basic cluster contains the basic properties of a device (e.g. software and hardware versions) and allows the setting of user-defined properties (such as location).
	Identity	The Identify cluster allows a device to make itself known visually (e.g. by flashing a light) to an observer such as a network installer.
	Alarms	The Alarms cluster is used for sending alarm notifications and the general configuration of alarms for all other clusters on the device (individual alarm conditions are set in the corresponding clusters).
	Time	The Time cluster provides an interface to a real-time clock on a device, allowing the clock time to be read and written in order to synchronise the clock to a time standard. This cluster includes functionality for local time-zone and daylight saving time.
	Commissioning	The Commissioning cluster can be used for commissioning the ZigBee stack on a device (during network installation) and defining the device behaviour with respect to the ZigBee network (it does not affect applications operating on the devices).
	Power Configuration	The Power Configuration cluster contains the properties of the device's own power source (which can be mains or batteries), and allows the configuration of under/over voltage alarms.
	Over-the-Air (OTA) Upgrade	The Over-the-Air (OTA) Upgrade cluster provides the facility to upgrade application software on the nodes of a ZigBee PRO network by distributing the replacement software through the network (over the air) from a designated node. In an SE network, this node is normally the gateway device.
Smart Energy	Price	The Price cluster provides the mechanism for sending and receiving pricing information within an SE network. The pricing information is sent by the utility company to the gateway device, which passes the information to SE devices in the utility private HAN (and possibly to other devices in a customer private HAN).
	Demand-Response and Load Control	The Demand-Response and Load Control (DRLC) cluster provides an interface for controlling an attached appliance that supports load control. The cluster is able to receive load control requests (from the utility company) and act upon them – the demand-response functionality.
	Metering	The Metering cluster provides a mechanism to obtain consumption data from a metering device (electric, gas, water or thermal).
	Messaging	The Messaging cluster provides an interface for passing text messages between ZigBee SE devices. These are likely to be

Category	Cluster	Description
		messages from the utility company received by the gateway device, which unicasts a received message to all registered SE devices that implement the Messaging cluster (or makes the message available to all devices for later collection).
	Tunneling (Complex Metering)	The Tunneling cluster provides an interface for implementing tunnelling protocols. It allows any existing metering communication protocol to be transported within the payload of standard ZigBee frames (this includes dealing with issues such as addressing, fragmentation and flow control).
	Prepayment	The Prepayment cluster provides support for pre-purchased credit which, in particular, can be used for electricity consumption. The cluster provides the facility to exchange prepayment information between devices in a HAN - for example, to allow prepayment data held on a Metering Device to be displayed to the customer on an IHD.
	Key Establishment	The Key Establishment cluster is used to manage secure communications in ZigBee, when the underlying network security cannot be trusted. A key agreement scheme is used, requiring the exchange of keying information between communicating devices.

4.4.7.8. ZigBee SEP devices

As seen in the Section - 4.4.7.4, ZigBee devices are defined by the clusters they use. The ZigBee SEP defines various devices used in smart metering. The ZigBee SEP defines the clusters used in each of these devices. For example Table 3 gives a list of clusters that can be included in a smart metering device and
Table 4 gives a list of clusters that can be included in a gateway device.

Table 3 - ZigBee Smart Meter Clusters

Basic
Identity
Key Establishment
Clusters with reporting capability
Power Configuration
Alarms
Commissioning
OTA Upgrade OTA Upgrade
Tunneling Tunneling
Manufacturer-specific
Simple Metering
Time
Price
Optionally Messaging

Table 4 - ZigBee Gateway Device Clusters

Basic
Identity
Key Establishment
Clusters with reporting capability
Power Configuration
Alarms

Commissioning
OTA Upgrade OTA Upgrade
Tunneling Tunneling
Manufacturer-specific
Messaging
Time
Price
Demand-Response/Load Control
Optionally Simple Metering

4.4.8. ZigBee event configuration and notification capabilities

4.4.8.1. Attribute reporting

A cluster client can poll the value of an attribute on the cluster server by sending a 'read attributes' request. Alternatively, the server can issue unsolicited attribute reports to the client using the 'attribute reporting' feature.

4.4.8.2. Attribute report configuration

If automatic attribute reporting is to be employed between a cluster server and client, the reporting rules must be configured. These rules are profile-specific but generally include the following parameters for each attribute:

- Time-interval between consecutive reports in periodic reporting
- Minimum time-interval between consecutive triggered attribute reports
- Minimum change in the attribute value that will trigger an attribute report

This configuration is conducted on the cluster server but is normally directed from a remote device via 'configure reporting' commands. The configuration of automatic attribute reporting follows the process:

1. The client sends a 'configure reporting' command to the server.
2. The server receives and processes the command, configures the attribute reporting and generates a 'configure reporting response' command, which is sent back to the requesting client.
3. The client receives the 'configure reporting response' and the ZCL generates events to indicate the status of the request to the client.

The "Prepayment" cluster specification includes a "CreditRemaining" attribute which represents the amount of credit remaining on the Metering Device. If Monetary based, this attribute is measured in a base unit of Currency. The following sequence diagrams models attribute reporting on the "CreditRemaining" attribute and the report generated by the metering device.

1. The application on the gateway device or the in house display (client) sends a 'configure reporting' command to the metering device (server). The command includes the candidate attribute identifier and the time interval between consecutive reports (For example: Report once daily).
2. The metering device (server) will automatically process the incoming 'configure reporting' command and perform the required configuration. Once the attribute

reporting has been configured successfully, the metering device (server) generates a 'configure reporting response' and sends it back to the requesting client.

3. The 'configure reporting response' consists of the status and the attribute to indicate the status of 'configure reporting' request for the specified attribute. If the 'configure report' was successful a 'SUCCESS' status is sent with the 'configure reporting status' command. Based on this response the client device can perform other actions, perhaps send a confirmation back to the utility supplier.

If automatic attribute reporting has been configured between the cluster server and a client, the reporting of the relevant attributes will begin immediately after configuration.
Attribute reports will be automatically generated when one of the following conditions are met

- Periodically with the configured time-interval between consecutive reports.
- When the attribute value changes by at least the configured minimum amount.

1. The application on the metering device will generate a report at the end of the time interval and send the attribute values to the client using a 'report attributes' command which includes the attribute identifier of the attribute being reported and its value.
2. The client device stores the new attribute value and may or may not perform other actions.

The SEP specification includes attribute reporting for attributes in the Metering, response and load control, and Price cluster.

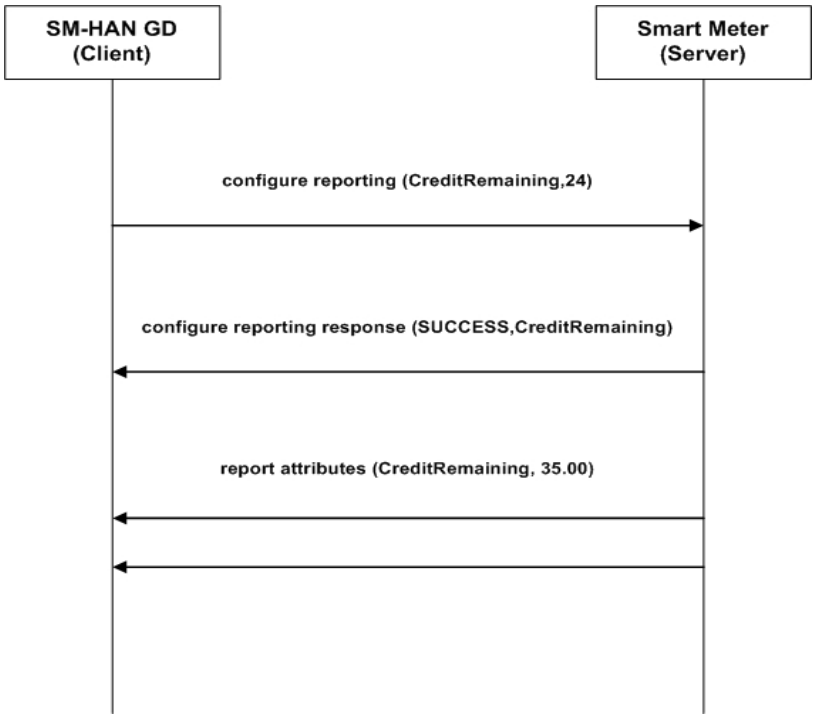


Figure 15 - ZigBee Attribute reporting

4.4.8.3. Alarms cluster and alarm attribute set

The ZigBee SEP specification includes the alarms cluster from the ZCL. The alarms cluster includes attributes and commands for sending alarm notifications and configuring alarm functionality. Alarm conditions and their respective alarm codes are described in individual clusters, along with an alarm mask field. Alarms are reported to subscribed targets using the "Alarm" command. The alarm command includes the cluster identifier and an alarm code.

Alarms are unsolicited notifications generated by the devices on a ZigBee PAN. The alarm command signals the alarm situation on the sending device. An alarm command is generated when a cluster which has alarm functionality detects an alarm condition, e.g. an attribute has taken on a value that is outside a 'safe' range.

The SEP "Metering cluster" includes a set of alarm attributes and specifies the alarm conditions (alarm codes). These attributes include error conditions that are common to all meters and also include error conditions specific to electricity, gas and water meter. The table in the appendix gives a list of the alarm attribute set included in the "Metering cluster".

4.4.8.4. Alarm mask

The "AlarmMask" attributes of the Alarm Attribute Set specify whether each of the alarms listed in the corresponding alarm group is enabled. For example: The alarm attribute set in the "Metering" cluster contains an attribute called "ElectricityAlarmMask" the value of this attribute indicate which alarm codes for an electricity meter must be enabled or disabled. When the bit number corresponding to the alarm number is set to 1, the alarm is enabled, else it is disabled. By default the "ElectricityAlarmMask" has value 0xffffffff, meaning all the alarms relating to electricity meter are enabled. The table lists the codes for generic alarms for all meters.

Table 5 - ZigBee Alarm Masks

Alarm Code	Description
01	Low Battery
02	Tamper Detect
03	Electricity: Power Failure Gas: Not Defined Water: Pipe Empty Heat/Cooling: Temperature Sensor
04	Electricity: Power Quality Gas: Low Pressure Water: Low Pressure Heat/Cooling: Burst Detect
05	Leak Detect
06	Service Disconnect
07	Electricity: Reserved Gas: Reverse Flow Water: Reverse Flow Heat/Cooling: Flow Sensor
08 – 0f	Reserved

4.4.9. ZigBee event storage and retrieval capabilities

The smart metering equipment technical specification document includes the requirement for a log to keep track of the latest 100 time stamped events. The alarm cluster includes an alarm table to store details of the alarms generated within the device. The maximum number of entries in the table is device dependent. When an alarm is generated, a corresponding entry is placed in the table. If the table is full, the entry with the earliest time stamp field is replaced by the new entry.

The general 'Write Attributes' command is used to set the alarm mask on the end devices.

The 'Get alarm' command in the alarms cluster can be used to retrieve the alarm with the earliest timestamp in the alarm table to be reported in a 'get alarm response' command. This command enables the reading of logged alarm conditions from the alarm table. Once an alarm condition has been reported the corresponding entry in the table is removed.

4.4.10. ZigBee device testing capabilities

The ZigBee SEP provides the following recommendations for tracking devices on the PAN.

1. A ZigBee coordinator should also be the PAN trust center.
2. The trust center should maintain a list of authorized devices and for each authorized device the trust center should also maintain the following items.
    a. Registered devices MAC address
    b. Device installation code
    c. Registration status
    d. Time and date stamps

A trust centre is a node in the ZigBee network that is responsible for managing security keys for the ZigBee PAN and it is also responsible for admission of new nodes into the ZigBee PAN.

In order to track a device, the ZigBee device discovery mechanism could be used. The ZigBee Device Discovery mechanism is supported for both the 64-bit MAC address and the 16-bit Network address. Device discovery can use unicast address to the devices MAC address. Only the specified ZigBee End device will respond with its address to the device discovery request. If the device does not respond within a timeout period, the node is marked as unreachable or failed.

4.5. ZigBee summary

Since ZigBee's focus is communication for low power devices, they address the issue of battery operated devices for gas and water meters. ZigBee's support for different kinds of nodes in PAN enables to provide connectivity to devices in hard to reach places. ZigBee provides a good set of features for event configuration, control, management and reporting. The attribute reporting feature enables user to conveniently setup reporting on individual devices. This can be a handy feature for both the network service providers and the end users alike to customize different kinds of reports from different end devices (different reports for electricity, gas and water meter). The attribute reporting can be easily setup and the frequency of reporting controlled using simple 'configure reporting' ZigBee command. The alarms cluster from the ZCL and ZigBee public profiles provides standardized implementation of

alarm configuration and reporting enabling interoperability between devices from different manufacturer operating on the network. Manufacturers can also extend these standard implementations to provide other fault and device management capabilities.

However, ZigBee devices can only communicate with devices that implement a ZigBee protocol stack. A gateway device is mandatory for managing ZigBee devices. In a large scale network the gateway device (coordinator) must have sufficient resources to maintain the device binding and service binding information. Since the ZigBee network is a resource constrained network and due to the low duty cycle of end devices, the events generated are propagated to the network managers in near real time (i.e. propagated when the devices wake up). This is true even when executing the device management commands, the commands sent to the end devices are executed only when the devices are awake. The resource constraint and device latency must be factored by the fault monitoring system.

4.6. DLMS/COSEM

COSEM (Companion Specification for Energy Metering) provides an interface object model for smart metering devices and is based on xDLMS (Extended Device Language Message Specification) standard. DLMS is an application layer protocol, specifying general concepts for the modelling of object-related services, communication entities and protocols. xDLMS is an extension to DLMS and describes how to access attributes and methods of COSEM objects.

4.6.1. COSEM Data Model

The main principle of COSEM is object modelling, meaning the real metering device is completely hidden from the user by providing a completely virtual device whose components are generic and standardized. The virtual device reflects exactly the metering device from an external point of view, meaning COSEM models only the elements of the meter that are visible externally.

COSEM modelling is based on a hierarchical structure comprising of a physical device, the logical device and the COSEM interface objects inside the logical device.

4.6.2. Logical device and Application Process (AP)

The physical device is the actual end device. Each physical device may contain several logical devices, for instance a single electricity meter may include a meter for measuring electricity consumption and a separate meter for measuring micro generation both encased within a single device. In this case the consumption meter is a logical device and the micro generation meter is another logical device. Each logical device is modelled as an application process.

4.6.3. COSEM Interface Class (IC) & COSEM interface objects

A logical device (AP) is a container for COSEM objects. A COSEM object is simply a structured piece of information with attributes and methods. Attributes represent the characteristics of an object. The value of an attribute may affect the behaviour of an object. An object may offer a number of methods to either examine or modify the values of the attributes. Objects that share common characteristics are generalized as COSEM Interface Class (IC). COSEM defines ICs for data storage, access control, management, time and event bound control. There are about 50 different ICs and about 150 COSEM objects defined by

DLMS UA for modelling different types (electricity, gas, water, heat) and aspects (meter data, errors, data registers, underlying physical communication medium etc) of smart meters (Interfaces classes and objects are specified in the DLMS UA Blue book and the object list)[30].

4.6.4. Client/Server model

DLMS/COSEM is based on a client/server structure in which the data collection system acts as a client requesting data from the servers (pull operation), in this case the meters. In this environment communication takes place always between a client and a server application process, i.e. the server application process provides remote services to the client application process. These services are provided via exchanging messages between the client and the server application processes.

4.6.5. Object Identification System (OBIS)

COSEM uses a methodology for identifying the different COSEM interface objects. The COSEM object naming is based on a 6 digit identification system called Object Identification System (OBIS). OBIS naming is used to make COSEM interface objects self describing (OBIS codes for commonly used COSEM interface objects are specified in the DLSM UA Blue book).

4.6.6. COSEM management logical device

According to COSEM standards, all physical devices must have a special logical device called the management logical device, with the predefined address 1. The management logical device itself may contain a lot of information, but, at the minimum, it has to contain a description of all the logical devices available in the physical meter, with their logical addresses and names. COSEM object SAP assignment is used for maintaining the list of all logical device name and addresses within the meter. The COSEM management logical device is also responsible for notification of events in the server to the clients Management AP. The predefined client address i.e. data concentrator address is configured during the device initialization stage and the server devices use this predefined address to send event notifications.

4.6.7. COSEM association object

Each logical device contains at least one object of class Association LN or Association SN (LN and SN is discussed below). The main role of an association objects is maintaining a list of all the other COSEM objects that are used in the logical device (AP). The association object has an attribute called the object list containing the list of all objects available in the logical device.

Note: The DLMS and ZigBee high-level data models are very similar: DLMS Logical Devices are Equivalent to ZigBee applications, DLMS interfaces objects are equivalent to ZigBee clusters. The DLMS Blue book is the equivalent of the ZigBee cluster library (ZCL). The fundamental difference is That ZigBee clusters behave as servers or clients, enabling peer to peer communication, while DLMS Interface objects are only servers. Another difference is that the Bluebook focuses on metering and Basic meter related I/O control, while the ZCL scope extends beyond metering.

4.6.8. Connection oriented service

The data communication uses a connection oriented service, where the client must first establish a connection with the server for the data exchange to take place. In order to allow the client party to access COSEM interface objects in the server, the DLMS-UA defined the concept of “Application Association” (AA). This application association is an application-level connection. It is established between a Client AP (application process) and a server AP. The client AP always initiates the establishment of the association. For very simple devices, one-way communicating devices, and for multicasting and broadcasting pre-established associations are also allowed using predefined addresses (A data concentrator in a network has a predefined client address which can be used by the meters for sending event notifications). After the association establishment, the client AP and the server AP can perform data exchange. Once the data exchange is completed the connection is terminated.

4.6.9. Logical Name (LN) and Short Name (SN)

COSEM standards support two kinds of data exchange with meters referred to as "contexts", which differs in the way the data is addressed (or referenced). In the logical name reference context (or LN) the data is referenced by the logical name (OBIS code). In the short name reference context (or SN) the data is referenced (addressed) by a unique 16 bit integer. Furthermore, the services used to access the data are different in each context. In LN context, the relevant services are Get (to read data) and Set (to write data) and in SN context the services are Read and Write. The context cannot be freely chosen by the client. Rather, it is fixed by the meter's manufacturer; it is a characteristic of its implementation. Therefore, the meter's context must be known beforehand.

4.6.10. COSEM_on_IP Profile

The COSEM_on_IP profile is a COSEM communication profile based on IPv4/IPv6 transport layer. A wrapper layer in between the COSEM application layer and the IPv4 transport layer provides the conversion functions between the COSEM AL to TCP/UDP functions and vice-versa. This enables exchange of DLMS/COSEM messages over a TCP/IP network. As seen in Sections 2.6.1& 2.6.2, PRIM PLC & G3 PLC use this profile [14].

4.6.11. Node addressing

In the TCP/IP based profiles COSEM physical devices are identified by their IP address. The COSEM AL listens only on one TCP or UDP port (port 4059) for exchanging messages between any client and server APs. But, in a single physical device several client or server APs may be present, an additional addressing capability is needed. This is provided by the wrapper layer which provides an identifier – wPort – similar to the TCP or UDP port numbers. A particular COSEM client AP and/or a particular COSEM logical device in the same physical device can be thus identified by its wPort number.

4.6.12. DLMS/COSEM device management data collection system

Smart meters connected on a TCP/IP based network are each assigned an IP address. IP addresses can be assigned both statically or using DHCP. Meters can be accessed over the internet. An additional data collection system to manage a group of meters is also included. To exchange data and device management commands between the smart meters and the managing system, the managing system (client) must also implement the COSEM_on_ip profile [30].

4.6.13. Data communication services

The event monitoring, configuration and notification services are achieved using the following data communication services provided by DLMS/COSEM.

Note: For brevity only the LN data communication service are discussed. The SN referencing system uses equivalent commands.

COSEM provides 3 kinds of data communication services

- COSEM interface object-attribute related services: GET, SET
- COSEM interface object-method related services: ACTION
- Event Notification services

The GET service is invoked by the client AP to request the value(s) of one or all attributes of one or more COSEM interface objects from the server AP.

The SET service is invoked by the client AP to request the remote server AP to set the value of one or more attributes of a COSEM interface object.

The ACTION service is used by the client AP to remotely invoke one or more methods of one or more COSEM interface objects in the remote server AP. The server AP executes the requested ACTION.

The Event Notification Service is used in order to enable the server AP to send an unsolicited notification of the occurrence of an event to the remote client AP. This notification contains the value of a COSEM interface object attribute.

4.7. DLMS/COSEM summary

The media and communication protocol independence of DLMS/COSEM makes DLMS/COSEM suitable (at the application layer level) for use in devices based on a multiple communication protocols. The 3 simple data communication commands (GET, SET and ACTION) can be used for exchanging both data and device management commands. The event notification feature enables server to send unsolicited messages to the client. The cosem_on_ip profile makes it easy to integrate smart meters on a TCP/IP network, which enables the use of the standard TCP/IP features (TFTP, SNMP) for managing these devices. However cosem_on_ip is supported only for certain communication protocol stacks.

On the negative side, DLMS/COSEM's media and communication protocol independence is only at the application layer level. Devices that are based on any single profile cannot communicate with devices based on a different profile. Devices must include multiple profiles to support cross profile communication. COSEM uses separate objects for representing every parameter of a smart meter. There are around 150 COSEM objects covering metering functionalities. The management logical device which keeps track of all the logical devices and all the COSEM objects in each logical device might require larger capacity if the number of logical devices and the number of COSEM objects in a meter increases [31]. COSEM objects models only the smart meters but as seen in previous discussions smart metering systems might include other physical devices such as control valves, load control devices, smart appliances etc. COSEM does not model these devices.

Although the connection oriented transmission provides a degree of reliability it also places a certain degree of overhead especially if it is used with wireless (battery operated) devices. The only wireless standard that DLMS/COSEM supports is wireless M-BUS. DLMS/COSEM tunnelling into ZigBee devices is still under development.

4.8. Conclusion

The fault management capabilities of both ZigBee and DLMS/COSEM were reviewed. Both technologies provide capabilities which can be used for monitoring and management of both business events and system faults in smart meters. Both technologies have merits and limitations. Although both technologies are competing in the smart metering market, they cannot on their own address the various implementation scenarios and challenges of smart metering. It is likely that both these technologies will co-exist and as a consequence the fault monitoring system must be able to monitor and manage both technologies. The fact that ZigBee and DLMS UA are working in alliance for integrating the two technologies supports that argument.

ZigBee is a short range communication technology and it is mandatory to use a gateway device to connect smart meters to central data and management centre. Although smart meters based on cosem_on_ip can be directly connected to an IP network, concepts such as application association will require an intermediate device for managing these devices (ZigBee has service binding). As seen in this chapter, both ZigBee and DLMS/COSEM can be used for propagating the events and management commands between smart meters and a gateway device. These events must be propagated further up from the gateway device to the network management system level. The next chapter discusses how the events are propagated to the network management system and the messages from the network management system sent down to the gateway device.

5. Integration with IP networks

It was highlighted in Section 2.2, DECC's intention to adopt a single network layer based on IP for WAN connectivity. It would be possible to use the traditional IP network management applications for managing devices on SM-HAN. This would require the integration of SM-HAN with IP network. As illustrated in Figure 9, the SM-HAN gateway device is the key component which enables the integration of SM-HAN with IP network.

In order to use IP network management applications for managing devices on SM-HAN, the events generated by smart meters must be propagated to the network management system also the commands issued by the network management system must be propagated to the smart meters. As discussed earlier, the events generated by smart meters are propagated to the gateway device using the communication protocol specific to SM-HAN. These events are then propagated by the gateway device to the network management system using the communication protocol suitable for IP networks as illustrated in Figure 9. Therefore a gateway device is a key component which helps in integration of two disparate networks by providing the protocol conversion functionality and thereby enabling the management of devices on SM-HAN using traditional IP network management tools.

REpresentational State Transfer (REST) and SNMP (Simple Network Management Protocol) IP communication protocols is commonly being used in smart metering gateway devices and data concentrators for exchanging device management data between the gateway devices and the network management systems [32][35][36].

The chapter provides an overview of the fault monitoring capabilities of these two protocols.

Note: The dependencies highlighted in Section 4.1 apply to the discussion in this chapter as well.

5.1. Simple Network Management Protocol (SNMP)

SNMP is a communication protocol that has gained widespread acceptance as a method of managing TCP/IP networks, including individual network devices, and devices in aggregate. SNMP was developed by the IETF (Internet Engineering Task Force), and is applicable to any TCP/IP network, as well as other types of networks. The advantages of using SNMP is that it is simple to use, interoperable, easy to implement and consumes minimal processor and network resources. SNMP is the most widely-used network management tool for TCP/IP based networks.

SNMP defines a client/server relationship. The client program (called the network manager) makes virtual connections to a server program (called the SNMP agent) which executes on a remote network device, and serves information to the manager regarding the device's status. The database, controlled by the SNMP agent, is referred to as the SNMP Management Information Base (MIB), and is a standard set of statistical and control values. SNMP additionally allows the extension of these standard values with values specific to a particular agent through the use of private MIBs. Through the use of private MIB variables, SNMP agents can be tailored for a myriad of specific devices.

Managed devices can be monitored and manipulated using four basic SNMP functions namely -

Get Request: Specific values can be fetched from the managed resource via the "get" request to determine the performance and state of the device. Typically, many different values and parameters can be determined via SNMP without the overhead associated with logging into the device, or establishing a TCP connection with the device.

Get Next Request: The SNMP standard allows network managers to "walk" through all SNMP values of a device (via the "get-next" request) to determine all names and values that a device supports. The "walk-through" feature is accomplished by beginning with the first SNMP object to be fetched, fetching the next name with a "get-next", and repeating this operation until an error is encountered (indicating that all MIB object names have been "walked".)

Set Request: The SNMP standard provides a method of effecting an action associated with a device (via the "set" request) to accomplish activities such as disabling interfaces, disconnecting users, clearing registers, etc. The "set request" provides a way of configuring and controlling network devices via SNMP.

Trap Message: The SNMP provides a mechanism by which devices can alert the network manager of a problem with the device using the "trap" message. The trap function typically requires each device on the network to be configured to issue SNMP traps to one or more network devices that are awaiting these traps.

SNMP specification includes certain management MIBs namely SNMP-NOTIFICATION-MIB, SNMP-TARGET-MIB and NOTIFICATION-LOG-MIB. These MIBs are included in all SNMP compliant devices. These MIBs are used for configuring targets for sending traps, parameters for sending traps to a host (the host address, the timeout and the number of times to retry a message), parameters for selecting specific targets for specific notifications, parameters for notification filtering and parameters for controlling the type and number of traps to be stored. These MIBs include data tables that are used for storing traps and the SNMP manager can query these tables to retrieve traps generated (stored) by the agent. With the help of these features, SNMP manager can selectively choose / filter traps generated by devices on the network. [37][39].

SNMP specification includes a feature called SNMP polling, in which the SNMP manager can send SNMP queries to all the configured agents or can also poll agents selectively. The frequency of polling can also be controlled. This method can be used for testing devices using SNMP.

5.2. REpresentational State Transfer (REST)

REST is a software architecture style in which the application state and functionality are divided into resources, every resource is uniquely addressable using a universal syntax for use in hypermedia links, and all resources share a uniform interface for transferring a state between client and resource. State transfer is accomplished by using the HTTP (or HTTPS) protocol, so these resources can be manipulated by using the four basic operations - Create, Read, Update, and Delete (CRUD- using HTTP methods POST, GET, PUT and DELETE). This principle is applied to the communication between the gateway device and the network

management system by defining a set of resources (specifying for the gateway device, the SM-HAN or the end device), tagging them with a uniform resource identifier (URI), and identifying each function with a state transfer between the network management system and that resource [38].

5.2.1. Resource Identifier

Since REST interfaces use the HTTP protocol, in order to address them, each resource must be associated to an HTTP URL. The object of an HTTP URL is to identify which IP host (and port) to contact and the path to a resource on that host that the client needs to access. For example the URL http://192.168.1.2:4059/restif/gd/version, points to the, "gd/restif/version‟ resource of the HTTP server listening on port 4095 of the host with an IP address 192.168.1.2. The path to the resource (i.e. /restif/gd/version‟ in this example), it can be further divided into two subparts

- The path shared by all the resources of the GD ("/restif/gd‟)
- The path of the resource actually accessed ("/version‟).

The first subpath (prefix) is typically needed when offering many different services on the same HTTP interface (e.g. "/mgmt/index.html‟ may be the path to an administrative web interface), and can be used to give a scope to the set of resources being accessed. This scoping technique may be used to separate the addressing space of GD resources from the addressing space of smart metering network and end nodes resources. This is demonstrated in the following examples [38].

http://192.168.1.2:4059/restif/gd/net/default/services
http://192.168.1.2:4059/restif/gd/net/default/nwnodes/3/services

In the above examples, the first URI may be used for accessing services offered for a network (example: list all routing devices on the network) and the second URI may be used for accessing the services offered by a network end node 3 on the network.

Note : Service offered by the end node does not mean the end node also has a rest interface. The GD uses procedures that are running at the specified URI which maps the http request to device specific commands that are passed on to the end node by the GD.

Typically the host port and the GD URI is referred to as the GDs root URI. In the above examples http://192.168.1.2:4059/restif/gd/ is the GDs root URI.
Therefore http://192.168.1.2:4059/restif/gd/net/default/nwnodes will be the nodes root URI.

5.2.2. Functions and event handlers

Functions are procedures that exist on both the GD and on the network management system. Functions are invoked with a request which may or may not include one or more parameters. Invocation of functions results in responses which are returned with one or more results.

Functions on the network management systems are useful for forwarding unsolicited events generated in the smart metering network or to send responses of non-blocking procedure invocation. Non-blocking procedures are procedures on the GD which can be carried out by the GD without any interaction from the network management system. The network management system invokes the procedure on the GD and the GD returns the results to the

network management system once the request is processed completely. During this processing, the network management system need not wait for the procedure to finish. Typically in sensor networks with sleepy end devices, the gateway device would have to wait for the end device to wake up before carrying out the requests. Non-blocking procedures are ideal in these situations.

Procedures on GD are termed functions and the procedures on the network management system are termed event handlers. Event handlers are also identified by their URIs [38]. Similar to the root URIs for GDs, a network management system would also have a corresponding NMS root URI ex: http://192.168.0.1:4059/restif/nms/.

5.2.3. Callback handlers

Callback handlers are entities on GDs which allows the GDs to supply events generated on the smart metering network to the network management system. Typically callback handlers have the information about Event handler URIs of the network management system and also the criteria for which the GD must invoke an event handler on the network management system. Callback handlers may be used for customising event reporting and event filtering capabilities [38].

5.2.4. Resource manipulation commands

As seen earlier, REST provides 4 basic resource manipulation commands which are used for manipulating the end resources and they are Create, Read, Update and Delete.

I. Read procedure

A read procedure can be a simple procedure for reading information relating to a specific attribute on the gateway device or an end device. It could also be implemented to perform aggregate read functions such as read specified attributes of all devices in the network. Irrespective of the implementation a read procedure uses a http GET, illustrated in the following example.

URI	GDs root URI/attribute Or Nodes root UIR/attribute
HTTP method	GET
Request parameters	None
Response	Attribute value

II. Update procedure

The update procedure could be a simple procedure for updating a specific attribute or an aggregate procedure to update more than one attribute. The update procedure uses a http PUT, illustrated in the following example.

URI	GDs root URI/attribute Or Nodes root UIR/attribute
HTTP method	PUT
Request parameters	Attribute to be updated
Response	None or a Success message

III. Create procedure

A create procedure could be used for creating callback handlers to monitor specific attributes of an end device. Create procedures would use http POST, illustrated in the following example.

URI	GDs root URI/callback Or Nodes root UIR/callback
HTTP method	POST
Request parameters	Attribute to be monitored
	Event criteria
	Event Filtering criteria
	Actions
	Event handler URI
Response	None or a Success message for successful creation of callback handler

IV. Delete Procedure

A delete procedure could be used for deleting an existing callback handler. Delete procedure would use http DELETE, illustrated in the following example.

URI	GDs root URI/callback Or Nodes root UIR/callback
HTTP method	DELETE
Request parameters	Callback handler
Response	None or a Success message for successful deletion of callback handler

V. Events

Events generated by end devices must be reported to the network management system. The GD would use a http POST to report events to the event handlers.

URI	NMS root URI/event handlers
HTTP method	POST
Request parameters	Attribute values
Response	None or a Success message

5.3. Sequence of events

Following the illustration of setting up attribute reporting in Section 4.4.8.2, the sequence diagrams in Figure 16 models setting up of an attribute reporting scenario from the network management system and the eventual propagation of attribute reporting events generated by smart meters to the network management system. This illustration assumes the use of REST as the communication protocol between the network management system and the gateway device. The sequence diagram models the invocation of a non-blocking procedure on the gateway device. The configuration of automatic attribute reporting follows the process:

1. The network management system (NMS) sets up a connection with the gateway device using authentication mechanism etc. Once the connection has been established, the NMS sends an http PUT followed by the XML file which includes information to setup a callback procedure on the gateway device for reporting the attribute "CreditRemaining" on the end device 3 in this example.
2. The gateway device validates the XML and sends http OK to the NMS indicating it has successfully received the information for setting up a callback procedure.
3. The NMS terminates the connection.
4. The gateway device parses the XML file and sends the 'configure reporting' command to the smart meter.
5. Once the smart meter is awake it fetches the outstanding commands from the gateway device and processes the command. It generates a 'configure reporting response' command upon successfully configuring the attribute reporting.
6. The gateway device receives the 'configure reporting response' and an event is generated on the gateway device to indicate the status of the request.
7. The gateway device updates the callback handler list with appropriate information (i.e. event handler information for the type of events etc)
8. Optionally the gateway device can now send a confirmation back to the NMS.
9. At specified time intervals, the smart meter generates the reports by sending 'report attributes' command to the gateway device.
10. The gateway device checks the event information, fetches the event handler information.
11. The gateway device establishes a connection with the NMS
12. The gateway device wraps the event using XML and reports the event using an http POST to the event handler function on the NMS.
13. Optionally the NMS can send event received confirmation or the connection is closed soon after the event is sent to the NMS.

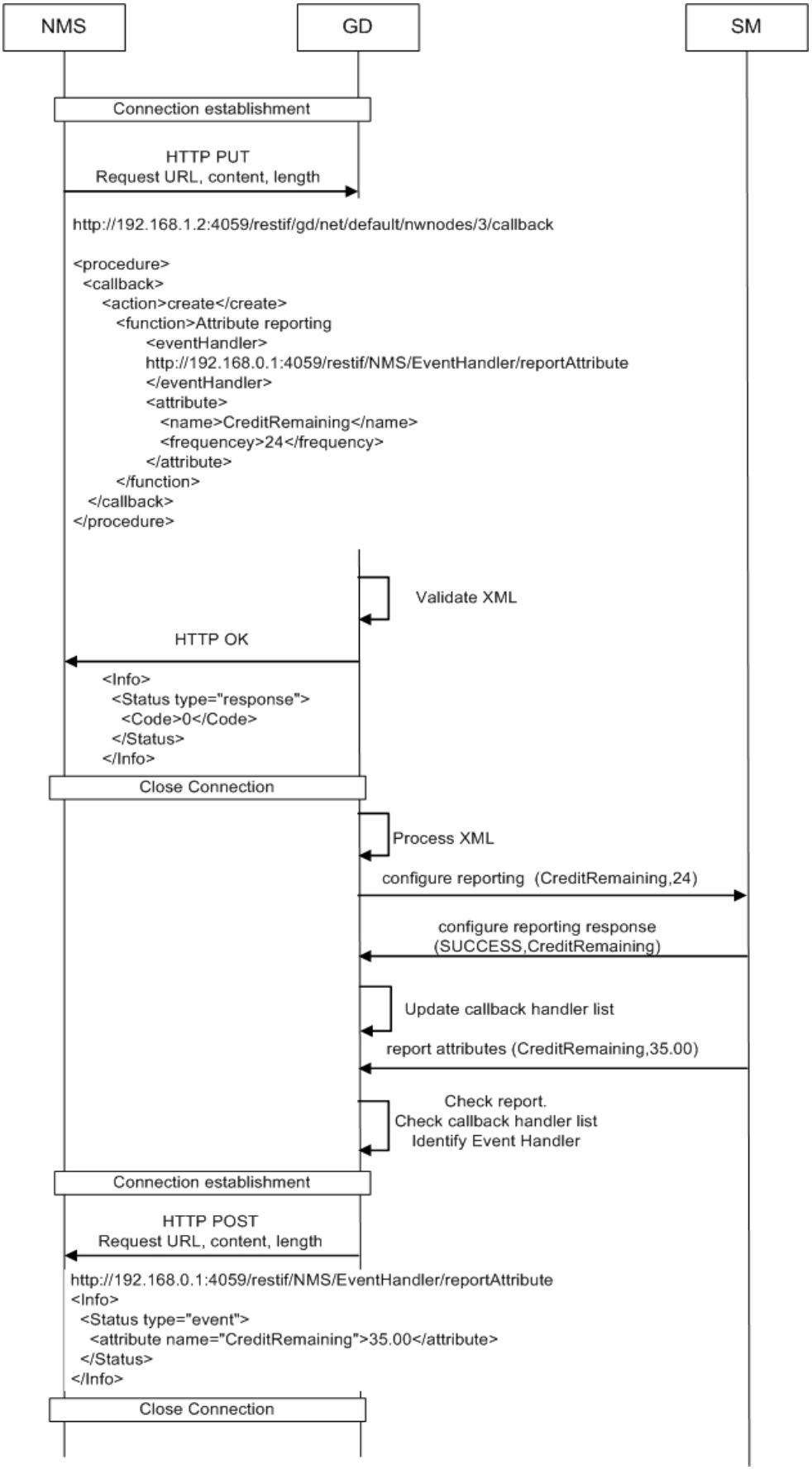


Figure 16 - Sequence of events for setting up attribute reporting from NMS

5.4. Summary

As seen in this discussion, a gateway device is a key component which is responsible for integrating smart metering networks with traditional TCP/IP networks. IC makers and equipment manufacturers in the Smart Grid sector are commonly using SNMP and REST as the communication interface for communication between NMS and the gateway devices (data concentrators). Due to the simplicity and wide acceptance of SNMP, several popular network management systems have the ability to manage SNMP devices. REST on the other hand provides a uniform interface to all the managed resources and hence scalability. The use of XML for message exchange provides a technology neutral platform and enables easy integration with traditional network management systems. The sequence diagram presents an illustration of smart meter attribute reporting scenario and its integration with traditional NMS. Principally the same concept can be applied for other implementation specific fault management scenarios.

6. Conclusion

The dissertation investigated the components and characteristics of the smart metering infrastructure and verified the capabilities of some of the major smart meter communication technology. A model for integrating smart meters with traditional IP network management systems was proposed.

Although smart metering is available in several parts of the world, the investigation carried out has highlighted the fact the main challenge of smart metering is the interoperability between several communication technologies. Although each of the investigated technologies have the capabilities to develop a full scale network management system, it would still require a lot of effort to integrate multitude of these technologies. The interoperability issue is mainly due to lack of universally agreed communication standards. A communication standard would not only address the interoperability issue it would also enable innovation and to bring maturity into the products and applications in the market.

The proposed fault management model uses a layered approach to distribute the responsibilities of managing/monitoring the devices at various levels. This approach clearly provides the benefit of convenient integration of heterogeneous technologies and provisioning of value added services at the service management layer. However, since smart meters are resource constrained devices these devices will have limited capability and therefore upper layers will have higher responsibility of managing/monitoring these devices on the network. As a result the distinction between the network element level and the element management level might converge into a single layer (transport layer).

There are several matured and powerful network management applications currently available in the market for managing devices on IP networks. These applications are capable of providing a very comprehensive set of network management services. The proposal to integrate with IP network management applications is clearly advantageous since these tools can be used to give the same level of services for managing smart meters. Additionally with the emergence of technologies such as IoT (Internet of things) IPv6 etc, it would be possible to connect smart meters directly to the IP network, thereby enabling easy integration with traditional IP network management tools.

The main focus of the study has remained on providing a fault monitoring application for smart meters. However, a full scale network management system (with configuration, accounting, provisioning and security management) would be required to efficiently manage devices on the network. This provides sufficient scope for further research and investigation.

The investigation carried out was mainly based on literature review, and it is worth noting that the actual implementation of the fault monitoring system may be slightly different. However, the dissertation provides a generic model and it might still be a suitable model.

7. References

[1] CIM, 61850, COSEM standards used in a Model Driven Integration approach to build the Smart Grid Service Oriented Architecture - P. Brédillet – Eric Lambert – Eric Schultz Measurement and Information System for Electrical Networks EDF Research and Development Division Clamart France

[2] The OPEN meter Consortium – Description of current state-of-the-art technologies and protocols – General overview of state-of-the-art technological alternatives.

[3] http://www.greentechmedia.com/articles/read/the-smart-meter-landscape-2012-and-beyond/

[4] http://www.thameswater.co.uk/water-meters/14849.htm

[5] http://www.scottishpower.com/PressReleases_1967.htm

[6] Department of Energy & Climate Change Smart Metering Publications of 5th April 2012

[7] DECC - Industry's Draft Technical Specifications - http://www.decc.gov.uk/assets/decc/11/tackling-climate-change/smart-meters/2393-smart-metering-industrys-draft-tech.pdf

[8] Energy Retail Association –('Supplier Requirements for Smart Metering) SRSM and beyond local communications development

[9] Web reference - http://meterpedia.com/mwp/market/sweden/

[10] Web reference - http://www.ZigBee.org/

[11] Web reference - http://www.prime-alliance.org

[12] Web reference - http://www.amperion.com/Amperion_NMS_DataSheet.pdf

[13] Web reference - http://www.ti.com/general/docs/lit/getliterature.tsp?baseLiteratureNumber=slyt431

[14] Smart metering standardization in Europe - THE M/441 MANDATE 3/2011

[15] ERDF - PLC G3 Profile Specification

[16] Web reference – http://www.enel.it/ewcm/salastampa/comunicati_eng/11332-1_PDF-1.pdf

[17] Analysis of State-of-the-art Smart Metering Communication Standards - Klaas De Craemer, Geert Deconinck

[18] ETSI GS OSG 001 V1.1.1 (2012-01) - DGS/OSG-001 Open Smart Grid Protocol (OSGP) specification document

[19] Web reference - http://www.knx.org/

[20] The M-Bus: A Documentation Rev. 4.8 - http://www.m-bus.com/mbusdoc/default.php

[21] Web reference - http://www.dlms.com/news/09-3-dlms-cosem-for-smart-metering.html

[22] The New Frontier of Communications Research: Smart Grid and Smart Metering - Zhong Fan, Georgios Kalogridis, Costas Efthymiou, Mahesh Sooriyabandara, Mutsumu Serizawa, and Joe McGeehan Toshiba Research Europe Limited, Telecommunications Research Laboratory

[23] Smart Grid Reference Architecture Volume 1 - SCE-Cisco-IBM SGRA Team July 14, 2011

[24] Web reference - http://www.etsi.org/WebSite/Technologies/oss.aspx

[25] Network Management Principles and Practice - Mani Subramanian NMSWorks Software Private Limited - ISBN 978-81-317-2759-1

[26] ITU-T Recommendation M.3010

[27] Telecommunication systems and technologies – vol 2 -Telecommunication Network Management - Raouf Boutaba and Jin Xiao University of Waterloo, Canada

[28] Introduction to TMN - Aiko Pras, Bert-Jan van Beijnum, Ron Sprenkels - CTIT Technical Report
[29] DECC - Smart Metering Implementation Programme - Smart Metering Equipment Technical Specifications - September 2012
[30] Web reference - http://www.dlms.com/documentation/overviewexcerptsofthedlmsuacolouredbooks/index.html
[31] Implementing DLMS/COSEM in Smart Meters - Gordan Štruklec, Josko Marsi - 2011 8th International Conference on the European Energy Market (EEM) 25-27 May 2011 Zagreb, Croatia
[32] ZigBee Document 053474r17 – Zigbee Specification
[33] ZigBee Smart Energy Profile Specification Document 075356r16ZB
[34] ZigBee Cluster Library Document 075123r04ZB
[35] Texas Instruments Data Concentrator System Solution ARM9 Chipset specification document
[36] Open meter - D 3.1 Design Of The Overall System Architecture V1.1
[37] Web reference - http://www.net-snmp.org/wiki/index.php/SNMP_notification_processing
[38] Zigbee document 075468r35 – Network Device Gateway Specification
[39] Advances in network management - Jianguo Ding – CRC Press ISBN 978-1-4200-6452-0
[40] Web reference - https://www.echelon.com/
[41] Web reference - http://h20195.www2.hp.com/V2/GetPDF.aspx/4AA1-7653ENW.pdf