

Document history			
V	Date	Author	Description
<i>0.1</i>	<i>2010-04-01</i>	<i>INFINEON</i>	<i>Draft</i>
<i>0.2</i>	<i>2010-05-27</i>	<i>ZIV</i>	<i>Comments from ZIV</i>
<i>0.8</i>	<i>2010-07-13</i>	<i>INFINEON, IMS, UniBo</i>	<i>Results from T2.2, T2.3</i>
<i>1.0</i>	<i>2010-10-28</i>	<i>INFINEON, UniBo</i>	<i>Results from T3.2, 3.6A, ZigBee latency and PER measurements</i>

Disclaimer

The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

The document reflects only the author's views and the Community is not liable for any use that may be made of the information contained therein.

Summary

The High level communication infrastructure concept release is a confidential document delivered in the context of WP3, Task 3.6B: Communication High level communication infrastructure concept with regard to design, develop and deliver Cell level communications within the eDIANA Platform. The concept provides details about the choice between several options and the concept for the prototype communication middleware for iEi to be developed and delivered.

This document is about dealing with the study of the communication protocols between the nodes (devices) at the Cell level. In particular, suitable multiple access control (MAC) protocols, and routing algorithms, are studied or if necessary designed. Other topics include investigation of flexibility in communication through standard protocols (IEC 870-5-102, IEC 870-5-104, MODBUS, DNP3, DLMS etc.).

Security against cyber-attacks is one of the key topics, ensuring that Cell level operations are controlled and secure. Therefore the development of safe communication between iEi and the e-Diana manager at Home level is considered.

This task interacts with WP1, WP2, WP3 tasks and WP9.

Contents

SUMMARY.....	3
ABBREVIATIONS	5
1. INTRODUCTION	6
2. REQUIREMENTS	7
2.1 REQUIREMENTS FROM WP1 DELIVERABLE T1.3	7
2.2 REQUIREMENTS FROM WP2 DELIVERABLE D2.1-B: eDIANA REFERENCE ARCHITECTURE .	7
2.3 REQUIREMENTS FROM WP2 DELIVERABLE 2.2 DESIGN AND DEVELOPMENT OF MIDDLEWARE TECHNOLOGIES FOR eDIANA.....	10
2.4 REQUIREMENTS FROM WP2 DELIVERABLE 2.3-A NETWORK TOPOLOGY AND COMMUNICATION ARCHITECTURE DEFINITION.....	11
2.5 REQUIREMENTS FROM WP2 DELIVERABLE D2.3-B: COMMUNICATION PROTOCOL SPECIFICATION	12
2.6 REQUIREMENTS FROM WP3 DELIVERABLE D3.1-A CELL LEVEL MONITORING AND METERING SYSTEM.....	12
2.7 REQUIREMENTS FROM WP3 DELIVERABLE D3.1-CELL LEVEL MONITORING AND METERING SYSTEM. DESIGN AND DEVELOPMENT OF POWER CONSUMPTION SENSOR.....	14
2.8 REQUIREMENTS FROM WP3 DELIVERABLE D3.2-A INTELLIGENT EMBEDDED INTERFACE ..	15
3. IMPLEMENTATION OPTIONS IEI COMMUNICATION MIDDLEWARE	17
3.1 DLMS.....	17
3.2 MODBUS	17
3.3 IEC 870-5-101	18
3.4 IEC 870-5-102.....	18
3.5 DNP 3.0	19
3.6 OPEN METERING SYSTEM GERMANY	19
3.7 COMPARISON OF DNP 3.0, IEC 870-5-101 AND MODBUS	20
3.8 ZIGBEE LATENCY AND PACKET ERROR RATE MEASUREMENTS	23
3.8.1 <i>Processing Time of the ZR</i>	24
3.8.2 <i>Synchronized Query</i>	25
3.8.3 <i>Periodic Traffic</i>	26
3.8.4 <i>Measurements in an Office</i>	27
4. CONCLUSION	30
ACKNOWLEDGEMENTS.....	30
REFERENCES	31

Abbreviations

eDIANA	Embedded Systems for Energy Efficient Buildings
MCS	Macro Cell Control
MCC	Macro Cell Concentrator
MCD	Macro Cell Data
CDC	Cell Device Concentrator
CMM	Cell Monitoring and Metering
CCA	Cell Control and Actuation
iEi	Intelligent Embedded Interface
CGS	Cell Generation and Storage
CUI	Cell User Interface
DLMS	Device Language Message Specification
COSEM	Companion Specification for Energy Metering
DNP	Distributed Network Protocol
SML	Smart Message Language
OSI	Open System Interconnection
OBIS	Object Identification System
ISO	International Organization for Standardization

1. Introduction

There is Communication middleware for iEis with regard to design, develop and deliver Cell level communications within the eDIANA Platform. The communication concept draft provides the specification for the prototype communication middleware for iEi to be developed and delivered.

This document is about dealing with the study of the communication protocols between the nodes (devices) at the Cell level. In particular, suitable multiple access control (MAC) protocols, and routing algorithms, are studied or if necessary designed. Other topics include investigation of flexibility in communication through standard protocols (IEC 870-5-102, IEC 870-5-104, MODBUS, DNP3, DLMS etc.).

Security against cyber-attacks is one of the key topics, ensuring that Cell level operations are controlled and secure. Therefore the development of safe communication between iEi and the e-Diana manager at Home level is considered.

2. Requirements

2.1 Requirements from WP1 Deliverable T1.3

The deliverable describes requirements for the intra-cell communication as follows: requirements will be accounted for in this Deliverable:

- Req. 1.2.2.2: cost of the solution. This issue has been considered in the identification of the middleware solutions to be used at the intra-cell level
- Req. 1.2.2.3: Standard-compatible solution. All selected solutions shall be compatible with a standard
- Req. 1.5.2.1: Use of multi-hop communication. In the intra-cell network multi-hop is used to allow connectivity of devices located at large distance from CDC
- Req. 1.5.2.7: No deployment of extra-cable. Wireless links shall be used for the intra-cell communication whereas PLC will be used in the intra-cell network if Ethernet will not be available.
- Req. 1.7.2.6: A maximum delay of 5 seconds shall be guaranteed for the delivery of controlling data from devices to the CDC and from the CDC to controllable devices
- Req. 1.7.2.10: A maximum number of 100 devices shall be considered in the prototype to be supported
- Req. 1.7.2.29: Easy commissioning e.g. the download and hassle free installation of devices shall be supported
- Req. 2.1.1.2.12: Prevent unintended registration. This issue will be supported by security means.

2.2 Requirements from WP2 deliverable D2.1-B: eDIANA Reference Architecture

WP2 deliverable D2.1-B: eDIANA Reference Architecture [1] defines the required components at cell level (Figure 1-1) and their interfaces.

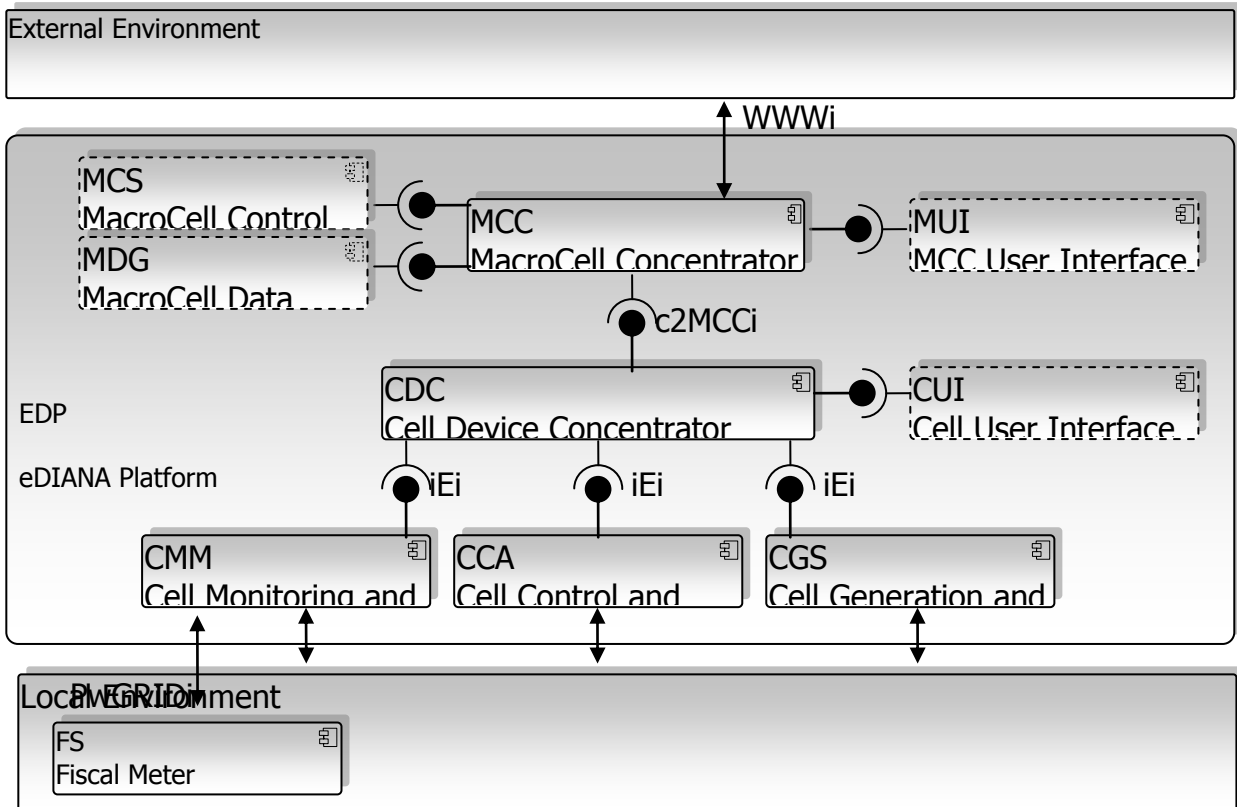


Figure 2-1, eDIANA Platform and external and local environment

These components respectively their interface requirements are:

- **Cell Device Concentrator (CDC):** Gathering and processing data and interfacing with higher levels e.g. MacroCells the CDC shall implement the iEi protocol, in order to connect to the components inside the Cell. In addition the CDC has to provide the interface towards the MCC.
- **Cell Monitoring and Metering (CMM):** Sensors such as temperature, lighting, sun radiation, people presence, energy generation, smart meters of plugged devices. CMM devices must implement part of the iEi protocol. If the protocol should not be implemented in the device, the vendor shall provide a translation driver compatible with the CDC. ZigBee is proposed besides cameras.
- **Cell Control and Actuation (CCA):** Actuators such as light dimming actuators, blind actuators, smart appliances etc.). The iEi shall operate as a bridge, providing the so-called iEi interface to the eDIANA network and in the case of intelligent devices, a specific interface to be flexible enough in order to adapt to proprietary interfaces if needed.

- Cell Generation and Storage (CGS): Energy generation and storage systems will be connected to an iEi element. Either they have to provide one of the standard interfaces implemented in the iEi or the iEi must act as bridge to use the proprietary interface provided by the energy-generation element.
- Cell User Interface (CUI): The User Interface Device to interact with the eDIANA system may be connected directly wire line or wireless to the CDC or to Internet. The inter-Cell network enables communications between the different Cells (CDCs) and the MacroCell and is not in the scope of this deliverable.

The iEi shall serve as main interconnect for all intra-cell CMM, CCA and CGS components linked to the eDIANA CDC for eDIANA compliant components as well as third party components with proprietary communication interface (figure 1-2).

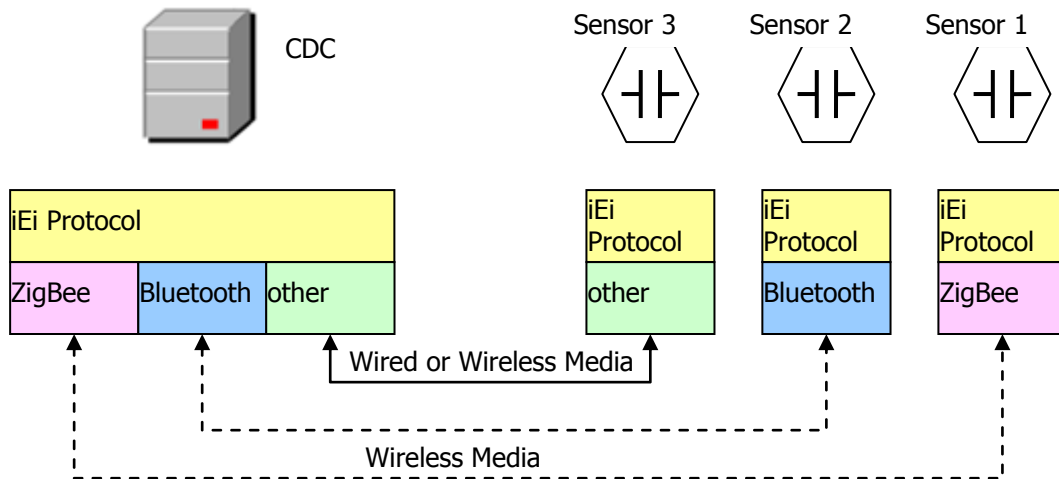


Figure 2-2, Communications layers in eDIANA

The iEi communication protocol shall provide a profile-based identification and authorization mechanism to allow components to identify and authenticate themselves automatically to the CDC. These component profiles will be referred to the eDIANA ontology for component awareness as described in deliverable D2.2-A.

The iEi communication protocol shall implement a polling mechanism to allow the CDC to check the status of the connected components and retrieve periodically data from them. In addition the iEi communication protocol shall provide means to adapt to non eDIANA communication protocols provided by third party components. These communication interface adopters could be either embedded in the CDC as well as in the CMM, CCA and CGS components.

Examples of communication technologies to be used for connecting CDC and third party CMM, CCA and CGS components via the iEis are IEEE 802.15.4 (ZigBee), Bluetooth Low Energy (BT LE) and Powerline (PLC).

2.3 Requirements from WP2 deliverable 2.2 Design and development of middleware technologies for eDIANA

Deliverable 2.2-A Ontology for Device Awareness (document and prototype) describes a semantic technology, for device discovery and interoperability in the context of eDIANA Platform and the prototype Ontology for Device Awareness that provides the semantic concepts of the interaction between the different components and devices to composite the internal situation of the system and its relevant external environment. Since this ontology applies to the cell systems (sensors and devices) that interchange information it has got impact on the middleware decision. The prototype could be used as a common semantic view of the data transferred between devices e.g. Ontology Information level, Ontology Service Level and Ontology Device Level.

Deliverable 2.2-B Software tools for run-time discovery of services and devices (document) describe software tools and platforms that could manage the real time incorporation or disconnection of devices and services through the discovery function. Since Bluetooth Low Energy is not considered anymore, ZigBee will be the main eDIANA framework at the cell level, the service discovery functionality provided by ZigBee has been analyzed.

Deliverable 2.2-C analyzed the impact of the incorporation of a new "framework", as OSGi system, into the eDIANA cell architecture and it was agreed that this is not a good decision because of the needed efforts for the adaptation of the OSGi platform to eDIANA platform and vice-versa. Therefore security facilities provided by ZigBee will be used instead of and it is recommended that the iEi should take care about how the utilization of the security capabilities provided by ZigBee could affect its implementation.

Deliverable 2.2-D describes the lifecycle management subsystem of device controlling software elements, in the context of eDIANA Platform. The prototype Lifecycle Management Support Subsystem provides not only functional or application-oriented code but also extra code that persists at runtime in order to create seamless and user independent manageability of the configuration properties common to all embedded devices within the architecture. Because the iEi could be considered as an other embedded device within the eDIANA architecture, the provision of a control of the lifecycle behavior of the iEi could be envisaged in the middleware.

Deliverable 2.2-E describes the adapted sensor collaboration middleware and its interfaces with the rest of eDIANA cell components. The decisions taken about all the

enumerated functionalities affect the eDIANA sensors as well as the CDC device, so to the iEi. It has been concluded that the first functionality, communication gateway, must be located and embedded into the iEi device.

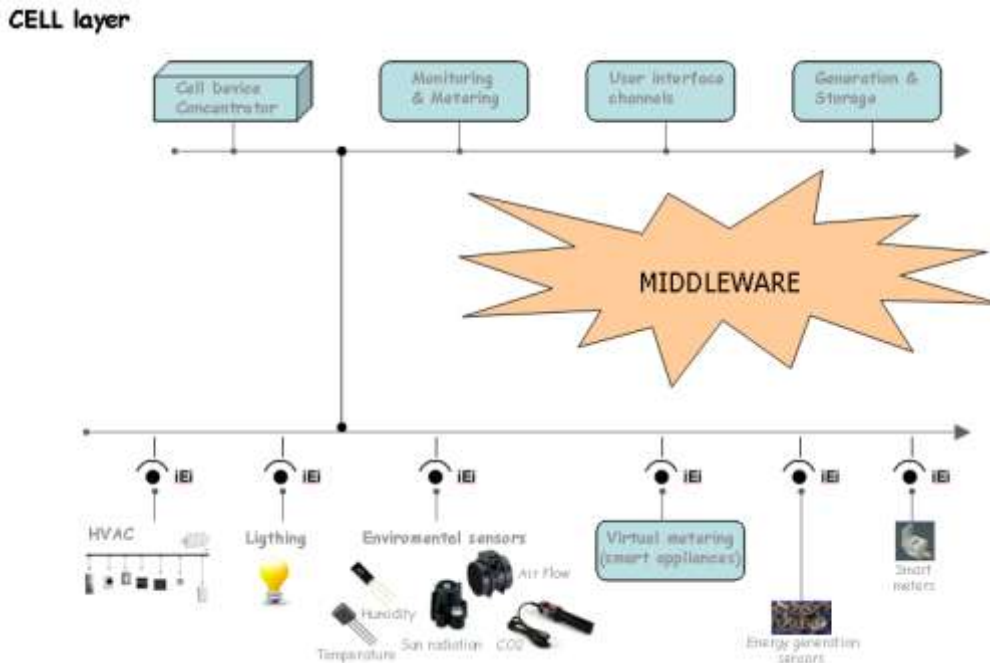


Figure 2-3 Middleware located between sensors and devices as of Deliverable 2.2-E

The following middleware functionalities identified have been analyzed: Communication gateway functionality, Sensors and devices firmware download tool, Service discovery functionality, Event-based data distribution functionality, Security management functionality and Configuration tool for middleware components. Since task T2.3 has been selected ZigBee as the main communication platform in the eDIANA intra cell framework the following middleware components will be available as prototype: Service discovery functionality, Event-based data distribution functionality, Security management functionality and the Configuration tool for middleware components. Communication gateway functionality and the Sensors and devices firmware download tool shall be provided by other means.

2.4 Requirements from WP2 deliverable 2.3-A Network topology and communication architecture definition

WP2 deliverable 2.3-A Network topology and communication architecture definition specifies the communications interface requirements in the intra-Cell network allowing communication among eDIANA components within the Cell between the iEi

and the CDC using IEEE 802.15.4 (ZigBee) as single wireless solution and de facto eDIANA standard solution [2].

At the Application layer, two ZigBee profiles are proposed to use, the Home Automation and Smart Energy profile. If these do not fit sufficiently application, modifications are under study and will be included in D2.3-B.

2.5 Requirements from WP2 deliverable D2.3-B: Communication Protocol Specification

Deliverable D2.3-B selected IEEE 802.15.4/Zigbee as the most suitable technology for intra-cell communication because of the presence of a plethora of products already available on the market and the fulfilment of the system requirements set by the applications, demonstrated through simulations and experimental measurements results done in Deliverable D2.3-A.

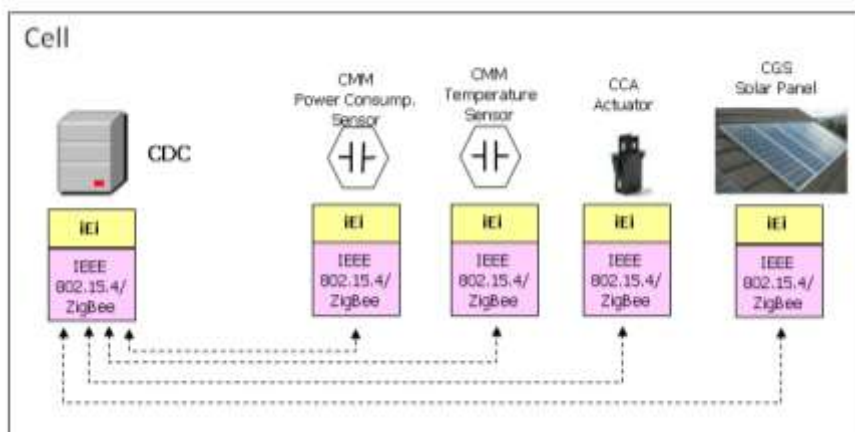


Figure 2-4: The intra-Cell communication network

Each Cell will be comprised of a Personal Area Network (PAN) including a Coordinator within the CDC whereas End Devices and Routers will be distributed over the Cell. A multi-hop network has to be established and mesh topologies will be used to allow the connection of many devices distributed in large area and to overcome problems caused by the death of Routers.

2.6 Requirements from WP3 deliverable D3.1-A Cell Level Monitoring and Metering System

WP3 deliverable D3.1-A Cell Level Monitoring and Metering System [3] specifies the data gathering strategies including the two way communication between the CDC and the eDIANA components through the iEi (figure 2-5).

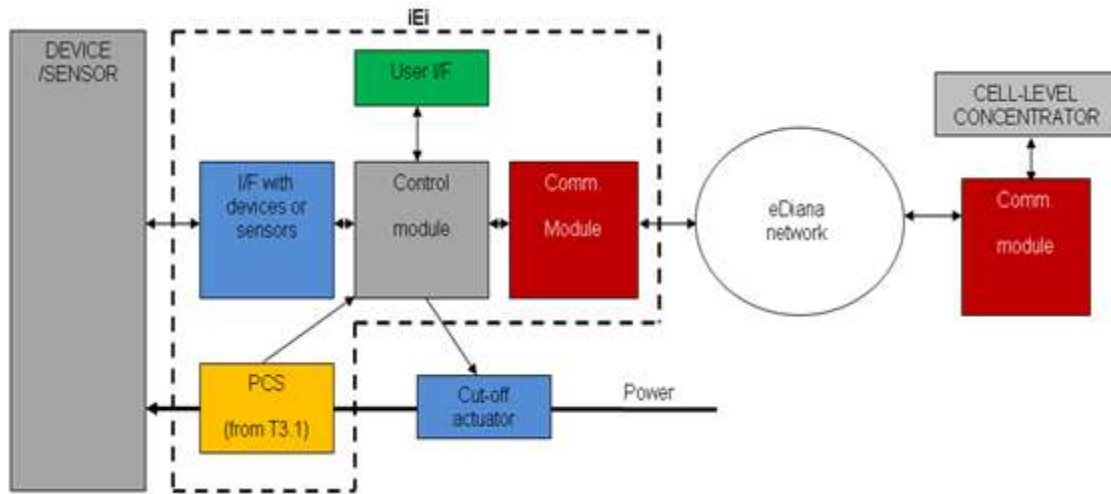


Figure 2-5: The iEi block diagram

The kind of traffic and the flow of data generated is Event-Driven (ED), Query-Based (QB) or a Command and will be supported by the chosen IEEE 802.15.4 air interface for the communication between the CDC and the Cell level devices. Therefore the middleware protocol of the iEi shall take this into account as well.

The OPEN METER Project [5] as one reference for a standardized European smart metering solution is referenced in particular its recommendations for communication protocols and middleware. The communication interfaces defined in OPEN METER system architecture are mapped to eDIANA inter-cell communications (table 2).

Components in OPEN METER	Components in eDIANA	Selected Technologies and lower layer protocols	Selected Upper layer protocols	Selected Data Models
E-Meter / Comms Hub- Concentrator	CMM, CDC	PRIME IEC 61334-5-1	DLMS	COSEM
Concentrator- Central System	CDC, MCC	UMTS GPRS	DLMS SML	COSEM
E-meter / Comms Hub- Central System	CMM, CDC, MCC	UMTS GPRS	DLMS SML	COSEM
Concentrator- Local O&M device	CDC, CMM, CCA; CGS	IEEE802.15.4 IEEE802.11-2007	DLMS SML	COSEM
Multi-utility meter- E-meter / Comms Hub	CMM, CCA, CGS, CDC	IEEE802.15.4 IEEE802.11-2007 Wireless M-Bus	DLMS SML Wireless M-Bus	COSEM
Concentrator- External devices	CDC, CMM, CCA and CGS	ZigBee WiFi	DLMS SML	COSEM
E-meter / Comms Hub- End Customer	CMM, CDC, CUI	Bluetooth	DLMS	COSEM

<i>devices</i>				

Table 2: Overview of selected technologies and protocols in OPEN METER

2.7 Requirements from WP3 deliverable D3.1-Cell Level Monitoring and Metering System. Design and Development of Power Consumption Sensor

The deliverable describes a list of devices which shall be compatible to the eDIANA framework and shall be available for prototyping. Most Devices of these devices can be mapped to an ZigBee smart metering or home automation profile although some devices require the implementation of more than one device profiles on different endpoint to function correctly. Some devices are not compliant to the Home Automation Profile or the Smart Energy profile.

eDIANA Device	Zigbee Profile	Domain	Device
Temperature Sensor	Home Automation	HVAC	Temperature sensor
Pressure sensor	Home Automation	HVAC	Pressure Sensor
Smart Electricity outlet	Home Automation & Smart Metering	General & Smart Energy	Mains power outlet & Simple metering device
Light Sensor	Home Automation	Lighting	Light sensor
Humidity Sensor	Zigbee Cluster Library	Measurement and sensing	Relative Humidity Sensor
White goods (washing machine, dryer, oven etc etc.)	Smart Metering	Smart energy	Smart Appliance
Stirling Engine	Home Automation	HVAC	Temperature sensor, Thermostat, Pump, Heating Cooling Unit.
Presence	Home Automation	General	Occupancy Sensor

Lighting products	Home Automation	Lighting	Dimmable Light, Color Dimmable light, Light Switch, Etc.
Door/Window sensors	Home Automation	General	Simple Sensor

Table 3: eDIANA devices versus Zigbee Profiles

2.8 Requirements from WP3 deliverable D3.2-A Intelligent Embedded Interface

WP3 deliverable D3.2-A Intelligent Embedded Interface [4] specifies the Intelligent Embedded Interface (iEi) to build an intra-Cell network linking the Cell Level Concentrator (CDC) with eDIANA cell-level components Cell Monitoring and Metering (CMM), Cell Control and Actuation (CCA), Cell Generation and Storage (CGS) and Cell User Interface (CUI).

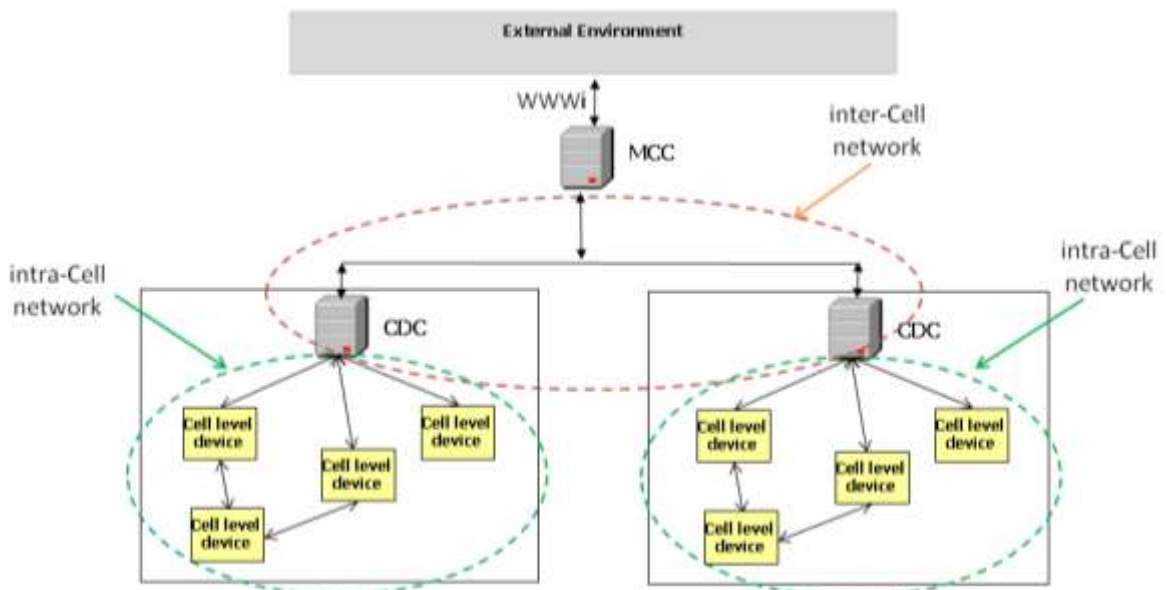


Figure 2-6: The communication Architecture

Each eDIANA framework Cell shall use a Personal Area Network (PAN) based on IEEE 802.15.4 (ZigBee), composed of a CDC and CMM, CGA and CGS components (figure 2-4).

There is a difference between the open eDIANA framework architecture (figure 2-2) and the closed eDIANA framework intra-Cell network proposed here (figure 2-4). Therefore it is proposed to use a Zigbee Gateway functionality plus Zigbee to allow the integration of existing or third party non Zigbee CDC and CMM, CGA and CGS components.

3. Implementation Options iEi Communication Middleware

3.1 DLMS

DLMS or Device Language Message Specification, is the suite of standards developed and maintained by the DLMS User Association and has been co-opted by the IEC TC13 WG14 into the IEC 62056 series of standards. DLMS/COSEM application layer can be used with several low-layer technologies. Currently, several profiles can be used (e.g. for IP-networks, PLC S-FSK and PLC OFDM PRIME). Other profiles are under development, like DLMS/COSEM over Zigbee networks. The reference at this point, once more, is the OPEN METER project. COSEM or Companion Specification for Energy Metering includes a set of specifications that defines the Transport and Application Layers of the DLMS protocol. The DLMS User Association defines the protocols into a set of three specification documents namely Green Book, Yellow Book and Blue Book. The IEC TC13 WG 14 defines the DLMS specifications under the common heading: "Electricity metering - Data exchange for meter reading, tariff and load control."

- IEC 62056-21: Direct local data exchange (3d edition of IEC 61107) describes how to use COSEM over a local port (optical or current loop)
- IEC 62056-42: Physical layer services and procedures for connection-oriented asynchronous data exchange
- IEC 62056-46: Data link layer using HDLC protocol
- IEC 62056-47: COSEM transport layers for IPv4 networks
- IEC 62056-53: COSEM Application layer
- IEC 62056-61: Object identification system (OBIS)
- IEC 62056-62: Interface classes

3.2 Modbus

MODBUS is an application-layer messaging protocol, positioned at level 7 of the OSI model. It provides client/server communication between devices connected on different types of buses or networks. The de facto industrial serial standard since 1979, MODBUS continues to enable millions of automation devices to communicate. Today, support for the simple and elegant structure of MODBUS continues to grow. The Internet community can access MODBUS at a reserved system port 502 on the TCP/IP stack.

MODBUS is a request/reply protocol and offers services specified by function codes. MODBUS function codes are elements of MODBUS request/reply PDUs. This protocol

specification document describes the function codes used within the framework of MODBUS transactions.

3.3 IEC 870-5-101

The IEC Technical Committee 57 (Working Group 03) have developed a protocol standard for telecontrol, teleprotection, and associated telecommunications for electric power systems. The result of this work is IEC 870-5. Five documents specify the base IEC 870-5. The documents are:

- IEC 870-5-1 Transmission Frame Formats
- IEC 870-5-2 Data Link Transmission Services
- IEC 870-5-3 General Structure of Application Data
- IEC 870-5-4 Definition and coding of Information Elements
- IEC 870-5-5 Basic Application Functions

IEC 870-5-101 (T101) is a companion standard generated by the IEC TC57 for electric utility communication between master stations and RTUs. The IEC 870-5-101 is based of the five documents IEC 870-5-1-- 5. Like DNP 3.0, T101 provides structures that are also directly applicable to the interface between RTUs and IEDs. It contains all the elements of a protocol necessary to provide an unambiguous profile definition so that vendors may create products that interoperate fully.

3.4 IEC 870-5-102

IEC 60870-5-102 is an international protocol standard, released by the IEC. It enables communication between a central unit and several counter value devices, in particular in the energy sector. The protocol is based on the EPA architecture (Enhanced Performance Architecture) and defines only the physical, link and application layers of the OSI model.

IEC 60870-5-102 is primarily used with relatively slow transmission media on the asynchronous V.24 interface. The standard promises baud rates of up to 9600 bit/s. X.24/X.27 interfaces with baud rates up to 64000 bit/s, also defined by the standard, could not establish them and are rarely used.

IEC 60870-5-102 is a companion standard, extended by these further standards:

- IEC 60870-5-1 defines different frame formats, though IEC 60870-5-102 uses only the FT1.2 format
- IEC 60870-5-2 defines the link layer transmission mode
- IEC 60870-5-3 defines the basic application data structure
- IEC 60870-5-4 defines how information is encoded
- IEC 60870-5-5 defines basic application layer functions

This protocol is intended for telemetry. Although it could be extended to be used for data and command exchange in the HAN, there are some lacks that should be taken into account. It is a point-to-point protocol, for use on serial links (direct or via modem). Point-to-multipoint communications are possible in bus configurations (RS485), but it has no multicast/broadcast mechanisms. There is no official IP profile for this protocol. Encapsulation in IP frames has been used, but we are talking about proprietary solutions that exceed the standard characterisation. Low security level, based on the concept of "data sessions", entered through a identification process via the corresponding password. Application payload could be encrypted, but using external mechanisms, not defined in the protocol profile.

On the other hand, given the fact that there is an interface with a meter device, this protocol could be a chance, but not for the HAN (communications between iEis) but for the CDC interface with the meter.

3.5 DNP 3.0

DNP was originally created by Westronic, Inc. (now GE Harris) in 1990. In 1993, the DNP 3.0 Basic 4 protocol specification document set was released into the public domain, turned over to Users Group in 1993. Core specification documents are

- DNP 3.0 - Basic 4 Document Set DNP 3.0 Data Link Layer
- DNP 3.0 - Transport Functions
- DNP 3.0 - Application Layer Specification
- DNP 3.0 - Data Object Library

The DNP 3.0 is specifically developed for inter device communication involving SCADA RTUs, and provides for both IED-to-RTU and master-to-IED/RTU.

3.6 Open Metering System Germany

The Open Metering System in Germany has favoured ZigBee as communication standard for a long time. But energy suppliers thought about alternatives due to the fact that the ZigBee standard came later as announced and showed drawbacks in field tests in particular in range. Therefore the Open Metering Group in Germany (an association of Figawa, KNX and ZVEI) released in September 2009 its own standard for the primary communication between sensor, actor and MUC (Multi Utility Communication) as so called OMS (Open Metering System).

The standard family is comprised of EN13757-1 DLMV based application layer, EN12757-2 physical and link layer wired, EN13575-3 application layer, EN13757-4 Physical and link layer ("Stationary Mode" S – unidirectional S1 or bi-directional S2, 32.768 kb/s, 868.3 MHz/ "Frequent transmit mode" T unidirectional T1 or bi-

directional T2, 100kb/s, 868.95 MHz and "Frequent receive mode" R 10 channels, 4.8 kb/s) and EN13757-5 repeating for Mode R. The OMS data are encrypted via AES.

The project „Multi Utility Communication“(MUC) uses for the interface of metering devices to the Multi-Utility-Communication Controller the following standards:

- EN13757-2/-3 M-Bus
- EN13757-4 Wireless M-Bus
- IEC1107 protocol according to DIN EN 62056

The interface to the Internet is a secure data link according to DIN 43863-4 Metering data communication IP-telemetry (GPRS, xDSL or PLC). All data are transferred via SML (Smart Message Language). Further standards used are DIN EN 62056-61 OBIS and DIN EN 62056-62 measurement of electrical power.

3.7 Comparison of DNP 3.0, IEC 870-5-101 and Modbus

To choose a middleware protocol for inter-cell communication one has the opportunity to take a protocol commonly used in the corresponding application domain. IEC 870-5-101 and DNP 3.0 are examples for protocols of these kind mainly used in the utilities industries to cover large cell sizes.

Another option is Modbus as a general purpose, simple and fast protocol which is mainly implemented in industrial applications where the amount of data transfer is small.

Feature	IEC 870-5-101	DNP 3.0	Modbus
Standardization	IEC Standard	Open industry specification	Not Applicable
Organization	IEC TC 57 WG 03	DNP users group	Modicon Inc.
Architecture	3-layer EPA architecture	4-layer architecture, supports TCP/IP or UDP/IP as well	Application layer messaging protocol
Physical layer	Point to Point, Multipoint to point, Implementation by X.24 / X.27 or V.24 /	Supports multiple masters, multiple slave and peer-to-peer communication,	RS 232 serial interface implementation, Peer to peer

	V.28 standard	RS 232 or RS 485 implementation, TCP/IP over Ethernet, 802.3 or X.21	communication, TCP/IP over Ethernet
Data link layer	Frame format FT 1.2, Hamming distance 4	Frame format FT3, Hamming distance-6	ASCII mode and RTU mode
Application layer	Time synchronization, Time stamped events, Select before operate, Polled report by exception, Unsolicited responses, Data group/classes Limited to single data type per message, Can control one point per message only, No internal indication bits, No application layer confirms for events	Time synchronization, Time stamped events, Select before operate, Polled report by exception, Unsolicited responses, Data group/classes Remote starting / stopping of software applications, Polling by data priority level, Broadcast addressing, Multiple data types per message are allowed, Internal Indication field, IID present in response header, Application layer confirms events; use of CON bit is made	Does not give time stamped events. Does not provide polled report by exception, Checksum ensures proper end-to-end communication
Device Addressing	Link address could be 0, 1, 2 bytes, Unbalanced link contains slave address, Balanced link is point to point so link address is optional (may be included for security)	Link contains both source and destination address (both always 16 bits), Application layer does not contain address 32 bit point addresses of each data type per device	Addresses field contains two characters (ASCII mode) or 8 bits (RTU mode), Valid address in range 1-247, Address 0 used for broadcast
Configuration	Baud rate, Device	Baud rate, Device	Baud rate, Mode

Parameters	addresses, Balanced / unbalanced Frame length, Size of link address, Size of ASDU address, Size/structure of point number, Size of cause of transmission	addresses, Fragment size	(ASCII or RTU), Parity mode
Application Specific information model	A few application specific data types available Data objects and messages are not independent to each other	Allows vendor to create application specific extensions Data objects and messages independent to each other	Allows user to create application specific model
Online configuration	En able/ disable communication control objects, Loading configuration, Change report / logging behaviour	Define group of data, Selecting data for responding, Enable/ disable communication control objects, Loading configuration, Change report / logging behaviour	Efficient online configuration could be made by Modbus TCP/IP
Open for other encoding solutions	Not Available	Open for other encoding solutions like XML	Source code in programming languages like C, VC++ & JAVA etc.

Table 4: Comparison of DNP 3.0, IEC 870-5-101 and Modbus

For the intra-cell communications, there is one key feature that must be taken into account: the ability of each solution to do the setup of the HAN automatically. In other words, the ability to be a plug and play solution, allowing the automatic assignment of addresses for all the devices involved and the setup or deletion of devices with no need to stop the network or even disturb it in any way.

3.8 ZigBee Latency and Packet Error Rate Measurements

A series of experiments have been conducted in order to measure the multi-hop latency and Packet Error Rate (PER) in a real ZigBee network. In the experiment we have compared the event-driven and query based methodologies and as expected it has been observed that event-driven methodology of monitoring results in better PER and Latency results. This was also the drawing conclusion in the deliverable D2.3-B Communication protocol Specification.

With the benefit of mesh topology ZigBee nodes could cover large areas and with the route discovery the nodes in the network could substitute the broken down nodes by finding out new routes. But before letting ZigBee nodes to establish their own routes we have forced a two-hop topology as shown in Figure 3-1 by restricting the number of children and routers that can associate to the ZC. The devices were randomly distributed over a 1x2 meters table in an office environment. ST SPEAr600 evaluation board and ZC constituted the CDC in the hardware setup. We have used MC1322X Platform from Freescale with BeeStack ZigBee PRO v3.0.7 stack for the ZigBee nodes.

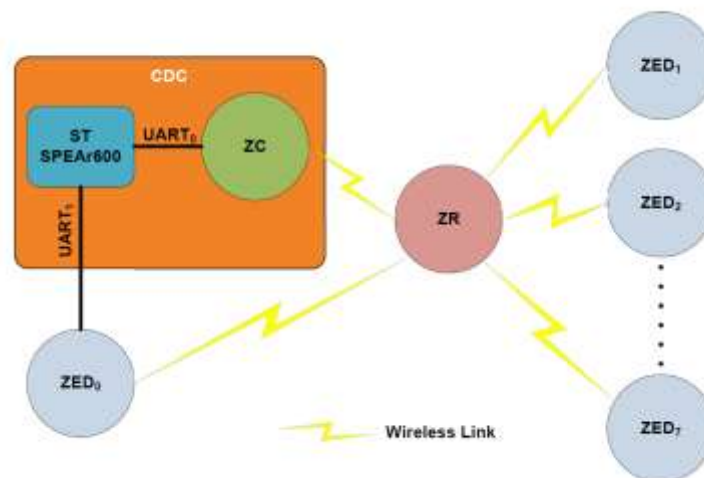


Figure 3-1 Two-Hop Tree Topology

In all the measurements ZC and ZED_0 were present but we have systematically add or remove other nodes in order to change the measurement conditions. ZED_0 and ZC were always connected to the SPEAr600 via UART ports to inform SPEAr600 about the time instances of events. Every measurement initiated by SPEAr600 by sending a command to the ZC. Latency of querying ZED_0 in different conditions and packet loses measured by SPEAr600. During the measurements transmit power was -1dBm

and for all set of measurements we have collected 10000 latency samples. After the two-hop tree topology measurements, furthermore, we have evaluated the latency and PER of a mesh network in WiLaB, University of Bologna (in Figure 3-5) in different query scenarios. In all experiments ZEDs were programmed to have the Smart Metering Cluster. For latency and PER measurements 41 bytes long read attributes commands are sent by the CDC in order to read the "CurrentSummationDelivered" attribute of ZED_0 and as defined in the ZCL, ZED_0 replied the CDC immediately after receiving the commands by sending a 38 bytes long read attributes response packets. In this way, we have obtained the both way latencies and PERs.

3.8.1 Processing Time of the ZR

Before going further with multiple ZED networks we measured the one hop and two-hop latencies between ZC and ZED_0 without any other ZED in the topology in order to provide some insights on the hopping time. In un-slotted CSMA/CA first backoff phase introduces a delay between 0 to $2240\mu s$. This statistically results $1120\mu s$ average delay if there is no competitor for the channel access. Then sensing phase which is $128\mu s$ takes place. Finally, if the channel is found free the packet is sent. The summation of average backoff delay and sensing phases results as $1248\mu s$ which represents the average delay introduced by CSMA/CA denoted as T_c . The packet durations, T_{tx} , for read attributes request and read attributes response were $2496\mu s$ and $2560\mu s$ respectively. In two hops case there was a ZR in between ZC and ZED_0 while in one hop case the connection was direct between ZC and ZED_0 . We have sent 10000 read attributes requests to ZED_0 and it replied with the read attributes response after each request. Following average latencies are found.

	T_{1HOP}	T_{2HOPS}
Request:	$7358\mu s$	$12680\mu s$
Response:	$6179\mu s$	$11370\mu s$

Table 5 Average Latencies

By using the difference between one hop and two hops we can calculate the time needed by ZR to process the packet after receiving it from ZC;

$$T_r = (T_{2HOPS} - T_{1HOP}) - (T_c + T_{tx})$$

Indeed we already know T_c and T_{tx} thus we can evaluate T_r . We have found T_r for request and response as $2826\mu s$ and $2631\mu s$ respectively. Consequently we can state that average time needed by ZR to process the packet is approximately $3ms$ which also includes the acknowledging the ZC.

3.8.2 Synchronized Query

By using the same group address for the ZR and ZEDs we have synchronously queried the ZR and a number of ZEDs in the topology shown in Figure 3-1 whereas we only considered the query, response time and PER between ZED_0 and ZC. Group addressing in ZigBee preserves the bandwidth by using only once the common links of the routes to the destination group members. In the setting, firstly ZC unicasts the read attributes command to ZR and after replying the ZC with read attributes response it forwards the command as a broadcast to all ZEDs. Thus ZEDs in the setup receive the query at the same time and then reply with read attributes responses while competing with each other to access the channel.

In synchronized query measurements ZEDs were always awake. In Figure 3-2 the measurement results are given in box-plots. In the query median value of latency, which is around $34ms$, is independent to the number of ZEDs since query finishes before ZEDs transmit any packet. PER is less than 1% in all the cases. On the other hand for the responses it can be seen clearly the increase on the latency and PER with respect to the number of ZEDs because of increasing amount of competition in the channel access. Median values of latencies are around $11ms$, $17ms$, and $22ms$ with respect to the number of ZEDs. PER is significant when there are three ZEDs. Lastly worth to note that when there is only one ZED (which is ZED_0) the median value of latency is close to $T2HOPS$ for the response in Section 5.1. This was an expected result since both cases are same with the exception of using group addressing.

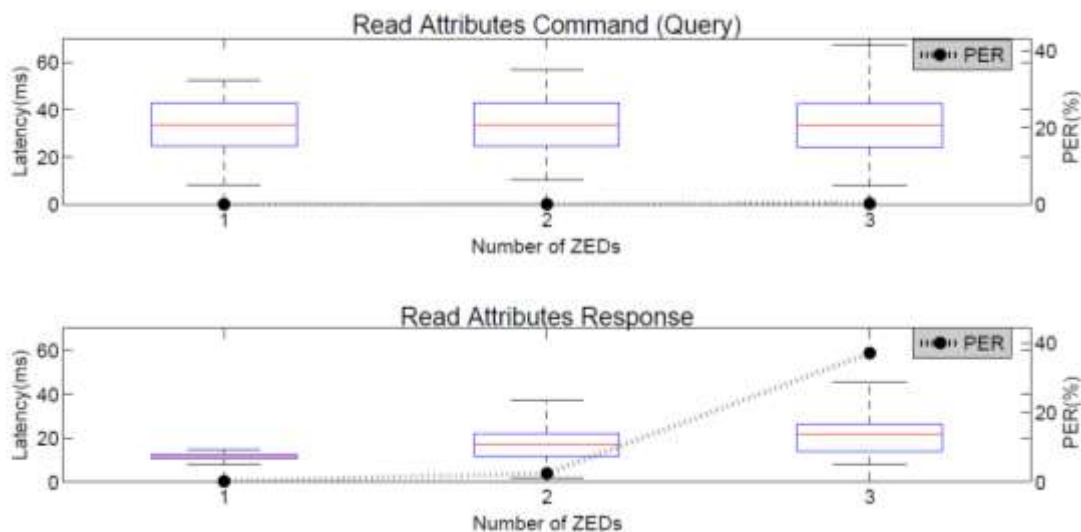


Figure 3-2 Group Query

3.8.3 Periodic Traffic

In periodic traffic measurements, we have configured ZED_1 to ZED_7 in Figure 3-1 as reporting devices therefore they have sent report attributes commands packed with "CurrentSummationDelivered" attribute to the ZC over ZR. ZEDs asynchronously reported this attribute and we have set two different reporting intervals as 3 seconds and 200 milliseconds to change the traffic density in the network. The length of the report attributes command was 45 bytes. In such periodic traffic conditions we have continuously queried ZED_0 with read attributes commands. ZED_0 was a sleeping device and the default parameter for pooling was 3s but if there is a continuous data stream to the direction of a ZED, ZigBee specifications states that the device may temporarily increase its polling rate and shall ensure that it polls its parent at least once every macTransactionPersistenceTime seconds. In our ZED_0 default fast polling interval was 200ms.

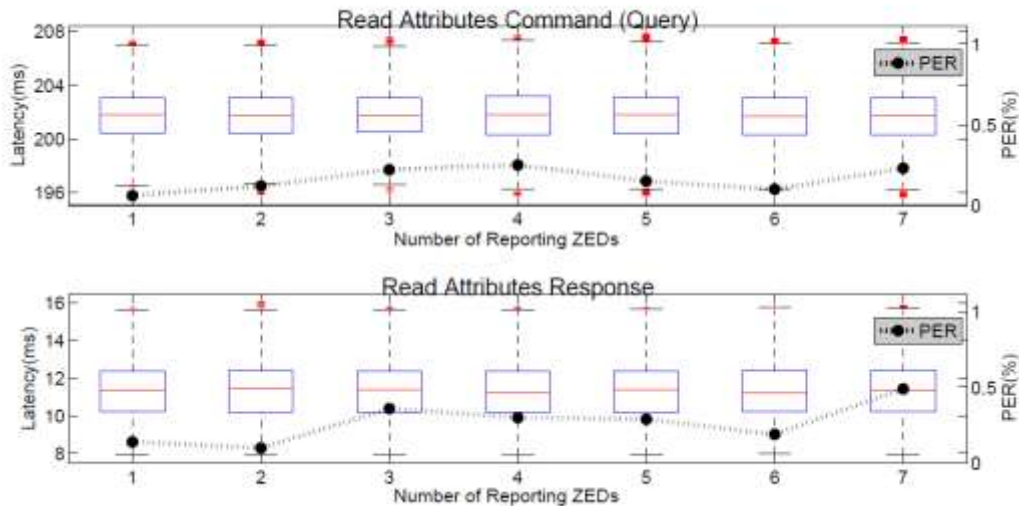


Figure 3-3 Query in Periodic Reporting ($\Delta T = 3s$)

The results for 3s and 200ms reporting intervals are shown in Figure 3-3 and Figure 3-4. In Figure 3-4 box-plots for different number of reporting ZEDs are all similar and PER values in all cases are less than 1%. Query is around 202ms which is highly dependent to the fast polling interval and response is like synchronized query case close to $T2HOPS$ value in Section 5.1. This means 3 seconds reporting interval is large enough not to impose any limitations on querying the ZED_0 . Thus we have increased the frequency of reporting by setting reporting interval to 200ms which is equal to fast polling interval of ZED_0 and obtained the results shown in Figure 3-4. Median values on the box-plots are similar to Figure 3-3 both for query and response but the increasing number of reporting ZEDs clearly populates the number of outliers in the box-plots by increasing the variance of latency. PER is less than 1% up to four

reporting ZEDs however the beginning of an upward trend, that starts at two reporting ZEDs, can be seen in both query and response.

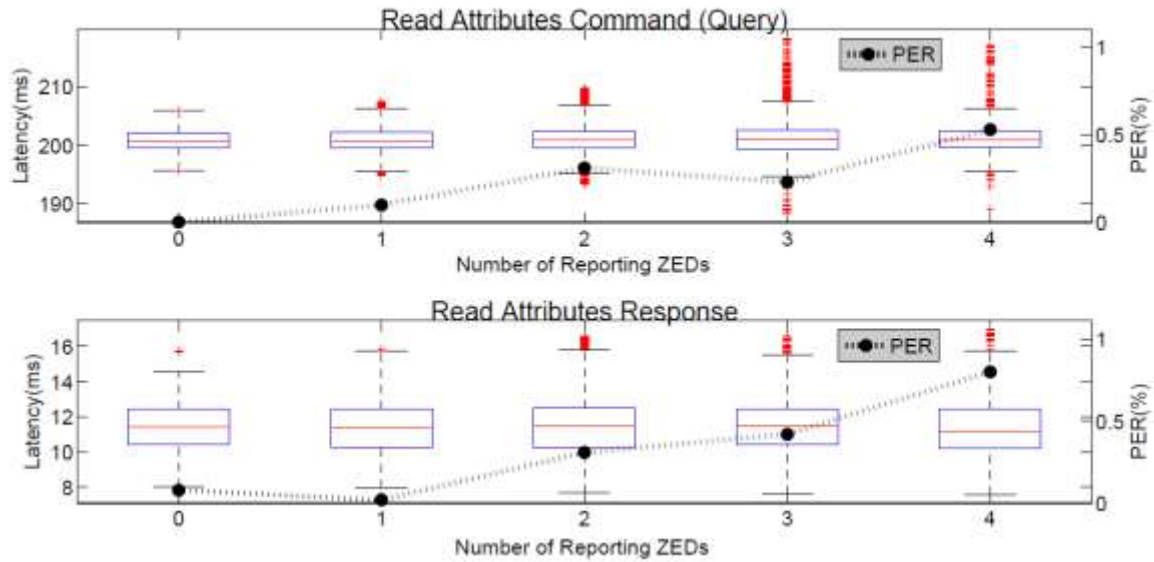


Figure 3-4 Query in Periodic Reporting ($\Delta T = 200ms$)

3.8.4 Measurements in an Office

After two-hop tree topology measurements we have distributed the ZigBee devices in WiLab at University of Bologna without any restriction on the topology and they have formed a mesh network with 1 ZC, 6 ZRs and 8 ZEDs. The locations of nodes and an instance of routes we have observed during the measurements with a sniffer is shown in Figure 3-5.

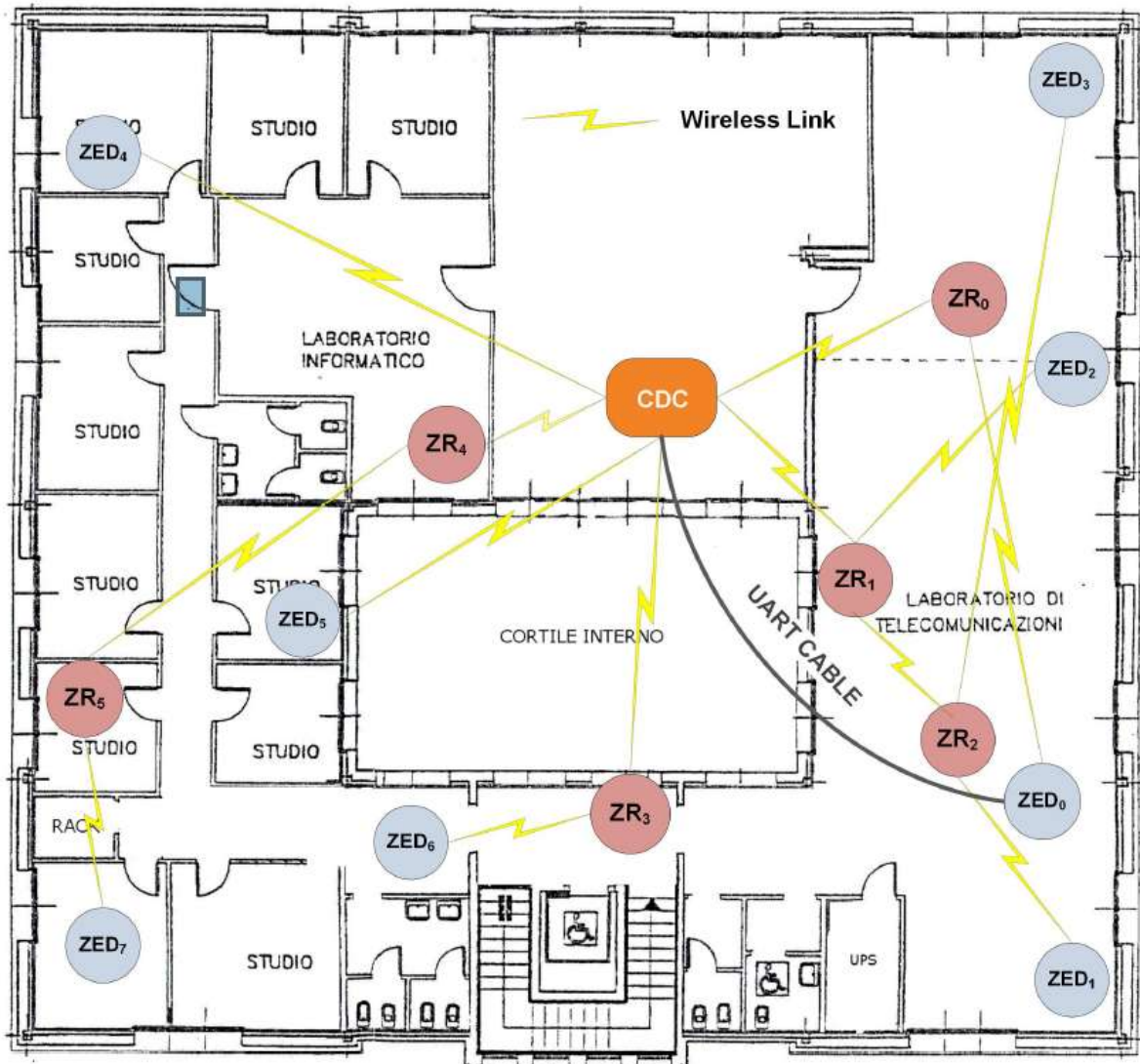


Figure 3-5 An Instance of Mesh Routes

Similar to the previous measurements we have measured the latency in two different settings; first we have set ZED_1 to ZED_7 as reporting devices and queried sleeping ZED_0 later on we have turned off the reporting in ZEDs and converted ZED_0 to a non-sleeping device. Then, assigned the same group address to ZR_0 , ZR_1 , ZR_2 , ZED_0 , ZED_1 , and ZED_2 and queried all. As previously mentioned latency and PER measurements were always between ZC and ZED_0 and in mesh case we have never witnessed more than two hops between them. The results are shown in Figure 3-6.

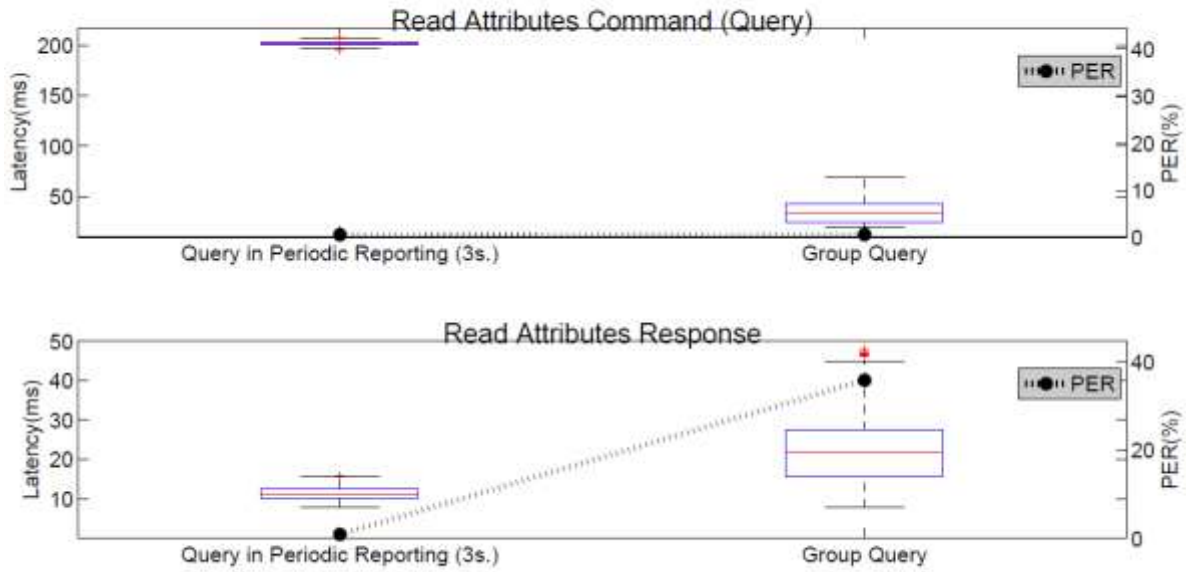


Figure 3-6 Mesh Measurements

In periodic reporting case, median value of query and response latencies are around 202ms and 12ms respectively. These results are close to the results in Figure 3-4. In group query, median value of the query is around 34ms and the median value of response is around 22ms which are close to the results of 3 ZEDs in Figure 3-3. PER in the response of group query is significant

Consequently, in all measurements except the group query with 3 ZEDs we have observed PER less than 1% and response latency was always less than 50ms. One of the important outcome of the measurements was observing the PER bottleneck in group query with 3 ZEDs in both mesh and three topologies. In the measurements we have focused on monitoring applications and for monitoring applications instead of querying a group of three or more nodes, configuring a periodic reporting mechanism is clearly should be the way to be followed.

4. Conclusion

It was initially proposed that DLMS, SML, M-Bus are used for inter-cell communication middleware to ensure required flexibility and openness for interfacing towards third party and eDIANA framework compliant components as well as to address the security requirements. In addition to that it was proposed that the eDIANA framework shall be able to connect to a variety of CDCs via MCC. The MCCs themselves shall serve via iEi as main interconnect for all inter-cell CMM, CCA and CGS. M-Bus protocol EN13757-3 would have been ported on top of ZigBee.

M-Bus EN13757-3 (M-Bus+ as planned future revision of the EN13757-3, DLMS/COSEM (Device Language Message Specification / Companion Specification for Energy) IEC 62056 / EN13737-1/SML+ and DLMS-UA or SML have been firstly proposed as application protocols to be applied in both iEi communication as alternative software solutions. These protocols transport the related OBIS-number together with each data point. OBIS (Object Identification System) EN 62056-61:2002 and EN 13757-1 coded COSEM or SML data may also be carried via M-Bus. To provide confidentiality of CMM, CCA and CGS data these should be encrypted. Encryption should be done at M-Bus protocol communication.

However the proposal using M-Bus, DLMS and SML as basis for middleware layer to ensure broadest possible interoperability connecting external devices and external networks with the eDiana framework and the implementation of the M-Bus stack prototype as open source has not been pursued.

It was agreed that T3.6 defines the inter-cell communication middleware and provides a middleware protocol prototype (incl. legacy device support requested by reviewers at 1st annual meeting) accordingly. Due to the fact that Zigbee/ IEEE 802.15.4 has been chosen as the main wireless communication protocol for the eDIANA intra-cell communication major parts of the necessary middleware communication prototype has to be compliant to Zigbee's application profiles and will be used from that. Wired communication in the intra-cell will be done via HomePlug and or Ethernet.

Acknowledgements

The eDIANA Consortium would like to acknowledge the financial support of the European Commission and National Public Authorities from Spain, Netherlands, Germany, Finland and Italy under the ARTEMIS Joint Technology Initiative.

References

- [1] eDIANA project, "D2.1-B: eDIANA Reference Architecture", February 2010
- [2] eDIANA project, "D2.3-A: Network topology and communications architecture definition", February 2010
- [3] eDIANA project, "D3.1-A: Cell Level Monitoring and Metering System. Design and Development of Power Consumption Sensor", April 2010
- [4] eDIANA project, "D3.2-A: Intelligent Embedded Interface (iEi) – Concept Release", April 2010
- [5] A. Ankou, G.Romero, A. Muñoz, G. Mauri, D. Moneta, W. Liu, J. Wikiera, G. Kmethy, G. Alberdi, A. Pajot, A. Gómez, C. Rodríguez, G. Fantini, I. Berganza, D. Gutschow, C. Rahm, N. DiPaola, A. Lasciandare, A. Moscatelli, M. Bauer, M. Sigle, A. Arzuaga, L. Marrón, X. Bilbao: "OPEN METER: Design of the overall architecture", version 1.1, February 2010. "OPEN METER. Energy Project No. 226369. Funded by EC".
- [6] M.Tech. Credit Seminar Report, Electronics Systems Group, EE Dept, IIT Bombay, 2003, Comparison of protocols used in remote monitoring: DNP 3.0, IEC 870-5-101 & Modbus Jay Makhija
- [7] Open Metering System Specification, Volume 1, General Part, Issue 1.2.0 / 2009-07-17
- [8] Open Metering System Specification, Volume 2, Primary Communication, Issue 2.0.0 / 2009-07-20 Release
- [9] Multifunctional electricity meters <http://www.e-meter.net/index.php?tt=firm>
- [10] ModBus protocol specification <http://www.modbus.org/specs.php>
- [11] MODBUS/TCP to MODBUS/RTU gateway server <http://mbus.sourceforge.net/>
- [12] Mbus Software C++, C, Java <http://www.mbus.org/sw.html>
- [13] Wireless M-Bus protocol software
<http://focus.ti.com/docs/toolsw/folders/print/wmbus.html>
- [14] Wireless M-Bus
<http://www.radiocrafts.com/index.php?sideID=429&ledd1=330>
- [15] Wireless M-Bus and ZigBee®- enabled GSM/GPRS/ EDGE gateway for smart metering <http://www.metering.com/node/13550>