Large Scale Integrating Project

EXALTED

Expanding LTE for Devices

FP7 Contract Number: 258512

WP2 – Business Models, Use cases & Technical Requirements

D2.1
Description of baseline reference systems, scenarios, technical requirements & evaluation methodology

Contractual Date of Delivery to the CEC:	31 May 2011
Actual Date of Delivery to the CEC:	31 May 2011
Responsible Beneficiary:	TKS
Contributing Beneficiaries:	ALUD, EYU, GTO, SC, TKS, TST, UNIS, UPRC, VID
Estimated Person Months:	12
Security:	Public
Nature	Report
Version:	2.0

Document Information

Document ID: D2.1_REVISED_FINAL.doc
Version Date: 30 January 2012
Total Number of Pages: 76

Abstract This is the first deliverable of EXALTED project, which defines technical requirements and high-level architecture for LTE-M, and gives an overview of EXALTED use cases and baseline reference systems. Guidelines for evaluation and assessment methodology are also described.

Keywords assessment, evaluation, LTE-M, M2M, reference system, requirements

Authors

Name	Organisation	Email
Nemanja Ognjanovic (editor)	TKS	nemanjao@telekom.rs
Gorica Nikolic	TKS	gorican@telekom.rs
Bojana Jakovljevic	TKS	bojanaja@telekom.rs
Katarina Sekeljic	TKS	katarinas@telekom.rs
Angeliki Alexiou	UPRC	alexiou@unipi.gr
Athanasios Lioumpas	UPRC	lioumpas@unipi.gr
Djelal Raouf	SC	djelal.raouf@sagemcom.com
Bruno Corlay	SC	bruno.corlay@sagemcom.com
Piraba Navaratnam	UNIS	p.navaratnam@surrey.ac.uk
Stephan Saur	ALUD	stephan.saur@alcatel-lucent.com
Alexandru Petrescu	CEA	alexandru.petrescu@cea.fr
Srdjan Krco	EYU	srdjan.krco@ericsson.com
Boris Akrapovic	EYU	boris.akrapovic@ericsson.com
Christian Ibars	CTTC	christian.ibars@cttc.cat
Jesús Alonso-Zárate	CTTC	jesus.alonso@cttc.es
Juan Rico	TST	jrico@tst-sistemas.es
Javier Valiño	TST	jvalino@tst-sistemas.es
Eleftheria S. Vellidou	VID	projects@vidavo.gr

Approvals

	Name	Organisation	Date	Visa
Internal Reviewer 1	Serdar Vural	UNIS	27/05/2011	OK
Internal Reviewer 2	Walter Nitzold	TUD	27/05/2011	OK
Technical Manager	Pirabakaran Navaratnam	UNIS	27/05/2011	OK
Project Manager	Djelal Raouf	SC	27/05/2011	

Executive Summary

This first public deliverable of EXALTED project defines a baseline system design and an evaluation methodology for other WPs as well as for the future implementation of LTE-M. The main concept of LTE-M describes a hybrid architecture, which consists of a core transport network that is backward compatible with LTE, and of capillary networks, such as WiFi or ZigBee. End-devices establish end-to-end (E2E) communication via gateways, which have at least two interfaces – one towards an LTE-M base station, and one for communicating with devices in a capillary network.

Among many possible implementations of M2M communication technologies, the following three scenarios are chosen as the most significant and illustrative examples for the purpose of EXALTED:

- Intelligent Transport System (ITS) – communication of vehicles and transport infrastructure with ITS application servers, which controls parameters such as transportation time, traffic collision avoidance, on-board safety, fuel consumption, and many others.
- Smart Metering and Monitoring (SMM) – very applicable use case of industrial, environmental, energy, and other types of monitoring.
- E-healthcare – a relationship between a healthcare organization and a patient, established through the M2M communication.

Technical system requirements for LTE-M are identified based on the analysis of the described scenarios. The system requirements are given in a consolidated manner, in order to ensure an effective end-to-end (E2E) system description, with references to particular scenarios that they can be applied to. The requirements are grouped into several categories:

- Functional – features of LTE-M functional elements.
- Service – M2M services offered through LTE-M.
- Network – requirements regarding network infrastructure.
- Non-functional – quality features of LTE-M system.
- Device – characteristics of end-devices, cluster-heads and gateways.

The baseline reference systems for LTE-M are GPRS/GSM and LTE as cellular network technologies, and WiFi and ZigBee as capillary networks. The disadvantages of these existing systems led us to work on a new LTE-M system that is designed to co-exist with LTE. For instance, LTE can serve for high data rate transmissions, while GPRS/GSM is not applicable in any scenario.

Some guidelines for evaluation and assessment methodology are also presented in this document, and any further development in WP2 is thus expected to follow those guidelines for the sake of consistency and comparability.

Table of Contents

1. Introduction

The concept of Machine-to-Machine (M2M) communications fits into the new trend of everyday devices' connectivity to the Internet and creation of a large network of machines. On the other hand, interoperability of M2M communications with the core networking technologies needs to be developed and eventually standardized. Some guidelines are given for particular aspects of this technology, such as ETSI's TS 102.689 [1], but the lack of an overall and consolidated approach to the definition of an end-to-end (E2E) system concept motivated EXALTED's initiative for introducing a combined "LTE - M2M" hybrid architecture. The main purpose of deliverable D2.1 is the high-level definition of this architecture.

This deliverable has an important purpose within the EXALTED project – it serves as a description of the baseline LTE-M system concept. It also contains a set of relevant technical requirements aimed to be referred to in not only other WPs of EXALTED, but also in the later implementation of LTE-M.

Use cases of M2M services and applications that are of interest are identified in Section 2 of D2.1. The emerging M2M services are expected to serve many business areas, and for the purposes of EXALTED the following services are recognized as the most relevant ones: Intelligent Transport Systems (ITS) in the automotive industry, Smart Metering and Monitoring (SMM) solutions in the energy efficiency markets, and health monitoring over Internet (E-healthcare) in smart homes. The scenarios are described with focus on their key features, and technical requirements are derived from them.

The core part of this deliverable is Section 3 that contains a set of technical requirements for LTE-M system and M2M devices. Based on the standardization bodies' point of view through the EXALTED prism, the technical requirements are extracted. These requirements serve as the baseline for the development of EXALTED system framework and components. The presentation of requirements is standardised for ease of use and cross-referencing in other sections and documents. Requirements are grouped into several sub-sections, and the reference to particular use cases is given for each requirement.

Section 4 gives an overview of relevant reference systems: GSM/GPRS, LTE, WiFi and ZigBee. They are described briefly for the purpose of comparison with LTE-M. The section offers an insight into the disadvantages of current systems for the purpose of M2M communication, which led us to invention of a new system (i.e. LTE-M).

The high-level system architecture for the hybrid LTE-M2M concept is outlined in Section 5. Types of nodes, elements, and the communication between them in LTE-M are presented through descriptive figures and explanations. Other WPs and future works and implementations in this area within the project should follow the initial concept defined in this document.

Finally, Section 6 gives an introduction to future evaluation and assessment methodologies for implementation of LTE-M by operators. It is done in a concise way for the purpose of this document, but further development is expected in WP2.

2. Scenarios Description

The field of possible applications for M2M communications is extremely wide, and covers almost all business areas. In EXALTED, three main scenarios are examined, namely Intelligent Transport System, Smart Metering and Monitoring and E-healthcare. Each scenario comprises several use cases, which are thoroughly described in this Section, along with their key features. The investigation of these features, many of which are common among the scenarios, indicates that the evolvement of a unified architecture for M2M applications is possible, consolidating the EXALTED's vision.

The selection of specific scenarios, which serves as a common platform for a focused investigation of the technical requirements of the EXALTED vision, was based on the following:

- The market's segmentation, forecasts and opportunities, as described by several researches.
- The technology roadmap (standardization and industrial). The investigation of the specifications groups', consortiums' and other stakeholders' multi-year activities on M2M, is taken into account towards a possible contribution of EXALTED to standardization bodies.
- The necessity for a LTE-based deployment of M2M communications.
- The completeness of the scenarios, in terms of providing fully functional M2M services.
- The diversity of requirements and challenges.
- The suitability of scenarios to highlight the key benefits of the EXALTED concept.

2.1 ETSI and 3GPP activities on M2M use cases and scenarios

2.1.1 Scope of standardization activities on the use cases and scenarios

The scope of the use cases and requirements activities within the standardization bodies is to provide those requirements that will enable consistent, cost-effective, communication **for wide-range ubiquitous M2M applications**. Specific use cases are presented as examples of the applicability and sufficiency of those particular requirements [1].

Since, one of the main goals in EXALTED is to contribute to the existing M2M standardization activities, the project is soundly based on those requirements proposed by ETSI & 3GPP, aiming at enriching those requirements and making them more consistent with the EXALTED vision, i.e. to support M2M applications through the LTE cellular network.

The primary reason for following this approach is that the uses cases identified and specified by ETSI & 3GPP is based on valid investigations on real-world applications, market needs and European activities. For example the smart metering use case investigated by ETSI [2] is based on the following activities:

a. *European Commission Standardisation Mandate M/441: "Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability* [3].

b. *Directive 2006/32/EC of the European Parliament and of the Council of 5 April 2006 on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC, published in the Official Journal of the European Union as OJ L 114 of 27.4.2006* [4].

c. *An ENA (energy networks association) project, which is focused on ensuring that the requirements of energy networks – in respect of the short, medium and longer term functionality required of smart metering, and associated communication infrastructure - are clearly defined and aligned with work being undertaken by the DECC/Ofgem E-Serve Smart Metering Implementation Project* [5].

In this way, by ensuring a full alignment with the standardization bodies activities, the possibility that the enriched EXALTED requirements lead to impractical implementations and concepts, is eliminated.

2.1.2 ETSI identified use cases

ETSI towards specifying the general and functional requirements for M2M communication services has taken into account the following use cases (Table 2.1):

Table 2.1: ETSI use cases [1], [2].

ETSI use cases	Sub use cases
Smart meters	• Obtain Meter Reading Data
	• Install, Configure & Maintain the Smart Metering
	• Support Prepayment Functionality
	• Monitor Power Quality Data
	• Manage Outage Data
	• Facilitate Demand Response Actions
	• Facilitate Distributed Generation Actions
	• Manage the Distribution Network using Smart
	Manage Interference and Malfunctions to the Smart
	• Manage Tariff Settings on the Smart Metering
	• Enable & Disable the Smart Metering Information
	• Interact with Devices at the Premise
	• Manage Efficiency Measures at the Premise using
	• Display Messages
E-Health	• Remote Patient Monitoring (RPM)
	• Patient – Provider Secure Messaging
	• Measurement of Very Low Voltage Body Signals
	• Telecare data traffic between home and remote
Track and Trace	
Monitoring	
Transactions	
Control	
Home automation	
City automation	
Connected consumer	
Automotive use case	• Cooperative traffic • efficiency • Tracking & Tracing • Co-operative local services • Global internet services

2.1.3 3GPP identified use cases

In a similar way 3GPP, has identified the following use cases (Table 2.2):

Table 2.2: 3GPP use cases [8].

3GPP use cases	Sub use cases
Security	Alarm systems, Backup for landline, Access control, Car/driver security
Tracking & Tracing	Fleet Management, Order Management, Pay as you drive, Asset Tracking, Navigation, Traffic information, Road tolling, Traffic optimisation/steering
Payment	Point of sales, Vending machines, Loyalty concepts, Gaming machines
Health	Monitoring vital signs, Supporting the aged or handicapped, Web Access Telemedicine points, Remote diagnostics
Remote Maintenance/Control	PLCs, Sensors, Lighting, Pumps, Valves, Elevator control, Vending machine control, Vehicle diagnostics
Metering	Power, Gas, Water, Heating, Grid control, Industrial metering

Again, the scope of 3GPP is to **identify and specify general requirements for machine type communications**, identify service aspects where network improvements and finally specify machine type communication requirements for these service aspects [6][7][8].

2.1.4 Use cases Analysis and requirements

2.1.4.1 Smart Metering and monitoring

2.1.4.1.1 ETSI activities

For each of the smart meters sub use case, ETSI has defined:

a. a general use case description
b. the possible stakeholders
c. the scenario case description
d. potential new requirements
e. the use case source

Considering the smart use cases, ETSI was based on [5] and the detailed scenarios described therein, in order to derive possible new requirements for M2M communications. A summary of those requirements can be found in Table 2.3.

Table 2.3: ETSI requirements for smart meters [2].

Use cases	Requirements
Obtain Meter Reading Data	• On demand readings with minimal delay • Accurate and secure time synchronization • Applications define periodic reporting • Receiving unsolicited or scheduled information • Authentication via Gateway or directly • Security should not prevent regulatory requirements • E2E data verification
Install, Configure & Maintain the Smart Metering Information System	• M2M Devices or M2M Gateways should be monitored proactively in order to attempt to prevent and correct errors • The M2M System should support auto-configuration functions • Accurate and secure time synchronization • Secure software and firmware provisioning • Configuration management • Subscription management • Capability to remotely change the state of a M2M Device • Simple and scalable provisioning of M2M Devices • Support autoconfiguration, that is without human intervention • Authentication via Gateway or directly • Security should not prevent regulatory requirements • E2E data verification
Support Prepayment Functionality	• Static information such M2M capabilities may be assigned to M2M Devices and Gateways • Support autoconfiguration, that is without human intervention • Accurate and secure time synchronization • Support autoconfiguration, that is without human intervention • Authentication via Gateway or directly • Security should not prevent regulatory requirements • Mechanisms required for secured and traceable compensation and micro-compensation • Applications define periodic reporting • Capability to remotely change the state of a M2M Device • Receiving unsolicited or scheduled information • Operating particular algorithms for retrieving information • Authentication via Gateway or directly • Security should not prevent regulatory requirements • E2E data verification • Support a mechanism for device integrity validation
Monitor Power Quality Data	• Accurate and secure time synchronization • Applications define periodic reporting

	• Receiving unsolicited or scheduled information • Authentication via Gateway or directly • Security should not prevent regulatory requirements • E2E data verification • Mutual authentication and authorization between the end-user and the application • M2M devices that require device integrity validation should provide a trusted execution environment
Manage Outage Data	• Accurate and secure time synchronization • Applications define periodic reporting • Receiving unsolicited or scheduled information • An object may be able to communicate in a peer-to-peer manner with any other connected object • Authentication via Gateway or directly • Security should not prevent regulatory requirements • E2E data verification • Mutual authentication and authorization between the end-user and the application • M2M devices that require device integrity validation should provide a trusted execution environment
Facilitate Demand Response Actions Facilitate Distributed Generation Actions Manage the Distribution Network using Smart Metering Information System Data Manage Interference and Malfunctions to the Smart Metering Information System	• Accurate and secure time synchronization • Capability to remotely change the state of a M2M Device • Applications define periodic reporting • Receiving unsolicited or scheduled information • An object may be able to communicate in a peer-to-peer manner with any other connected object • Authentication via Gateway or directly • Security should not prevent regulatory requirements • E2E data verification • Mutual authentication and authorization between the end-user and the application M2M devices that require device integrity validation should provide a trusted execution environment

The main actors of the smart metering case are depicted inFigure 2.1, as well as the contribution of the EXALTED project.

2.1.4.1.2 3GPP activities

In contrast with ETSI, 3GPP is not aiming at investigating in details each use case, but to identify and specify general requirements for machine type communications and not only applicable to a limited number of cases.

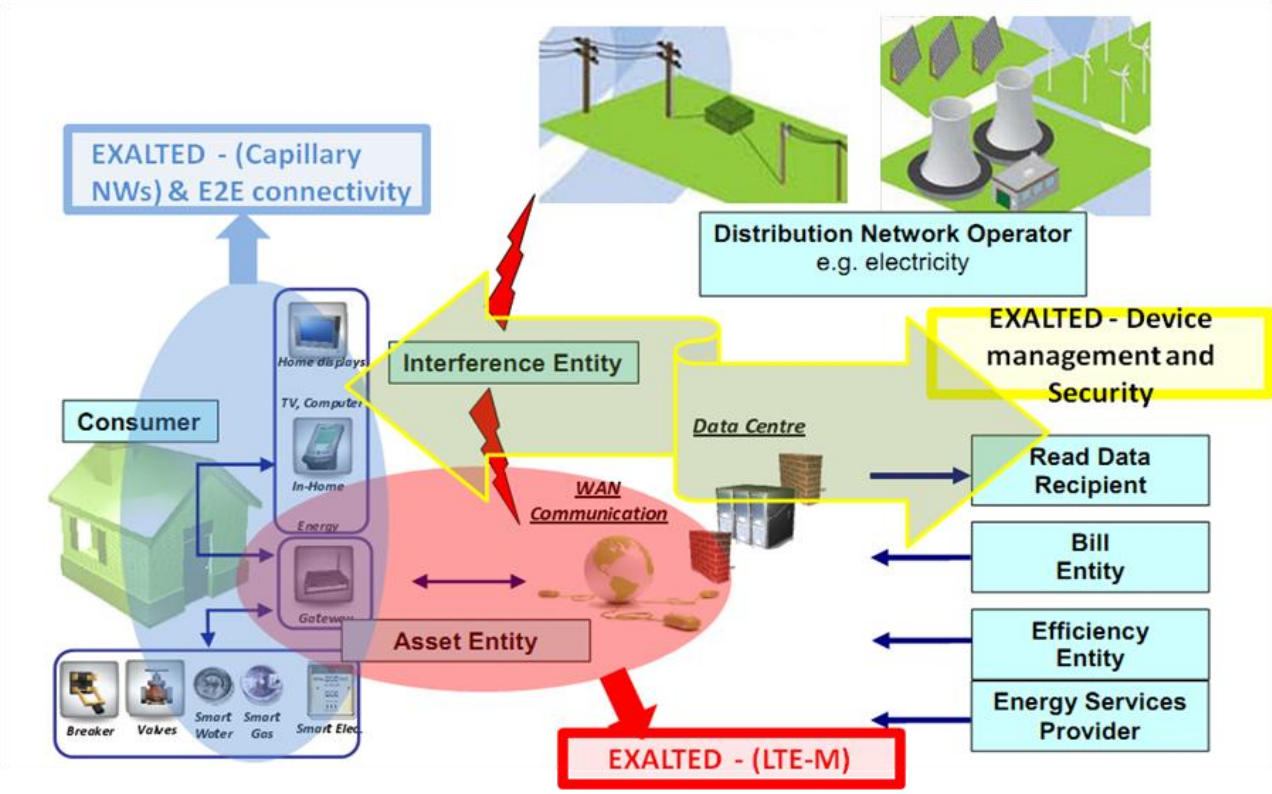

Figure 2.1: Actors of a Smart Metering Information System [2] and the contribution of EXALTED.

2.1.4.2 Intelligent Transport Systems

2.1.4.2.1 ETSI activities

Regarding the ITS use case, the activities within ETSI can be found in [9], [10], [11], [12], [13], [14]. The main ITS use cases may be found in Table 2.4.

Table 2.4: ETSI ITS use cases [16].

ETSI ITS application class	use case
Cooperative traffic efficiency	• Emergency vehicle warning • Slow vehicle indication • Intersection collision warning • Motorcycle approaching indication • Driving assistance - Road • Hazard Warning • Emergency electronic brake lights • Wrong way driving warning • Stationary vehicle - accident

	• Stationary vehicle - vehicle problem • Traffic condition warning • Signal violation warning • Roadwork warning • Collision risk warning • Decentralized floating car data - Hazardous location • Decentralized floating car data - Precipitations • Decentralized floating car data - Road adhesion • Decentralized floating car data - Visibility • Decentralized floating car data - Wind
Tracking & Tracing	• Regulatory / contextual speed limits notification • Traffic light optimal speed advisory • Traffic information and recommended itinerary • Enhanced route guidance and navigation • Limited access warning and detour notification • In-vehicle signage
Co-operative local services	• Point of Interest notification • Automatic access control and parking management • ITS local electronic commerce • Media downloading
Global internet services	• Insurance and financial services • Fleet management • Vehicle software / data provisioning and update • Vehicle and RSU data calibration

The selection of the ITS use cases were extracted based on several requirements, such as strategic, economical, system capabilities organizational, legal standardization requirements. For each sub case, the main technical requirements are summarized in Table 2.5.

Table 2.5: requirements for ITS [16].

Use cases	Requirements
Emergency electronic brake lights	• Capability for a vehicle, from the emergency electronic brake lights activation, to broadcast in V2X decentralized environmental notification messages. • Capability for concerned vehicles to receive and process V2X decentralized environmental notification messages. • Minimum frequency of the periodic message: 10 Hz • Critical time (latency time less than 100 ms)
Safety function out of normal condition warning	• Capability for a vehicle to detect a safety function being out of its normal condition and then to broadcast in V2X decentralized environmental notification messages. • Capability for all crossed vehicles and road side units to receive and process V2X decentralized environmental notification messages. • Minimum frequency of the periodic message: 1 Hz • Critical time (latency time less than 100 ms)
Emergency vehicle warning	• Capability for an emergency vehicle to broadcast V2X co-operative awareness messages with relevant

	emergency signs being activated. • Capability for all vehicles and relevant road side units to receive and process V2X co-operative awarenessmessages. • Minimum frequency of V2X co-operative awareness messages issued by the emergency vehicle: 10 Hz. • Critical time requirement: Latency time less than 100 ms. • Specific use case security requirement: protection and authentication of the CAM message.
Vulnerable road user Warning	• Capability for a human equipped with relevant device or for a road side unit equipped with relevant system to broadcast I2V co-operative awareness messages providing information on the presence, trajectory and speed of a vulnerable road user. • Capability for concerned vehicles to receive, decode, and process I2V co-operative awareness messages and provide warnings to driver to avoid collision with the vulnerable road user. • Maximum latency time: 100 ms. • Minimum CAMs frequency of the vulnerable user: 1 Hz.
Traffic condition warning	• Capability for a vehicle, from detecting a traffic jam, to broadcast/geocast in V2X decentralized environmental notification messages the traffic jam notification. • Capability for concerned vehicles to receive and process the V2X decentralized environmental notification messages. • Capabilities for all vehicles crossing the car signalling a traffic jam to store and forward received V2X decentralized environmental notification messages according to their geocasting parameters. • Minimum frequency of the periodic message: 1 Hz
Wrong way driving warning	• Capability for a vehicle, to detect that it is driven in a wrong way and to broadcast in V2X decentralized environmental notification messages its current "wrong way heading" status. • Capability for concerned vehicles to receive and process V2X decentralized environmental notification messages. • Minimum frequency of the periodic message: 10 Hz. • Critical time (latency time less than 100 ms).

Signal violation warning	• Capability for a road side unit to broadcast (upon reception of a V2X co-operative awareness message) V2X decentralized environmental notification messages indicating signal violation to all surrounding vehicles. • Capability for a concerned vehicle to receive and process V2X decentralized environmental notification messages and to provide warning to drivers according to the collision risk level. • Minimum frequency of C2X decentralized environmental notification messages: 10 Hz. • Maximum latency time: 100 ms.
Decentralized floating car data	• Capability for a vehicle, from detecting a local danger or event (fog, heavy rain, slippery road heavy wind, traffic jam, etc.), to broadcast/geocast in V2X decentralized environmental notification messages the local danger notification. • Capability for concerned vehicles (on the same road, and same heading of the cars having detected a traffic jam) to receive and process the V2X decentralized environmental notification messages. • Capabilities for all vehicles crossing the car signalling traffic jam to store and forward received decentralized environmental notification messages according to their geocasting parameters. • Minimum frequency of the periodic message: 1 Hz to 10 Hz according to considered event.
Across traffic turn collision risk warning	• Capability for a vehicle which will be turning left to broadcast its status in V2X co-operative awareness messages. • Capabilities for concerned vehicles to receive and process V2X co-operative awareness messages. • Road side unit to be installed if line of sight between vehicles is obstructed. RSU needs to be capable to relay signal or to detect and signal a collision risk. • Minimum frequency of the CAMs: 10 Hz. • Maximum latency time: 100 ms.
Regulatory/contextual speed limits	• Capability for a road side unit to gather regulatory/contextual speed limits and to broadcastthem periodically in I2V co-operative awareness messages. • Capability for a vehicle to receive and process I2V co-operative awareness messages containing regulatory/contextual speed limits. • Minimum frequency of the periodic message: 1 Hz to 10 Hz according to used broadcasting technology.

Along with these high level requirements, ETSI has extracted some functional requirements per sub case (see Table 2.6 for an example on emergency electronic brake lights).

Table 2.6: ETSI functional requirements for ITS sub case [12].

[FR_UC005_001]	Unique use case identifier shall be defined for this use case.
[FR_UC005_002]	Unique event identifier shall be assigned to the "emergency electronic brake lights" event.
[FR_UC005_003_VS]	The vehicle ITS station shall have access to the in vehicle system to detect the "emergency electronic brake lights" event. This shall be at least the emergency brake light and the vehicle brake status.
[FR_UC005_004_VS]	The vehicle ITS stations shall be able to verify whether the "emergency electronic brake lights" event may be a risk to other vehicles.
[FR_UC005_005_VS]	If an ITS station detects an "emergency electronic brake lights" event, the corresponding RHW application shall be triggered.
[FR_UC005_006_VS]	The corresponding RHW application shall request to construct and transmit an "emergency electronic brake lights" DENM.

In Figure 2.2 a simplified view of an ITS environment is depicted along with the EXALTED contribution.

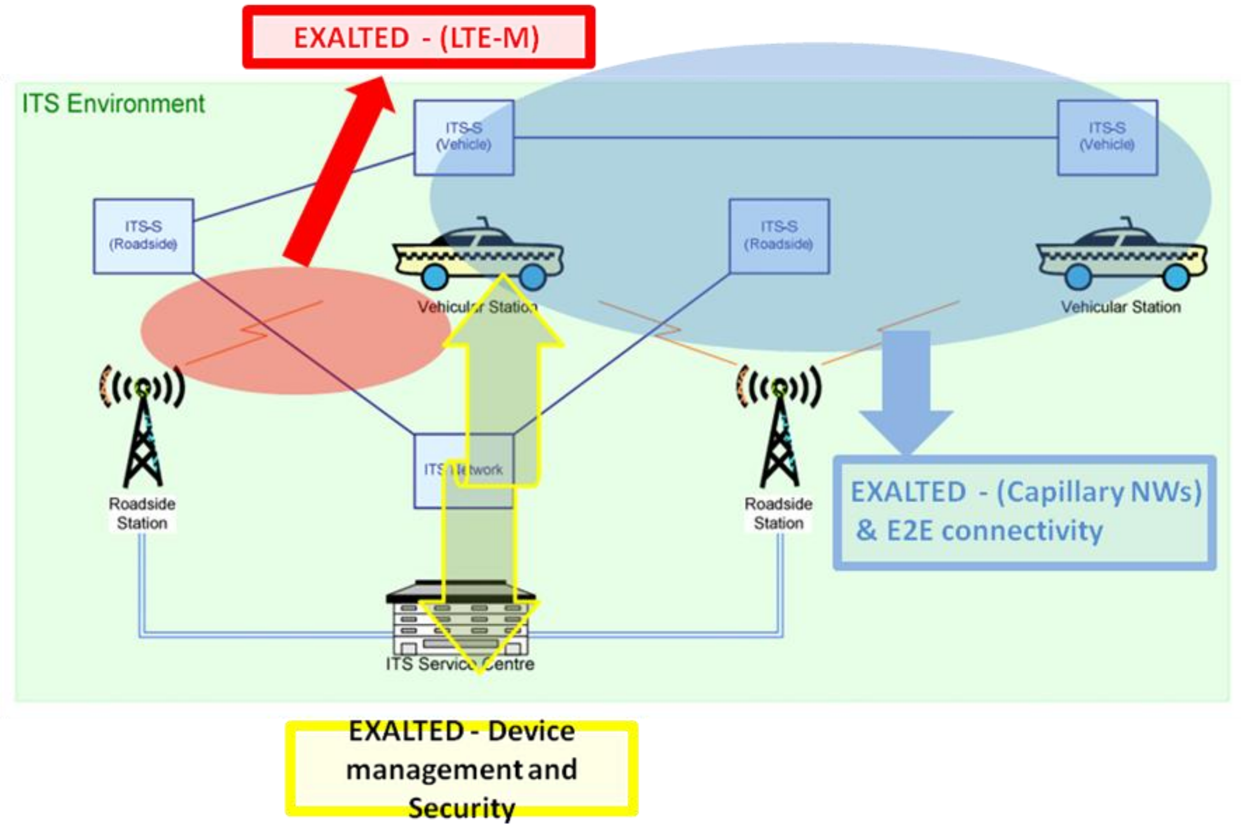

Figure 2.2: A simplified view of an ITS environment and the EXALTED contribution [14].

2.1.4.2.2 3GPP activities

The 3GPP activities on ITS (as in other use cases) are limited to the general concept of the Public Transport Information Broadcast Service, which is a service that provides information of public transport (e.g. current bus location, passenger boarding state, estimated arrival time) to mobile users [15]. However, no specific requirements are identified for this use case.

2.1.4.3 Smart Metering and monitoring

2.1.4.3.1 ETSI activities

ETSI is working on the M2M E-health applications and has published a draft document related to specific application, use cases and possible new requirements. This information id summarized in Table 2.5.

Table 2.7: ETSI use cases and requirements [1], [2].

ETSI E-health use cases	Requirements
Remote Patient Monitoring (RPM)	•Integrity validation based on a trusted execution environment •Alarm signalling to indicate initialization failure •Support for secure storage of sensitive data •Support for secure communication via a secure protocol •Support for time critical message handling and delivery •Support for secure time synchronization •Support for ordered message delivery based on prioritized service handling •Support for priority communication to time-sensitive health services
Patient – Provider Secure Messaging	•Updates to Security Protocols •Portability of Connection •Location Tracking •Establishment (Registration) of Secure Messaging Capability •User – Device Communication (User Initiated) •Device Initiated Communication •Software update
Measurement of Very Low Voltage Body Signals (MVLBS)	•Non-interference with electro medical devices •Radio transmission activity indication •Radio transmission activity control

Telecare data traffic between home and remote monitoring centre	• The M2M system would need to be capable of handling M2M traffic of different categories (i.e. of different priorities and with different characteristics) • The M2M system would need to be capable of supporting applications to establish 2-way voice communication at the request of applications and prioritize traffic accordingly. • The M2M system would need to be capable of supporting applications to establish other real-time interactive or real-time streaming communication (e.g. video) at the request of applications and prioritize traffic accordingly • In case of failure of communication links (partial link loss, drop in quality, need to switch to backup etc): o High resilience is provided for alarms traffic o No data loss is incurred (all types, or just alarm and certain medical data?) o Enable voice services to be maintained to accepted performance standards • Must be able to work simultaneously with a normal array of 'home' IP related services running over the same connection (home automation, entertainment etc as well as other remote monitoring services, such as telehealth).

2.2 EXALTED use cases and scenarios

One of the main goals in EXALTED is to contribute to the existing M2M standardization activities. Therefore, the EXALTED requirements should soundly base on the requirements proposed by ETSI & 3GPP, aiming at enriching those requirements and making them more consistent with the EXALTED vision, i.e. to support M2M applications through the LTE cellular network.

Moreover, following the concept of ETSI and 3GPP, the scope of EXALTED is not to focus on a specific M2M use case or application or to derive requirements for specific use case. On the contrary the primary target is to **provide a scalable unified solution with long term value, which will be the enabler for developing a large diversity (ideally any) of M2M applications.**

The procedure that is followed in EXALTED, regarding the use cases and the extracted requirements includes the thorough investigation of the use cases and the requirements as presented by ETSI and 3GPP, and filtering them through the prism of LTE and heterogeneous capillary networks in order to conclude to those technical requirements, which are aligned with the EXALTED objectives (Figure 2.3). In the following, the ITS, Smart meter and e-health use cases are presented as seen in EXALTED.

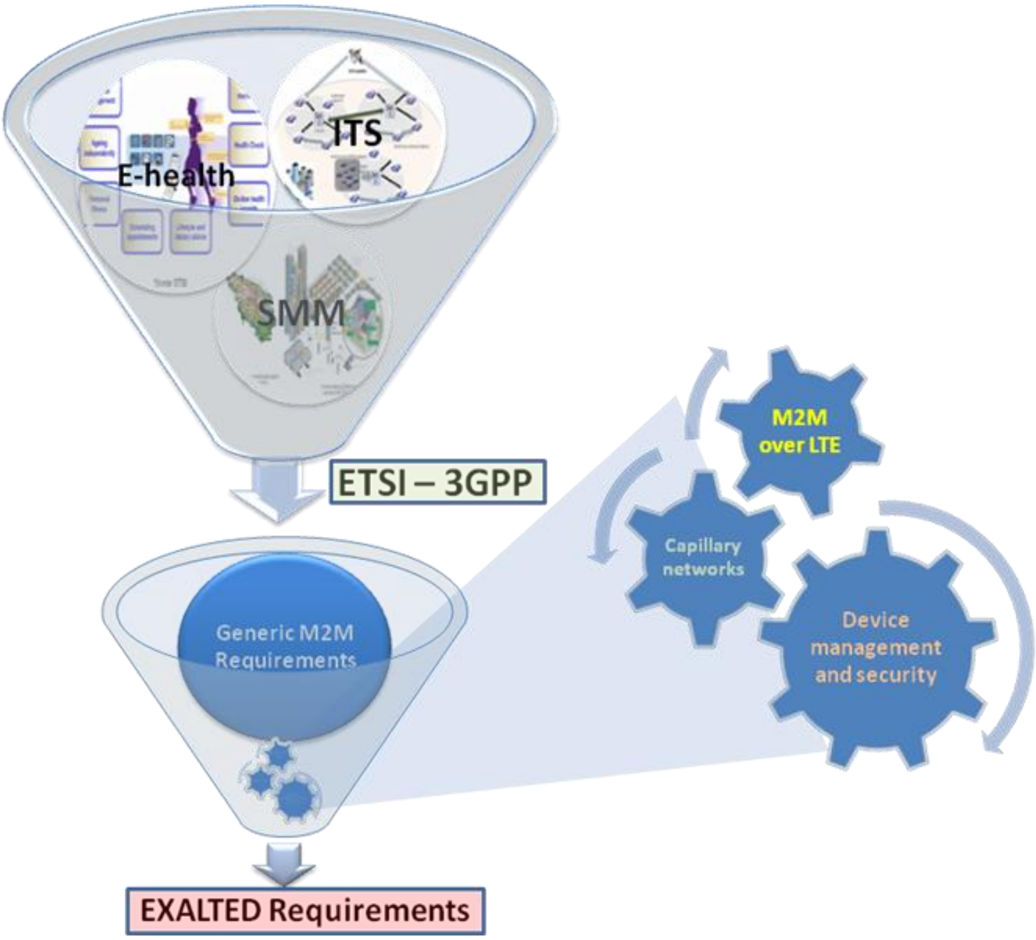

Figure 2.3: Towards consolidating M2M requirements for operation over LTE.

2.2.1 Intelligent Transport System (ITS) Scenario

2.2.1.1 Description of ITS Scenario

Intelligent Transport Systems (ITS) are based, among other things, on communication methods and technologies that enable exchange of information between vehicles and transport infrastructure on one side and ITS applications on the other. ITS applications manage various parameters related to automotive industry, such as transportation time, traffic collision avoidance, on-board safety, fuel consumption, and many others.

The use of M2M class of devices in automotive allows the improvement of current applications and at the same time opens the door to novel use case scenarios. Wireless in-vehicle diagnosis and wireless bumper camera are two such M2M improvements of existing applications (wired Controller Area Network (CAN) diagnosis, and live camera for rear view exist for a couple of years). Some examples of novel use case scenarios are the emergency alerts propagating *hop-by-hop* between the vehicles in traffic jams. Currently there is no deployment of vehicle-to-vehicle (V2V) communications other than pure radio-emission-reception for collision avoidance.

The widespread adoption of communication facilities embedded in numerous small devices is clearly the stimulating factor towards M2M automotive networking scenarios. On the other hand, the mismatch between the fundamental mobility pattern of vehicles, and the architecture of the Internet with static addresses (one address is topologically correct at only one place in the Internet), constitutes the main factor hampering the use of Internet connectivity in M2M automotive scenarios.

Within the scope of EXALTED, the ITS use case for LTE-M includes the following automotive applications:

- Remote Monitoring of Vehicle Data: mileage, engine temperature, etc.
- In-Vehicle M2M Diagnosis: in-vehicle wireless check (e.g. rear light bulb).
- Railway remote monitoring and failure detection.

Besides these uses cases that assume *vehicle-to-application server* communication, EXALTED also examines the following *vehicle-to-vehicle* scenarios:

- Parking time check.
- Vehicle collision management.
- Gateway vehicle for car-to-car communication.

2.2.1.2 Remote Monitoring of Vehicle Data

In the use case *Remote Monitoring of Vehicle Data*, a server located in the fixed infrastructure monitors the data emitted by M2M devices deployed in a vehicle. For example, the Server may monitor a counter device ("odometer" for path measurement) of a vehicle and raises an alert when the mileage limit is reached for periodic vehicle safety inspection.

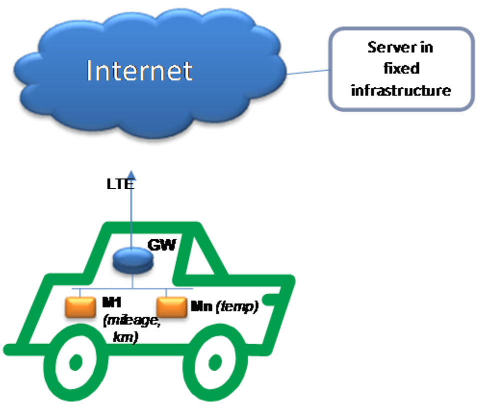

Figure 2.4: Remote Monitoring of Vehicle Data.

As shown in Figure 2.4, the counter device M1 is connected to GW (a Gateway, or a "box") in the same vehicle, which is connected over the LTE-M network and the Internet to the server.

The data being monitored is not restricted to mileage information. Other use cases may involve measuring the temperature of the engine with the goal of alerting in case of engine fire (and perhaps send fire squad to the incident scene). Furthermore, use cases vary according to different types of M2M devices: impact detection (car crash), water detection (accidental diving), gyroscope and location (reverse driving), etc.

2.2.1.3 In-vehicle M2M Diagnosis

The use case of diagnosis in-vehicle using M2M devices is described mainly as a wireless counterpart to the wired use case whereby a technician checks various local points of vehicular health data: fuse state, light bulb state, cable continuity, etc. Instead of plugging a wired device on a special socket, it is possible to use a low-power short-range wireless communication technology to query status data from dedicated M2M devices deployed in a vehicle. As an example, the Figure 2.5 shows the case of checking the health status of a light bulb deployed at the rear of the vehicle, using a light sensor M2M device enhanced with a wireless communication interface (e.g. IEEE 802.15.4).

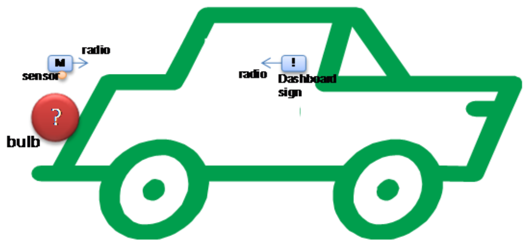

Figure 2.5: In-vehicle M2M Diagnosis.

In this illustrative example use case the "M" indicates an M2M ultra-small device (very low power, very constrained in terms of memory and CPU) placed near the light bulb. It uses a simple light detector which is activated when the bulb emitting light (turned on). It sends this data to a similar M2M device attached to the driver's dashboard. In this way, a technician (or even a trained driver) would be able to make sure the rear light bulb turns red when s/he steps the brake pedal.

This diagnosis scenario may be extended to other devices in the vehicle. Its main characteristic is that it is very easy to deploy (no need for CAN connection), very low-power (can function for years) and transmits very simple data (status bits).

2.2.1.4 Railway remote monitoring and failure detection

Railway tracks can be equipped with sensors able to measure the state of the rails and the electrical conditions that ensure the proper operation of the system. In addition, detection of breaks in the rails or detection of obstacles on the railway can help in avoiding accidents. Trains can be equipped with sensors to track the state of the wheels and the engine, as well as with actuators that take immediate corrective measures to avoid accidents.

Applications related to safety present time-critical constraints, while some other applications dedicated to monitoring might be time-tolerant. In any case, the deployment of sensors along the trains and all over the tracks will require strong energy-efficient operation of the communications, so that the costs of maintaining the infrastructure can be controlled.

2.2.1.5 Parking Time Check

Parking Time Check is a scenario related to the law enforcement vehicles. While other described scenarios involve a connection to the Internet, this case relies extensively on a local vehicle-to-vehicle communication capability between machine-type devices (V2V and M2M).

A law enforcement vehicle drives along a line of parked vehicles and sequentially queries data from M2M devices deployed in these vehicles. The large vehicle is equipped with a gateway capable of communicating wirelessly with the M2M devices of each vehicle. This communication should be standardized.

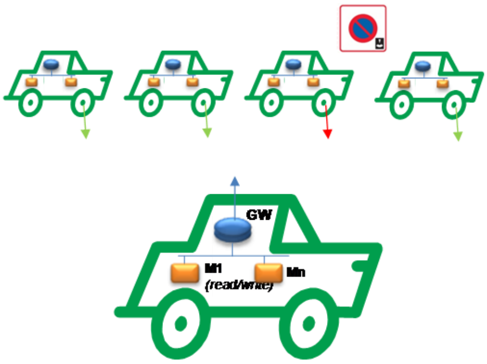

Figure 2.6: Parking Time Check.

The use case involves mainly data querying, but it may be possible that an initial writing pass is needed, where the law-enforcement vehicle first stamps each vehicle's local memory with a distinguishing mark. This mark is used if the law-enforcement vehicle passes after a specified amount of time, to identify which stamp is still there (time expired). This also involves a notion of localization.

2.2.1.6 Vehicle collision management

This scenario includes important features concerning the pre-crash sensing warning and collision detection, including the use of car sensors. All sensors (car, highway camera) send the information to the back-end system (Collision avoidance system – Auto-pilot application). The back-end system broadcasts notifications to all vehicles in the vicinity of the location of the collision, and information about actuation of relevant controls in the car. In all the receiving cars, the automatic driving systems based on the received information take over the control fully or partially (brakes activated, driving direction changed, seating belts tightened, passengers alerted etc). If there is no such system in a car that can perform all these actions, the driver is notified and instructed. Furthermore, depending on the proximity of the accident, cars receive different commands, i.e. cars that are closer to the place of the possible collision get immediate commands for the actuators, while the cars that are far away from this place get information for the driver.

Cars are equipped with a "box" which contains relevant sensors and an application which is taking the measurement results from sensors and formatting them. Moreover, based on the information received from the Auto-pilot application server, the application executes appropriate car controls. The box is connected to an LTE-M terminal to enable interaction with the application server.

The Auto-pilot combines data received from the cars (through LTE-M network), and data received from the fixed sensors along a road (through a possibly dedicated mesh network and/or LTE-M network).

2.2.1.7 Gateway Vehicle for C2C Communications

Car-to-car (C2C) communications are important for vehicle collision detection and avoidance. Pre-collision information is sent instantaneously from the colliding vehicles to other vehicles which may be subject to the further shockwave propagation. The effectiveness of accident prevention depends on various factors: data propagation speed vs. vehicular propagation speed, human driver reaction time and decision accuracy, and others.

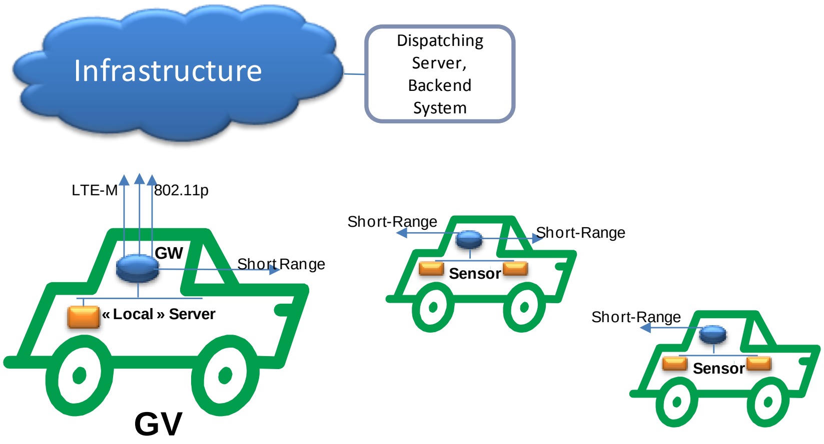

Figure 2.7: Gateway Vehicle and Multihop Scenario.

The scenario presented above (Figure 2.7) is a first step, in which vehicles are connected to the infrastructure with LTE-M and all can receive emergency information. Further, an enhanced scenario is where vehicles communicate directly and exchange data in a hop-by-hop manner, potentially building a *multi-hop* system. Some vehicles are equipped with a *Gateway* (GW) enabled with LTE-M, whereas others use a smaller router using short-range communication as shown in Figure 2.7.

In this scenario, the Gateway Vehicle (GV) is *strongly* connected to the Internet. It is equipped with several connectivity interfaces, in order to accommodate a large variety of coverage and QoS requirements situations: LTE-M and 3G+, a satellite link in rural areas and eventually WiFi interface for small hotspot areas. The GV uses selectively one or several of its interfaces to connect to the Internet, depending on various factors like link quality, bandwidth, or cost. It offers connectivity with an additional short range interface to vehicles in close range, as offered by IEEE 802.11p (PHY/MAC Layers) for Dedicated Short Range Communication (DSRC).

Other vehicles use Routers instead of Gateways. A Router is equipped exclusively with short-range communications interface such as IEEE 802.15.4 or DSRC (but not LTE). A vehicle with a Router may help propagate data hop-by-hop faster than communicating the same data through LTE-M to the Dispatching Server fixed in the infrastructure. It is important to identify the best adapted means, depending on the emergency nature of data to be transmitted.

2.2.1.8 ITS Features

The main features of the ITS scenario can be identified in Table 2.8.

Table 2.8: ITS Scenario Features.

Scenario’s features	Remarks
Mobility	ITS applications should deal with high mobility patterns. Note that some applications, such as parking time check may not expect high mobility.
Outdoor operational environment	Most ITS applications (except for in-vehicle diagnosis) occur in outdoor environments.
Urban operational	Most ITS applications are envisioned in urban environments.

environment	However, ITS applications running on highways or railways may be operated in rural environments when long-distances are covered.
Large geographical coverage	The mobility capability of vehicles envisions applications that require large geographical areas of coverage to monitor a fleet of vehicles.
Number of devices	Most ITS scenarios consider medium-to-high number of devices. In applications such as in-vehicle diagnosis, the number of devices might be fairly low.
Energy-constrained devices	In-vehicle diagnosis and railway remote-monitoring scenarios may require high energy-efficient operation. This requirement is not associated to all scenarios, as remote-monitoring may not require such efficient operation as the gateway installed in vehicles may be connected to the batteries of the vehicle.
Reliability	When safety is involved, reliability is a critical requirement in ITS. Applications such as parking time-check may not require strong reliability as retransmissions can be scheduled. However, real-time applications involving safety pose strong reliability requirements.
Real time performance	Remote-monitoring application for the ITS scenario do not require real-time performance. However, control applications involving safety impose severe requirements in terms of real-time operation.
Server initiated communications	Remote-monitoring applications for the ITS scenarios require server initiated communications, as they may be based on a data polling scheme, from a central server to the devices monitoring the environment. Applications such as C2C communications may not need this kind of operation.
Use of Gateways	Each vehicle may be equipped with a gateway providing LTE-M connectivity. This means that devices installed on-board may be simple and energy-efficient, as they may establish communication through a capillary network with a gateway connected to the LTE-M system.
Multi-hop architecture	Applications such as C2C communications may use multi-hop connectivity to create communication paths between vehicles. This requirement also applies to the railway application, where the devices installed along the rails may establish a multi-hop communication architecture.

2.2.1.9 ITS target parameters

Beside the generic ITS features that have been identified within EXALTED by the corresponding expert partners, key parameters have been also identified that help validating the adequacy of the solutions proposed by the other technical WPs with the EXALTED objectives.. These key parameters are presented in Table 2.9, along with the respective justification, where applicable.

Table 2.9: Parameterization for the ITS use case.

M2M Network			Justification
Deployment architecture	Device-to-device communication	YES	The devices inside a vehicle can communicate with each others.
	Infrastructure-to-device communication and vice versa	NO	The devices in a vehicle are connected to the infrastructure through a gateway.
	Hybrid architecture, devices-to-cluster head	YES	Please see previous clause.
	Cluster head -to-infrastructure	YES	Please see previous clause.
Communication type	Peer-to-peer	YES	Device-to-device communication inside a vehicle
	Multi-hop	YES	V2V2I communication.
	Device to gateway	< 10m	Only devices inside an IV can communicate directly with the gateway. LVs devices need a V2V communication in order to reach the gateway.
	Device to device	<10m	Device-to-device communication inside a vehicle.
	Power consumption	On-board units (OBUs) EIRP Max 33 dBm	[TR 102 492-1 Part 1, 2005]
		Road-side units (RSUs) EIRP Max 33 dBm	[ETSI EN 300 674, 1999]
Network partitioning	Spectrum usage	5.850 GHz to 5.925 GHz (5.795 to 5.815 GHz for short-range Applications)	[ETSI EN 300 674, 1999], [ETSI TR 102 492-1 Part 1, 2006]
	Interference management Self-organized network	YES	IVs close to each others use different channels to communicate with their attached LV.
Devices' transmission range		YES	The routing protocol deployed on the capillary network allows upcoming vehicles to be attached to the network.
	Periodic messaging	1-10 Hz for Co-operative road safety applications	[ETSI TR 102 638 V1.1.1 (2009-06)]
	Latency time	100 -500 msec for Co-operative road safety applications	

2.2.2 Smart Metering and Monitoring (SMM) Scenario

Smart Metering and Monitoring (SMM) applications include several scenarios, mainly differentiated by the application scale (e.g. home, industry or environmental), which also determines each corresponding set of requirements.

2.2.2.1 Energy Smart Metering – Building Management

The scope of Advanced Meter Management (AMM) is large, allowing the Energy Grid Operators to avoid any outage on the energy grid with load-balancing tools, the Energy Service Providers to offer a range of services at different prices depending on the demand, and the consumers to better manage their energy consumption.

The Consumers might be very interested to use a tool like an Energy gateway, to manage remotely a wide range of devices connected over short range RF, as represented in Figure 2.8. Consumers would be able to use their smartphone to connect to the Energy gateway, read remotely their electricity consumption, shut down the heating in their house, etc.

The Energy Service Providers will use the energy gateway to access to the electronic meters, and read remotely the power consumption to send the invoice to the consumers.

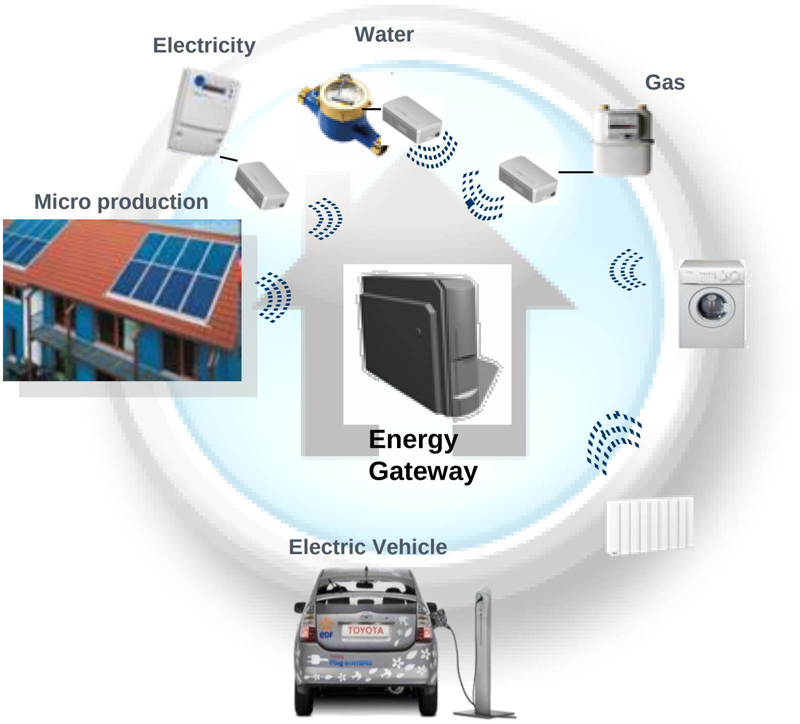

Figure 2.8: Energy gateway ecosystem (Source: Sagemcom E&T, 2011).

The system must ensure security for the data (prevent eavesdropping), and security for the system itself (hacker attack, quality of service).

The Energy gateway, Meters or Data concentrators may be placed in positions where they are subject to physical tampering, e.g. fraudulent alteration of the meter reading. Meters which are autonomously connected to public IP networks may also be subject to IP-based attacks, which may be fraudulent or malicious. The Energy Service Providers (ESP) or the Smart Metering Provider (SMP) wishes to assess the security of the meter periodically by remote means, so that appropriate action may be taken.

The Smart Meters, Energy gateway or Data concentrators can initiate the process upon query from the EMP or SMP (e.g. before reporting its readings) or may autonomously report its security status at regular intervals. After performing an integrity check, the smart meter provides a statement of security status to the SMP who can take appropriate action, such as sending personnel to check the meter if tampering was detected. The tampered device may also be prevented from accessing the communication network.

2.2.2.2 Industrial Monitoring

There is a huge market for M2M applications focused on remote control and remote monitoring of industrial environments. Remote control is intended to interact with physical mechanisms, for instance lighting, access facilities or elements on an industrial assembly line. On the other hand, remote monitoring allows to keep under control variables associated either to the industrial equipment (errors, lacks of materials, alarms, etc.) or the environment (keeping the devices between a temperature or pressure range, detect potential problems, help programming scheduled tasks, etc.). For both remote control and monitoring, M2M appears as an easy to deploy, robust and reliable way of communication.

The use cases that fit best here are summarized in **Table 2.10**.

Table 2.10: Industrial remote control use cases.

Field Covered	Envisioned Application
Remote based control	Lighting Control (Switching on and off streetlights manually or on a scheduled way in order to avoid energy consumption peaks)
	Access control (Granting access to some facilities based on user privileges or automatically open or close ways of access)
Industrial automation	Industrial Inventory Management (Tank farms, oil caverns…)
	Diagnostic alerts in order to increase the security level
	Decrease maintenance and deployment costs (A/D, D/A, PLC I/O, wires)
	Control Unmanned offshore plants (e.g. Gas plants)
	Maximization of the Productivity
	Assembly chain timing optimization (remote control of device status in order to schedule material refilling and picking up just in time)
Parameter monitoring	Keep continuous control of sensible parameters in industrial processes.

A deeper insight of the aforementioned scenarios shows the remarkable role of LTE-M in scenarios regarding industrial processes. The first group, remote based control activities, points out the possibility of handling remotely lightning control and access control to facilities, based on M2M communication and information hosted in servers accessible through LTE-M network. As a second group of potential use cases covers industrial automation, assembly chains consist of many different processes, each of them controlled by their own subsystem.

By using M2M solutions these processes can be optimized as a global one managed in a remote fashion. Finally M2M is a suitable solution for keeping parameters under control in potentially dangerous zones. Using WSN, it is possible to know how the environment reacts when some human-initiated hazardous actions take place.

Figure 2.9 depicts a general scenario for remote access and lightning control using M2M communication. Devices are controlled remotely by a web server, where client commands are translated into operation orders that LTE/ZigBee gateway introduce into the capillary network, in this case, ZigBee. Each remote node is capable of controlling a number of relays and getting info from some sensors. By taking advantage of capillary networks' transmission capabilities, the messages are distributed and delivered to the gateway, that is in charge of sending those messages through its LTE-M interface to a centralized server controlling the whole system.

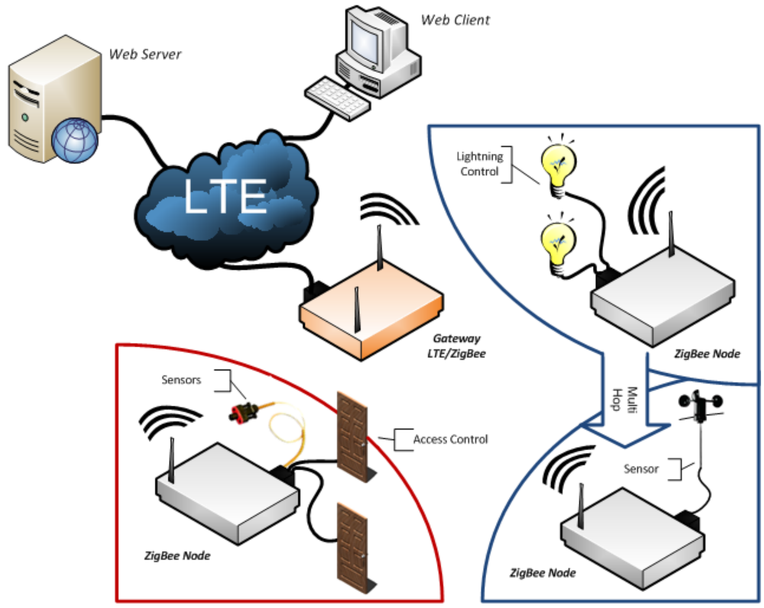

Figure 2.9: Lighting and access control example for industrial purposes.

2.2.2.3 Environmental Monitoring

In this use case, M2M communications are expected to grow quickly in the coming years with climate changes and pollution as focal points. Most beneficial applications and services related with environmental monitoring (Figure 2.10) are expected to be:

- Remote water quality monitoring.
- Remote water level monitoring (e.g. for flood management control).
- Remote optimum management of water usage for agricultural activities.
- Remote air-quality monitoring.
- Remote monitoring of sensitive areas (e.g. forests) for preventing environmental destructions.

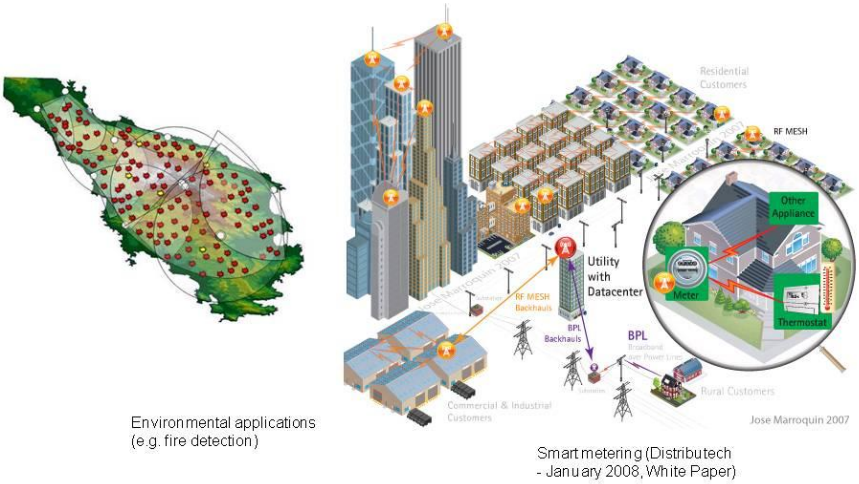

Figure 2.10: Illustration of the Smart Metering Scenario.

Moreover, levels of pollution in different districts of a city can be measured with sensors mounted on public transport vehicles, since they can make measurements on almost all spots of interest in the city. By adding the monitoring of vehicle position, e.g. using GPS receivers with these devices, location of vehicles can be determined, which can be used for identification of particular area where the data is collected. Devices with sensors can measure the level of Sulphur dioxide (SO_2), Carbon monoxide (CO), Carbon dioxide (CO_2), Nitrogen dioxide (NO_2), or any other gas that is dangerous to human health. Sensors can also record parameters related with weather conditions, such as temperature, humidity, and pressure. The devices send this information to application servers through a wide area network (LTE-M).

The key characteristics of such M2M applications are the outdoor operational environment and the large scale of deployment, with the devices having to cover huge geographical areas, while no human intervention should be required.

2.2.2.4 Security – Surveillance

This group of applications may be divided into two main categories based on the mobility of the involved devices. Sample applications in the first category are:
- Surveillance of buildings;
- Prevention of theft;
- Intruder detection.

Such applications are characterized by the indoor operational environment and devices with low or no mobility.

In the second category, applications such as tracking of valuable objects or humans can be found, where the M2M devices are expected to operate also in an outdoor environment and have high mobility.

Applications that may demand high data rate transmissions (e.g. video streaming), are exception compared to the majority of the rest of the M2M applications, and could by served by existing solutions (e.g. LTE).

2.2.2.5 Scenarios key characteristics

As described in the previous subsections, a diverse of different requirements and characteristics can be found in the Smart Metering and Monitoring use cases. However, several key features are common, providing the possibility for a more efficient network design. In Table 2.11, the most critical key features for each use case in SMM are summarized.

Table 2.11: Environmental Monitoring (EM), Energy Smart Metering (ESM), Industrial Monitoring (IM) and Security – Surveillance (SS) features.

Scenario's features	Remarks	Use Case
Outdoor operational environment	Impact on channel mitigation techniques	EM, SS
Non-urban operational environment	Impact on channel mitigation techniques (e.g. shadowing)	EM
Indoor operational environment	Impact on channel mitigation techniques	ESM, IM, SS
Urban operational environment	Interference with other domestic/urban networks	ESM, IM, SS
Extreme operational conditions	E.g. Heat, humidity, underwater operation	EM IM
Remote management	Cases in which human-intervention is either too costly or too tedious or too time-consuming (e.g. isolated devices)	EM, ESM, IM, SS
Very large number of devices	Probably leading in small density networks	EM
Large geographical coverage		
Small-medium number of devices	Probably leading in high density networks	ESM, IM
Small geographical coverage		
Device location awareness	Not necessarily with GPS (depending on device cost)	EM
Self diagnostics	Devices may report failure or malfunctions	EM, ESM, IM, SS
Battery dependent devices	Efficient power management for long-term operation	ESM, EM, SS
Battery independent devices	Most devices are expected to be plugged in.	ESM, IM
Mesh routing	Multi-hop communications	EM
Very low volumes of data	Bursty transmissions	EM, ESM, IM
Event-triggered connections	Benefits for power consumption, network signaling and scheduling.	EM, ESM
No device mobility	Mobility management may be omitted	EM, ESM, IM
High mobility is expected	Tracking of moving objects/persons	SS
Utilization of aggregation nodes	Aggregation nodes may take the on communication with the Gateway	EM, ESM, IM
Connection to LTE/LTE-M through a Gateway	The devices should communicate with LTE/LTE-M through a gateway, when possible.	EM, ESM, IM, SS

Low-end devices	Due to the expected large volume of devices for such applications, expensive devices may not be suitable	EM, ESM, IM
High-end devices	Video, GPS, mobile…	SS
Small size devices		EM
Connectivity	Application dependent	EM, ESM, IM
Reliability		EM, ESM, IM
Real time performance		EM, ESM, IM
Server initiated connections	Connection is not always triggered by the devices	EM, ESM, IM, SS
Devices within capillary network with high probability	Application dependent	EM, ESM, IM
Devices not always within capillary network	Due to expected mobility	SS
Advanced security	Ensure at least data integrity and authenticity	ESM, SS

Similarly to the ITS use case, the key parameters for SMM are presented in Table 2.12 along with the respective justification, where applicable.

Table 2.12: Parameterization for the Smart Metering and Monitoring use case.

M2M Network			Justification
Deployment architecture	Device-to-device communication	YES	
	Infrastructure-to-device communication and vice versa	YES	O4.1 DoW. DM operations requires communication in both directions, being contactable all devices in a capillary network. ETSI requirements for DM.
	Hybrid architecture, devices-to-cluster head	Possible	O4.4 and O4.1 of DoW. Energy optimization approaches focus on clustering as a mean of aggregate traffic reducing overall consumption. Based on this principle it is mandatory to support this communication.
		Possible	
Communication type	Simplex	For low complex. apps	Do not fulfill ETSI M2M TS102689 Requirements. Require bidirectional communication in order to address DM requirements.
	Half-duplex	YES	Compliant with ETSI M2M TS102689 requirements
	Full-duplex	Improbable	Extra complexity level not mandatory for being compliant with ETSI requirements
	Peer-to-peer	Possible	Functional Requirement from ETSI TS102689 Req. 6.9 demands path diversity
	Multi-hop	YES	Wireless mesh technologies demands this connectivity. In order to cover larger areas without increasing transmission power in devices.
	Multicast	YES	ETSI M2M TS102689 Requirement 6.3 Functional requirements Group Mechanisms

Network partitioning	Clustering	YES	[16][17]
	Cluster-head selection	YES	[18]
Devices' transmission range	Device to gateway	< 200m	@2.4 GHz 1mW 100 m LOS, 30m NLOS. For single hop communications. Max number of hops 255. – Typical values extracted from Digi XBee modules
	Device to cluster head	< 200m	
	Device to Base station	N/A	
	Device to device	< 200m	
Device capabilities	MIMO	NO	
	CSI	NO	
	Data rate requirements	<20Kbps	Typical monitoring applications. 1 param, 1 measure/hour, including all layers overhead supposes a data rate of 0.189 bps/ device.
	Processing capabilities	Very Low	8bit PIC can handle the operations required for SMM applications. http://code.google.com/p/xbee-arduino/
	Power consumption	<0.1mW	This parameter is highly dependent on duty cycling techniques implemented. Consumption can be estimated based on: sleep time, wake time, sleep current, TX current, RX current. It is not possible to provide exact figures to this params due to the variety of the values it allows. By the way, typical deployments are below 0.1mWatts. The next generation of Smart metering solutions for water and gas requires a battery lasting at least 20 years.
	Bandwidth usage	<50KHz	EN 13757-4 (Wireless M-Bus) current standard gives 12,5KHz of bandwidth
Miscellaneous	Cognitive radio	Possible	Complexity of devices increases when these techniques are used. This requires coordination in at least one point of the communication link.
	Interference management	YES	
	Self-organized network	YES	Bootstrapping and routing protocols within the capillary networks allow the attachment of new devices once the network has been deployed.

2.2.3 *E-healthcare Scenario*

E-healthcare, or E-health, according to *Health Information and Management Systems Society (HIMSS)* is defined as "the application of Internet and other related technologies in the healthcare industry to improve the **access, efficiency, effectiveness, and quality of**

clinical and business processes utilized by healthcare organizations, practitioners, patients, and consumers to improve the health status of patients."

E-health is not a surrogate for the clinician. It does provide the means to extend the reach of the provider beyond a face-to-face patient encounter, with the advantage of expanding the delivery of limited resources and expertise. For instance, using electronic images and pictures, diagnoses may be made from a remote location, either within or outside the facility.

The E-health Systems Architecture can be divided into several categories, according to the specific environment:

1. Internet: access to information and sites with adequate access privileges per user category (doctors, nurses, administration etc.) or universal access to public content such as education material with epidemiological characteristics (e.g. information on HPV, HIV, TBC etc.).
2. Extranet: secure, remote connections between predefined participants (links between primary, secondary and tertiary healthcare levels) even including e-commerce (ERP systems).
3. Intranet: communication infrastructure within the enterprise, which may facilitate and deliver access to internal and core data systems to all participants in the healthcare delivery chain.
4. Core Data Systems: function-based systems that support the key processes of an enterprise. These may be financial, clinical or administrative systems. Included in this group are systems such as the electronic health record (EHR), PACS, Diagnostic Support Systems (DSS), admission and appointment systems, financial patient accounting systems as well as the internal infrastructure systems.
5. Telecommunications: the physical and technical layer that enables the connections and interchange of information through all available media: wireless, fiber, cable, satellite, and any other new and emerging means. Voice and e-mail are interchangeable on some of the new devices. Recording, storing and transmitting this information falls within the boundaries of E-health.
6. Hardware: computers, pagers, personal digital assistants (PDA's), PC, tablets, telephones, servers and vital signs sensors to be used in conjunction with the DSS provide the physical support for this infrastructure.

The E-health environment is provided by the relatively seamless interaction of these layers permitting the exchange of information and transactions. The rapid development of new technologies is also reflected in the adoption of many tools even from the M2M world, often but as expected significantly less expensive than the prior generations.

E-health, as a type of M2M application, is growing independently and can be used for patient monitoring, remote diagnostics, activity monitoring, lifestyle suggestions, and personal security. E-health is increasing efficiency in healthcare, thereby decreasing costs but also improving quality. Directing patient streams to the best quality providers and on-line scheduling appointments are examples of improved quality of care. Effectiveness and efficiency should not be assumed but proven by rigorous scientific evaluation in the E-health concept. E-health creates knowledge bases of medicine and personal electronic records, accessible to consumers over the Internet, and enables evidence-based patient choice, education of physicians through online sources (continuing medical education) and education of consumers (health education, tailored preventive information). E-health enables consumers to easily obtain health services online from global providers. These services can range from simple advice to more complex interventions or products such as pharmaceuticals. E-health involves new forms of patient-physician interaction and poses new challenges and threats to ethical issues such as online professional practice, informed agreement, privacy and equity issues.

New technologies are easily integrated into existing scenarios when they address issues not yet resolved under the current implementations. Contemporary E-health reality consists of a combination of sensors for individual's vital signs measuring or even tracking his position in case of an emergency as is often the case with elderly suffering from senile dementia. These sensors come in the form of lightweight portable (or even wearable) devices for enhanced user acceptability.

The individuals who need continuous monitoring are not rare. Unfortunately they represent quite a significant percentage of the population and as our planet ages, and Europe is considered a rapidly ageing continent, the numbers are going to exponential increase. These people suffer from chronic conditions, prominent amongst them cardiovascular diseases (CVD), pulmonary conditions (e.g. Chronic Obstructive Pulmonary Disease – COPD), diabetes mellitus type II, and neurodegenerative diseases such as Alzheimer's disease. Most of these conditions do not require confinement for their patients, on the contrary, physical exercise and increased mobility is often part of the therapeutic regime.

A typical case of monitoring requires a belt that could be worn round the chest with incorporated sensors measuring heart and respiration rates and ambulatory ECG recorder (event triggered). The signals have to find their way into the treating physician's computer in order to assist to further diagnosis and treatment. Today's implementations feature the combination of bluetooth device for short range communications (hence constituting a Personal Area Network – PAN) and GPRS access for fulfilling their primary target, that is patient monitoring.

The limitations that are also challenging for the research community are the following:

1) Power autonomy: Large number of supported functions, with a longer time of monitoring, makes the energy demands greater. Increased size of batteries is not an option as it will lead to higher weighted products, thus drastically reducing both usability and user satisfaction.
2) Ubiquitous tracking for patients with senile dementia (currently based on GPS/GPRS): indoor operation can be proven somehow problematic with the aforementioned combination of technologies while the user requirement should be strictly followed.
3) Security: an individual's most sensitive data are connected to his health condition. One of the inhibitors of the monitoring applications is described as the difficulty in convincing patient that their personal data will not be compromised.
4) Interference with other networks, especially in densely populated areas, might be an issue.
5) High transmission speed could be a critical consideration when handling emergency alarms (rescue missions)

The main features of the E-health scenario are presented in Table 2.13.

Table 2.13: -healthcare scenario features.

Scenario's features	Remarks
Urban operational environment	Interference with other domestic/urban networks
Remote management	Cases in which health practitioner intervention is required (e.g. change in

	event recording frequency)
Small-medium number of devices	Probably leading in high density networks
Small geographical coverage	
Device location awareness	Not necessarily with GPS (depending on device cost)
Self diagnostics	Devices may report failure or malfunctions
Battery dependent devices	Efficient power management for long-term operation
Mesh routing	Multi-hop communications
Event-triggered connections	Benefits for power consumption, network signaling and scheduling.
High mobility is expected	Tracking of moving objects/persons
Utilization of cluster-heads	Cluster-heads may take on the communication with the Gateway
Connection to LTE/LTE-M through a Gateway	The devices should communicate with LTE/LTE-M through a gateway, when possible.
Reliability	High reliability due to sensitive nature of data
Real time performance	Only for emergency handling – latency is not prohibiting
Devices not always within capillary network	Due to expected mobility
Advanced security	Sensitive data due to health application

Similarly to the ITS and SMM use cases, the key parameters for SMM are presented in Table 2.14, along with the respective justification, where applicable.

Table 2.14: Parameterization for the E-health use case.

M2M Network			Justification
Deployment architecture	Infrastructure-to-device communication and vice versa	YES	For emergency reasons, the device should be able to connect to the network without the need of a gateway.
	Hybrid architecture, devices-to-cluster head	YES	Please see previous clause
	Cluster head -to-infrastructure	YES	Please see previous clause
Communication type	Simplex	NO	
	Half-duplex	NO	
	Full-duplex	YES	Current solutions rely on Bluetooth
	Peer-to-peer	YES	Current solutions rely on Bluetooth
	Multi-hop	Possible	Current use of medical devices does not require this capability. This might be considered in the future, e.g. in hospitals, provided that data privacy is absolutely preserved during the hopping.

	Multicast	NO	Current use of medical devices does not require this capability. A medical device is usually attached to the identity of a single user; hence distributing the same message to several devices at once makes little sense, or would pose data privacy issues.
Devices' transmission range	Device to gateway (capillary)	<10m	Typical range for ehealth applications and current solutions rely on Bluetooth
	Device to cluster head	<10m	Typical range for ehealth applications and current solutions rely on Bluetooth
	Device to Base	N/A	
	Device to device	N/A	
Device capabilities	MIMO	NO	
	CSI	NO	
	Data rate requirements	<5Kbps	Typical values for medical devices
	Processing capabilities	Low	High processing capabilities usually come with higher power consumption, which is not adequate for medical devices.
	Power consumption	<0.1mW	Typical values for medical devices
	Bandwidth usage	<5KHz	Typical values for medical devices

3. Technical Requirements

This section describes the technical requirements, which are derived from the scenarios discussed in Section 2. These scenarios have to be understood as examples for M2M communications and have been selected as EXALTED key applications because we expect notable business opportunities. The EXALTED system framework will of course not only support these key scenarios, but also other M2M services. Therefore, we won't distinguish in the following which requirement has been derived from which scenario, but present a harmonized view. However, it must be clear that some requirements are based on one specific scenario and don't have much impact on other scenarios. The requirements will serve as the baseline for the specification of the EXALTED system framework and its components.

For better readability and systematic approach, the following presentation of the technical requirements is standardized. An identification number is allocated to each requirement. The meaning of the acronyms is as follows:

FU	Functional requirements	see section 3.1
SV	Service requirements	see section 3.1
NT	Network requirements	see section 3.3
NF	Non-functional requirements	see section 3.4
DV	Device requirements	see section 3.5

Each sub-section starts with a brief introduction of the respective category. In the individual description of each item, the importance of the requirement for the realization of the EXALTED system is declared as one of the priorities: mandatory, high, medium and low. Apart from the definition and the rationale of each requirement, also dependencies between the requirements are indicated.

3.1 Functional Requirements

Functional requirements describe specific features of the EXALTED system that are needed to enable the envisaged use cases.

ID and Title	FU.1 – Support of large number of devices
Priority	Mandatory
Dependencies	NT.10
Description	M2M services are expected to require that a large number of devices (larger than the capacity of cellular systems for human-to-human communication) are connected simultaneously to one base station, either directly or through a gateway. The following aspects have to be considered: • Identification of a large number of devices both individually and by group (e.g. connected via a gateway) • Differentiation between M2M and non-M2M devices • Tracking the state of each M2M device (e.g. active, inactive, sleeping, "dead") • Provision of ubiquitous device management (e.g. when the devices move to different cells), mobility management (for both directly and indirectly connected devices) • Management of different device / service classes (e.g. different priority levels)
Rationale	Supporting a large number of devices is a mandatory crucial requirement for

	most M2M services. The incapability of current cellular networks to support a very large number of devices is one main reason that the envisioned M2M services and applications cannot be supported. Thus, technical solutions that fulfill this requirement are of particular interest.

ID and Title	**FU.2 – Efficient spectrum management**
Priority	Mandatory
Dependencies	
Description	Optimum spectrum management for maximizing the number of supported devices, taking into account: – Coexistence of M2M and non-M2M devices – Diverse M2M device classes Diverse M2M services and corresponding requirements (e.g. level of priorities, data rates, delay tolerance)
Rationale	Supporting a large number of devices with the existing resources requires an optimum spectrum management.

ID and Title	**FU.3 – Support for diverse M2M services**
Priority	Mandatory
Dependencies	
Description	The existence of different types of M2M services, each with different requirements and characteristics makes it necessary for EXALTED system to establish adaptive transmission mechanisms, for example PHY layer techniques (e.g. adaptive modulation and coding) and MAC scheduling.
Rationale	Adaptive mechanisms supporting diverse services will facilitate establishment of a unified system for M2M services with global coverage.

ID and Title	**FU.4 – Network initiated packet-data communication**
Priority	Mandatory
Dependencies	
Description	This is a mechanism that permits a remote device or equipment (such as an application server) to trigger a packet-data communication on the local cellular device, especially when this local device is not currently connected to the network. This requirement induces other additional requirements such as to avoid constantly waking-up a device to exhaust its battery.
Rationale	The rationale for this functional requirement is that an embedded device may have duty cycles where no packet data context (mainly an IP address), is allocated to it, for example to save power for from pervasive communication. It requires a collaboration with the core network to: – allocate this packet-data context – let the remote equipment know this new packet-data context to communicate with the device

ID and Title	**FU.5 – Local and remote device management**
Priority	High
Dependencies	
Description	EXALTED system needs to manage devices, deployed over a wide area, either locally or remotely in order to ensure the reliability of the services that rely on these devices. This requirement includes easy installation,

	configuration, global identification, self-diagnosis, and interaction with other devices and may also include supporting standard network interfaces such as LTE.
Rationale	Efficient and cost effective operations of M2M devices demand this requirement for providing wide coverage for M2M services around the globe.

ID and Title	**FU.6 – Unique identification of devices**
Priority	High
Dependencies	NT.16
Description	M2M Devices in EXALTED system should be able to uniquely identify and refer to each other. Inside capillary networks, devices that are not shared globally may still have non-global names (e.g. a NAT IP-address). The latter is required to support the existing technology that does not support global identifiers.
Rationale	This is needed to identify the devices (sensors, actuators, or gateways) which are part of the M2M services.

ID and Title	**FU.7 – Security and provisioning**
Priority	Mandatory
Dependencies	
Description	Comprehensive M2M (machine-to-machine) communication should include methods of security and provisioning. Common security management solution needs to automate the provisioning and identity management of M2M devices access.
Rationale	The M2M service infrastructure deals with common tasks such as security and communication aspects. These include service topics such as optimized routing, guaranteed quality of service, diagnostics (analytics tools to offer in-depth real-time and historic data, i.e. event logs), provisioning, applying security features, management, billing and more. End-to-end solutions are adjusted per specific needs, covering an on-device application on the one end and a back-end system that handles security, communication, monitoring, management, and service application on the other end. It might be required to develop a mechanism to prevent theft, spoil subscription credentials and misuse of subscription information. In addition, it might be necessary to develop some special mechanism to authenticate M2M devices. With provisioning, it could be possible to capture, monitor, control client's remote assets, manage and analyze real-time and historic data, which can be used to make financial, operational and business decisions. Utilizing common solution, it could be achieved a consistent, centralized global provisioning process, thereby improving overall system security.

3.2 Service Requirements

This section describes the technical requirements related to M2M services such as prioritization, session continuity, coexistence of multiple service providers on one single device, provisioning, remote change of subscription, delegation of functionality, and security aspects.

One important example for this category of technical requirements is device management that will be therefore introduced in more detail. It has traditionally been (from a mobile operator perspective) an efficient instrument to boost the usage of packet services and thereby increase revenues. The evolution of device management has also gone through a number of phases and is now facing the challenges to handle M2M scenarios, which sets a number of new demands on the device management domain, for example higher degree of automation and autonomy due to the lack of human intervention in most M2M scenarios.

One of the biggest obstacles when identifying a potential device management service for the EXALTED system is the vast number of vertical solutions which in many cases already have well defined, but proprietary management solutions. These solutions rarely achieve small communication costs and do not scale well for millions of devices, which are the main EXALTED requirements.

EXALTED will develop methods for a unified, multi-customer device management service. This device management service will be able to handle a fleet of heterogeneous M2M devices in a reliable and scalable fashion.

A potential Device Management service needs to support the following typical uses:

- Detection and Registration
- Addressing
- Provisioning
- Wake up
- Configuration
- Software Update
- Data Collection
- Remote Control
- Remote Monitoring
- Alarms
- Remote Diagnostics
- Real Time Interactions
- Distributed Device Management
- System Security
- High Scalability/High Availability
- Low-Energy Consumption and Low-cost devices

In the following tables, service requirements are described in detail.

ID and Title	SV.1 – Overall QoS
Priority	Mandatory
Dependencies	NT.14, NF.5
Description	QoS concept allows proper prioritization of service and device communication, scheduling mechanisms, and session continuity. Critical services have certain guarantees depending on the application types for required data rate and proper functionality in different M2M networks and in range of environmental factors (humidity, temperature, velocity...).
Rationale	Classification and prioritization of services is necessary in M2M networks with a large number of devices and different services. Mechanisms for unique device/user identification and recognition of different traffic types should be applied.

ID and Title	SV.2 – Allow multiple service providers on M2M devices
Priority	Low

Dependencies	SV.3, NF.3
Description	M2M devices, mainly gateways, supporting multiple service providers allow operations or connections from different service providers. In that case, an initial operator provides a framework on the device to allow other operators to develop new applications for new services that were not included at the beginning. To avoid unwanted interactions between applications, the device assigns permissions to applications, preventing them to access some resources if necessary. Furthermore, only authorized applications are allowed to be installed on the device.
Rationale	This requirement is interesting to extend the functionalities of an M2M device once it has been deployed in the field to provide on-demand services, depending on user's subscription.

ID and Title	**SV.3 – Efficient provisioning of a set of M2M equipments**
Priority	Mandatory
Dependencies	NF.1, NT.13, DV.1, DV.10
Description	The provisioning consists in initializing, bootstrapping, or updating all necessary configuration of an M2M Equipment (M2ME) to allow it to provide its services, often after field deployment. This requirement addresses the need for an M2M service provider, who manages a fleet of M2ME, to rely on automated, scalable, and efficient provisioning procedures with respect to message exchanges and number of roundtrips, without compromises on security.
Rationale	Because of the expected large number of M2ME in the EXALTED system, and to avoid costly physical accesses to the equipments, remote provisioning must be possible.

ID and Title	**SV.4 – Change of subscription**
Priority	Mandatory
Dependencies	SV.3
Description	In line with the GSMA-led Task Force on Embedded Sim (e.g. see [20]), the device management system must let remotely change the network subscription of a fleet of M2ME to a different MNO in a short time and for an unlimited number of subscription changes.
Rationale	Being indefinitely tied to a given MNO at field deployment phase is commonly perceived as hindering the M2M market growth. Indeed, considering the large potential number of M2ME, currently, the subscription change procedure requires tedious manual work, which is not cost productive. It becomes then imperative to introduce a method for remote subscription change, which would let M2M service providers switch to a different MNO after field deployment and thus allow M2M market growing faster.

ID and Title	**SV.5 – Delegation and distribution of functionalities**
Priority	Mandatory
Dependencies	NT.4
Description	The capacity for the gateway to assume functions otherwise located in other nodes of the network. Delegation has to be tightly controlled by the entity that delegates.
Rationale	Delegation is a mechanism that allows a secured distribution of functions in

	order to prevent congestion at a single access point; the benefit is a better use of network resources, a better control over application deployment and device management. Delegation, while interesting to split network load over several nodes, requires tightly secure schemes. Moreover, delegation requires the support of multi-hop communication (see NT.4).

ID and Title	SV.6 – Security
Priority	Mandatory
Dependencies	
Description	When it comes to security, device management implemented in the EXALTED system must ensure data protection (health, payment, meter reading information) and protection of the system itself (hacker attack, quality of service). It should be possible to securely change the subscription in the M2M equipment remotely and also remotely upgrade security credentials, cryptographic contexts, cryptographic algorithms and methods. A mechanism should exist to prevent the loading of unauthorized software on the M2M equipment. Data traffic sent or received by an M2M terminal should have the same protection against eavesdropping or modifications as traffic processed by any 3GPP UE.
Rationale	System Security is critical and universal.

3.3 Network Requirements

Under this section, system requirements related to network infrastructure needed for establishing E2E M2M communication are described.

ID and Title	NT.1 – Heterogeneous networks
Priority	Mandatory
Dependencies	
Description	EXALTED should support heterogeneous networking between LTE network and all types of capillary networks such as Bluetooth network, IEEE802.15.4 network, IEEE802.11 network, etc. This should include both ad-hoc and infrastructure-based networking.
Rationale	Network access technologies for M2M devices widely vary, based on scenario, application, or location. EXALTED system should accommodate the promising network access technologies for capillary networks.

ID and Title	NT.2 – LTE-M backward compatibility
Priority	Mandatory
Dependencies	
Description	The introduction of LTE-M must not affect the functionality of legacy LTE terminals. This is one key requirement of EXALTED.
Rationale	3GPP does not accept contributions that harm the functionality and QoS of legacy LTE terminals, i.e. LTE terminals do not need to support additional LTE-M functionality. LTE-M terminals (one category of M2M devices) can constitute one or more new 3GPP device classes dedicated to the particular needs of M2M communication.

ID and Title	NT.3 – Minimum number of modifications in the network infrastructure

Priority	Mandatory
Dependencies	NT.2
Description	LTE network infrastructure, e.g. LTE base stations, is already deployed. The introduction of LTE-M will require some modifications. The number of modifications should be kept at minimum.
Rationale	Such an approach will minimize the upgrade costs from LTE to LTE-M. If possible, the RF processing should not be affected, but only the baseband processing. Preferably, the required modifications can be done by means of software updates.

ID and Title	**NT.4 – Support of multi-hop communication**
Priority	Medium
Dependencies	
Description	Retransmission of neighbor's data or transmission of their own messages to a pair, in case the neighbors or the node itself is not able to reach the sink/cluster-head/gateway node.
Rationale	This is one of the EXALTED general assumptions when talking about capillary networks. For large sets of M2M devices, the multi-hop requirement appears as critical in order to achieve the auto-deployment and self-healing characteristics of this kind of networks. This requirement, combined with the appropriate routing protocols, enables scalability of capillary networks.

ID and Title	**NT.5 – Half duplex operation of terminals**
Priority	Mandatory
Dependencies	
Description	A half-duplex system provides communication in both directions, but only one direction at a time (not simultaneously). Typically, once a party begins receiving a signal, it must wait for the transmitter to stop transmitting, before replying (antennas are of trans-receiver type in these devices, so as to transmit and receive the signal as well).
Rationale	Full duplex operation requires substantial extra complexity in RF design of terminal devices. This is particularly the case when devices need to operate on more than one band. The RF filters needed for full duplex operation impose extra losses which increase transmitter power consumption. Half duplex operation (as used in GSM) will be essential to keeping down the cost and power consumption to enable a mass market. As with GSM, base stations will operate full duplex to make maximum use of spectrum resources.

ID and Title	**NT.6 – End-to-end device-to-device communication**
Priority	Mandatory
Dependencies	NT.4
Description	M2M devices can establish and maintain direct E2E communication, with or without the support of the core LTE-M network. If using the core network, the communication will be between devices on different environments (i.e. different capillary networks or between a capillary network and devices connecting directly to the LTE-M network). The core network may not be used if the communication is between nodes within the same capillary network or between capillary networks operating in the same technology (if gateways support direct communication between pair within coverage).
Rationale	Developing smart M2M devices capable of establishing such communication

	will reduce the operational cost.

ID and Title	**NT.7 – Flexible addressing scheme**
Priority	Mandatory
Dependencies	NT.3
Description	Each device should be able to be reached using a unique address, both from inside its own network and from any other point connected to the LTE-M network. Moreover, LTE-M network should handle variations on the population of a cell in an efficient way, by assigning each device an address, reusing the ones previously freed.
Rationale	In order to be able to enable all the features intended to be demonstrated on the EXALTED project regarding routing protocols, mobility, device management, etc., the use of an addressing scheme is critical. An IP-based scheme would be the most desirable scheme in order to reach all the requirements, but, as some M2M devices may have little resources, at least other simple addressing schemes must be implemented. Then, the gateway should take care of routing in an appropriate way the data coming from and going to each node.

ID and Title	**NT.8 – Mobility management**
Priority	Mandatory
Dependencies	
Description	Mobility management is responsible for the handover of M2M devices and gateways. This requirement strongly depends on the characteristics of the use cases.
Rationale	Particularly for the use case of *Intelligent Transportation System* (ITS), we expect mobile M2M devices. It may happen that a big number of devices request a handover at the same time, or the gateway of one complete capillary network requests a handover. On the other hand, assuming stationary devices, mobility tracking can be switched off to reduce signaling. Therefore, mobility management has to be highly scalable and needs particular consideration in the design of the EXALTED system.

ID and Title	**NT.9 – Reliable delivery of a message**
Priority	High
Dependencies	
Description	The information carried by packets must be delivered to the destination points via link-level and transport-level retransmission and error feedback mechanisms.
Rationale	Having acceptable level of reliability for most applications is very important. Notification of any failure to deliver the message is a key issue in WP4. Protocols intended to be used for monitoring and auditing the devices must be reliable in order to maintain the satisfactory level of operation of the network.

ID and Title	**NT.10 – High node density**
Priority	Medium
Dependencies	NF.6
Description	Large sets of M2M devices connected to the LTE-M network through single access points.

Rationale	Monitoring applications require a large number of sensors in specific and reduced locations, in order to capture a spatial phenomenon in a large geographical area (adding several locations). The effect of high node density can lead to difficulties on gateway nodes in order to handle it, or from the point of view of a MAC protocol, this creates a high-link-level delay since nodes should first need to acquire channel access.

ID and Title	**NT.11 – Traffic aggregation**
Priority	Medium
Dependencies	
Description	Data collected from large sets of M2M nodes is aggregated by a cluster head or a gateway in order to minimize signaling overhead, improve energy efficiency, and reduce operational cost of the network.
Rationale	Sensors observations are strongly correlated (in space and/or time). Such correlation can be exploited to design energy-efficient encoders to compress the information at each sensor node and reduce traffic load at the gateway. Moreover, cost and battery constraints of end devices which short range communication with cluster-head (with respect to long range communication via LTE-M), can be regarded as compelling reasons for including this traffic aggregation.

ID and Title	**NT.12 – Self-diagnostic and self-healing operation**
Priority	Medium
Dependencies	DV.1
Description	Detecting network status and dynamic reconfiguration when topology changes.
Rationale	The network itself should evaluate its status and detect changes in the topology regardless of events that cause those changes. LTE-M network should adapt to their capabilities and available resources for offering the best QoS possible to the connected devices.

ID and Title	**NT.13 – Multicast and broadcast communication**
Priority	Mandatory
Dependencies	
Description	Transmission techniques specified for transmission to multiple destinations in broadcast or multicast mode.
Rationale	M2M communication requires mechanisms for unicast, broadcast and multicast techniques in order to provide specific device functions related to device management (e.g. software updates, simultaneous authentication of a large number of devices, instructing a M2M device/gateway to perform a particular measure emergency messages distributing etc.). 3GPP talks about group-based services.

ID and Title	**NT.14 – End-to-end QoS system**
Priority	Mandatory
Dependencies	NT.6, NT.8
Description	Scalable and independent end-to-end QoS system that provides service policy management. System is designed to enable mapping between different protocols and communication methods with no service/session interruption.

Rationale	QoS system is designed for large number of M2M devices, with dynamic modification of parameters and attributes during an active communication session. Support for all IP and LTE-M wireless protocols and bearers, is required. Should be backward compatible with legacy technologies.

ID and Title	**NT.15 – End-to-end session continuity**
Priority	Mandatory
Dependencies	NT.6, NT.8, NT.9
Description	Regardless node activity (mobility), session should be maintained although handover process will be triggered.
Rationale	An active session is maintained regardless of the network topology and the number of network nodes involved in communication between devices. Session continuity is provided on all LTE-M network segments. Legacy IP and 3gpp (wireless) protocols should be also supported.

ID and Title	**NT.16 – Support for dual stack IPv4/IPv6**
Priority	Mandatory
Dependencies	NT.7
Description	M2M nodes have to support both IPv4 and IPv6 stacks.
Rationale	Long term strategy should only involve IPv6 but also IPv4/IPv6 coexistence is required for a period of time. IPv6 solves the address deficiency problem. IPv6 comes with improved QoS support for real-time applications. Security was an integral part of IPv6 from its inception (IPSec). IPv6 will be one of the drivers of mobility (always-on mobile devices).

ID and Title	**NT.17 – Reduced signaling**
Priority	Mandatory
Dependencies	DV.3
Description	Signaling needed to manage devices (from the LTE-M network) should be reduced at most in order to avoid large amount of traffic and battery consumption due to only this feature.
Rationale	The operability of a network consisting of a large number of devices requires an important reduction of traffic, which could be probably achieved by using transmission techniques with low signaling overhead.

3.4 Non-functional Requirements

Non-functional requirements are used to outline the required quality characteristics of a system. The non functional requirements specified in this section may apply to all use cases and scenarios. However, the use cases may differ in the way the priority is assigned for a non-functional requirement, and trade-offs are made in their system design choices to capture the generality as much as possible.

ID and Title	**NF.1 – Scalability**
Priority	Mandatory
Dependencies	NF.6
Description	EXALTED system should be scalable with the number of devices, networks, as well as with the demand.
Rationale	Local capillary networks of M2M devices may have a very high density

	(hundreds, thousands, or even more) of sensors, and/or actuators. EXALTED system needs to support communication to and from these in a way that respects the other non-functional requirements as well as between capillary networks through the LTE network with potentially trillions of sensors and actuators, and billions of users world wide.

ID and Title	**NF.2 – Energy efficiency**
Priority	Mandatory
Dependencies	DV.3, DV.9
Description	This technical requirement is one key objective of EXALTED. The consumed power of the M2M devices should be as low as possible in order to prolong battery lifetime. The following aspects will be considered: • Save both processing power and transmission power • All devices should support sleep mode. • Adapt protocols to the individual M2M services (e.g. if support of mobility is not required, mobility tracking can be switched off). • Traffic characteristic (e.g. periodic time-driven transmissions vs. event-driven traffic) • Utilize delay tolerance of some applications
Rationale	This requirement ensures that power consumption of the devices is minimized. Energy efficiency is essential for several M2M services involving devices with batteries that are difficult to replace. Moreover, an efficient energy management would result in reduced interference.

ID and Title	**NF.3 – Extensibility and adaptability**
Priority	Medium
Dependencies	
Description	This requirement addresses the extensibility and adaptability of the proposed technical solutions beyond EXALTED.
Rationale	It should be easy to develop applications on top of the EXALTED system. Therefore, the EXALTED framework needs to be flexible and extensible with new devices, modules, services, and other entities. Additionally, EXALTED framework shall be run-time reconfigurable so that changes can be made without taking down the entire system.

ID and Title	**NF.4 – Real time performance**
Priority	Medium
Dependencies	
Description	EXALTED system needs to be able to support and guarantee real-time constraints in scenarios where this is needed or essential.
Rationale	Some M2M scenarios/applications require a response to changes in a reasonable timeframe. How much delay is acceptable can vary from scenario to scenario. Generally a distinction is made between hard real time constraints where certain behavior is required within timeframes typically specified in milliseconds or less and soft real time where it is desirable that most of the time the system responds within tenths/hundreds of a second. In the context of EXALTED system, supporting hard real time constraints may be not feasible or required. Most of the real-time like requirements listed in this document are of a soft nature where it is merely desirable that delays are kept to a tolerable minimum for the user.

ID and Title	NF.5 – Congestion control mechanism
Priority	Low
Dependencies	
Description	Congestion control mechanism needs to be implemented in order to ensure that network meets the stability requirements. Overload protection should be in the areas such as signaling, limiting payload traffic, processor and memory load of network nodes, buffers on interfaces, etc.
Rationale	Congestion control mechanism will prevent a large number of Devices/Gateways from overloading the eNodeB and the rest of the network.

ID and Title	NF.6 – Address space scalability
Priority	High
Dependencies	
Description	Future-proof address concept needs to be developed.
Rationale	Due to the foreseen shortage of MSISDN addresses, number of devices that can be deployed may be limited and scalability of the system impaired.

ID and Title	NF.7 – Control signaling integrity protection and encryption
Priority	Mandatory
Dependencies	
Description	The control signaling between the Device/Gateway and LTE network should be integrity protected and encrypted. Integrity protection is mandatory, and encryption is optional.
Rationale	Integrity ensures that signaling traffic cannot be modified in transit.

ID and Title	NF.8 – Service provisioning for MNO/SP customers
Priority	Mandatory
Dependencies	SV.3
Description	LTE network operator (an MNO) shall provide interface allowing SPs to perform mass provisioning operations on Devices/Gateways on ad hoc basis. SPs shall be able to perform mass activation/deactivation of Devices/Gateways based on selected criteria (per building, per area, etc.) without involving the MNO.
Rationale	This requirement is one of prerequisites for efficient network operations.

ID and Title	NF.9 – Roaming support
Priority	Mandatory
Dependencies	NT.8
Description	The M2M service infrastructure deployed by operators must support both tightly coupled and loosely coupled models. In the tightly coupled model the Service Provider connects to devices by an access network that he operates itself. In the loosely coupled model the Service Provider connects to devices via other access operators. There are several ways of doing this, such as roaming, peering, etc. The system shall at least support roaming: the ability of a visited PLMN to serve a Device/Gateway, which is still anchored in a home PLMN. Also, the system should support home PLMN change: a permanent change of serving/anchoring network, after which the old home PLMN is no longer keeping data/state/keys for the Device/Gateway moved.

Rationale	This requirement improves usability of the network and ease deployment of applications by Service Providers.

3.5 Device Requirements

Finally, the technical requirements that are closely related with the different devices in the EXALTED system are described. For the sake of clearness, we start with a brief definition of the device categories and continue with the requirements afterwards.

In this section, under the designation of M2M (remote, embedded) equipment, we mean an M2M device or an M2M gateway, or an M2M cluster-head. Their definitions are given below.

M2M Devices:
An M2M device is a discrete hardware entity that is an ending node in a M2M application and situated outside of the network domain. Functionally, a M2M device includes at least one M2M device application (the part of the M2M application that resides in the device) and one communication module.

M2M Cluster-heads
An M2M cluster-head is a network node that collects multiple streams of data and outputs them into a single stream. A device may temporarily act a cluster-head depending on the context.

M2M Gateways
An M2M gateway is a network node that provides a variety of services to other nodes. These services may cover different domains such as, but not limited to, communication services (protocol interworking, interconnection to the network and application domain, etc), security services (authentication, authorization, etc), device management services (provisioning, monitoring, etc), etc. The list of services a gateway supports may or may not be static (see **SV.2 – Allow multiple service providers on M2M devices)**.

In the following tables, device requirements are described in detail.

ID and Title	**DV.1 – Self organized M2M equipments**
Priority	Mandatory
Dependencies	
Description	The ability for M2M equipments to: ▪ Self configure at installation time: the device is able to automatically retrieve profiles that customize its capabilities ▪ Self optimize at operational time: the device is able to adjust its performances in order to match specific requirements (network resources preservation, reduced signaling, power saving, etc).
Rationale	Self organized M2M equipments allow better cost effectiveness in the deployment and the maintenance of networks.

ID and Title	**DV.2 – Reliable M2M equipments**
Priority	High
Dependencies	
Description	The equipment estimates and provides its operational status and may be able to initiate appropriate corrective actions autonomously or under control.
Rationale	High density networks of M2M equipments generate lots of operating data especially when tight device management is involved. Highly autonomous

	M2M equipments shall be able to assume self diagnostic as well as proceeding to appropriate corrective actions as much as possible in order to prevent mundane reporting from saturating the network. Local device management may be controlled by remote device management or by a local secured element.

ID and Title	DV.3 – Energy efficient duty cycles
Priority	Mandatory
Dependencies	NF.2
Description	Energy efficient duty cycle describes the different power saving strategies we could apply to the system based on its sequence of active and inactive states. Usually, power saving is optimal when the system reaches the idle state for which the device achieves minimal activity (besides OFF state) so maximizing the time spent in states that provide best power saving strategies ensures efficient energy resources management in the device. Duty cycle might be remotely controlled (by a gateway for instance) or based on different local policies.
Rationale	Usually, typical M2M equipment activity is not constant over time but, instead, shows peaks and inactive intervals. We should be able to identify, organize or even force these activity intervals in order to apply adapted power saving strategies.

ID and Title	DV.4 – Location information
Priority	High
Dependencies	
Description	The capacity to provide the equipment's geographical position.
Rationale	Security, maintenance, deployment, M2M applications require the possibility to localize the device. Precision is application dependant and does not belong to the requirement.

ID and Title	DV.5 – Location locked M2M equipment
Priority	High
Dependencies	
Description	The ability to temporarily or permanently associate M2M equipments with a geographical position or to restrict its mobility to a specific area.
Rationale	Geographically restricted devices shall be able to detect unauthorized attempts at re-localizing them.

ID and Title	DV.6 – Gateway detection and registration
Priority	Mandatory
Dependencies	NT.13
Description	When powered up, devices are automatically detected and attached to a gateway which registers them onto an M2M Application. For standalone devices (no gateway), they are detected and registered by the Core Network. It should be possible to choose an M2M provider after the manufacturing. Registration should be independent of the telecom provider.
Rationale	Automatic detection of devices/gateways followed by automatic registration is required in order to facilitate the installation of new devices/gateways (out of the box).

ID and Title	DV.7 – Protocol translation at the gateway
Priority	Mandatory
Dependencies	NT.1
Description	The capacity to provide protocol translation between capillary networks and LTE/LTE-M protocols in order to interface two different network technologies.
Rationale	Typical Exalted scenarios involving gateways show groups of devices belonging to a capillary network exchanging information with a remote application server. In order to reach the remote server, the devices get WAN access through a LTE/LTE-M gateway. Such a gateway extracts the data received through its connection to the capillary network and forwards them to the distant server using its LTE/LTE-M connectivity realizing protocol translation between the capillary network protocol and the LTE/LTE-M protocol.

ID and Title	DV.8 – Information routing at the Gateway
Priority	Mandatory
Dependencies	NT.1
Description	The capacity for the gateway to select a path in the network for the traffic it forwards.
Rationale	A gateway may be connected to different PDN or other network equipments and shall be able to select the correct path in order to minimize the number of hops packets will suffer before reaching the end point of the communication.

ID and Title	DV.9 – M2M equipment wake-up
Priority	Mandatory
Dependencies	
Description	Device/Gateway may have a scheduled M2M Core connection defined. M2M Application should be able to use Wake-up to trigger an immediate action without waiting for the next scheduled connection.
Rationale	Low-power consumption and low-activity devices may have a long sleeping cycle. Sometimes an action is needed without wait.

ID and Title	DV.10 – Remote configuration
Priority	Mandatory
Dependencies	NT.12
Description	Remote configuration of M2M remote equipments allows modifying a set of key parameters on them. For example, periodicity of data posting, server URL for posting data, software update, severity level of alarms, data to send for diagnostic, etc. Gateway should be able to send configuration messages to multiple devices connected to it.
Rationale	M2M Applications need to be able to send new settings to M2M remote equipments.

ID and Title	DV.11 – Software update over the air
Priority	Mandatory
Dependencies	

Description	The ability to remotely control the software update over the radio interface of devices/gateways is required to efficiently manage their life cycle.
Rationale	Massively deployed devices/gateways may not be easily accessible with reasonable costs.

3.6 Summary

Table 3.1 gives a coherent view of all technical requirements in EXALTED derived from the three key use cases *Intelligent Transportation System*, *Smart Metering and Monitoring*, and *E-healthcare*, but valid for other M2M applications as well. This is a summary of the previous sections 3.1 to 3.5.

Table 3.1: Summary of technical requirements in EXALTED

ID	Title	Priority	Dependencies
FU.1	Support of large number of devices	Mandatory	NT.10
FU.2	Efficient spectrum management	Mandatory	
FU.3	Support for diverse M2M services	Mandatory	
FU.4	Network initiated packet-data communication	Mandatory	
FU.5	Local and remote device management	High	
FU.6	Unique identity for devices	High	NT.16
FU.7	Security and provisioning	Mandatory	
SV.1	Overall QoS	Mandatory	NT.14, NF.5
SV.2	Allow multiple service providers on M2M devices	Low	SV.3, NF.3
SV.3	Efficient provisioning of a set of M2M equipments	Mandatory	NF.1, NT.13, DV.1, DV.10
SV.4	Change of subscription	Mandatory	SV.3
SV.5	Delegation and distribution of functionality	Mandatory	NT.4
SV.6	Security	Mandatory	
NT.1	Heterogeneous networks	Mandatory	
NT.2	LTE-M backward compatibility	Mandatory	
NT.3	NT.3 – Minimum number of modifications in network infrastructure	Mandatory	NT.2
NT.4	Support of multi-hop communication	Medium	
NT.5	Half duplex operation of terminals	Mandatory	
NT.6	End to end device to device communication	Mandatory	NT.4
NT.7	Flexible addressing scheme	Mandatory	NT.3
NT.8	Mobility management	Mandatory	
NT.9	Reliable delivery of a message	High	
NT.10	High node density	Medium	NF.6
NT.11	Traffic aggregation	Medium	
NT.12	Self-diagnostic and self-healing operation	Medium	DV.1
NT.13	Multicast and broadcast communication	Mandatory	
NT.14	End-to-end QoS system	Mandatory	NT.6, NT.8
NT.15	End-to-end session continuity	Mandatory	NT.6, NT.8, NT.9
NT.16	Support for dual stack IPv4/IPv6	Mandatory	NT.7
NT.17	Reduced signaling	Mandatory	DV.3
NF.1	Scalability	Mandatory	NF.6
NF.2	Energy efficiency	Mandatory	DV.3, DV.9
NF.3	Extensibility and adaptability	Medium	
NF.4	Real time performance	Medium	
NF.5	Congestion control mechanism	Low	
NF.6	Address space scalability	High	
NF.7	Control signaling integrity protection and encryption	Mandatory	
NF.8	Service provisioning for MNO/SP customers	Mandatory	SV.3
NF.9	Roaming support	Mandatory	NT.8

DV.1	Self organized M2M equipments	Mandatory	
DV.2	Reliable M2M equipments	High	
DV.3	Energy efficient duty cycles	Mandatory	NF.2
DV.4	Location information	High	
DV.5	Location locked M2M equipments	High	
DV.6	Gateway detection and registration	Mandatory	NT.13
DV.7	Protocol translation at the gateway	Mandatory	NT.1
DV.8	Information routing at the gateway	Mandatory	NT.1
DV.9	M2M equipment wake-up	Mandatory	
DV.10	Remote configuration	Mandatory	NT.12
DV.11	Software update over the air	Mandatory	

4. Baseline Reference Systems

M2M applications are already running, based on existing architectures and technologies, such as GPRS or LTE. As long as these applications are characterized by a small number of connected devices, comparable to the capacity of current networks, these technologies are more than sufficient for supporting specific type of M2M services. However, in the immediate future, radical changes are expected in the field of M2M communications, with the most two challenging ones being:

- The support of at least two orders of magnitude more devices compared to human-to-human communications.
- The vast diverse of applications and services, compared to the existing ones, which are mostly limited to telematics and metering.

In the following, the suitability of existing cellular technologies (GSM/GPRS and LTE) is analyzed, briefly mentioning the major prohibitive reasons for them supporting the future M2M applications, including the lack of mechanisms for managing larger number of devices in a scalable manner, the vast overhead required for low data rate communications and the difficulty in providing network-initiated communication. While GSM/GPRS is totally inappropriate for satisfying the M2M requirements specified in the previous section, LTE could be extended towards enabling the envisioned M2M applications and services.

Moreover, two possible candidates for the M2M capillary networks are presented, namely 802.11 and ZigBee, along with their advantages and deficiencies. These technologies (both for the cellular and capillary part of the network) will be used as reference systems to be compared with the final EXALTED solution.

4.1 GSM/GPRS

General Packet Radio Service (GPRS) is an extension of GSM (Global System for Mobile Communications), satisfying the need for a packet switched bearer service. GPRS utilizes a packet radio principle used for carrying end users' packet data protocol such as IP information to/from GPRS terminals and/or external networks. GPRS is designed for bursty traffic, usually characterizing applications such as Internet browsing or e-mail access. According to the GSM standard [23], resources for GPRS traffic can be reserved statically or dynamically, whereas a combination of both is also possible.

As mentioned, GPRS was designed for bursty traffic, a kind of traffic also caused by several M2M applications. Nowadays, almost all available M2M applications and services are based on GPRS, with the main reasons being the following as argued by the vendors and providers:

- Immediate M2M business entry
- Low-cost and convenient deployment
- Ubiquitous and international operability
- Roaming between mobile operators
- GPRS is a proven real-world tested technology, also open and standardized.

The GPRS modules for M2M applications are continuously evolving and are mainly characterized by their small sizes and low power consumption. Currently, commercially available M2M applications and services are limited, mainly including applications related to telematics and metering, with a relatively small number of low-mobility (or static) devices.

According to Infonetics [24] in 2009, there were 87 million M2M telematic devices on the market. When there are few M2M devices in the network, SMS is a compromise to transmit data in the GSM network, making GPRS temporary an adequate solution for M2M applications. However, by 2014 there should be more than 428 million such devices in play [21], while some M2M applications are expected to require higher bandwidth connections (e.g. surveillance applications).

GPRS is a low-cost and well established technology but it also comes up with several limitations, which raise serious considerations for its suitability for the future M2M applications. The capacity of a GPRS cell depends on several parameters, such as the partitioning technique utilized or the reuse pattern. However, assuming only GPRS traffic, the spectral efficiency of a GPRS cell usually cannot exceed the 100-150Kbps/cell/MHz [25][32]. Additionally, if voice users are also assumed to be active the number of supported data users becomes too limited (<30) [26]. Therefore, it is more than obvious that the GSM/GPRS capacity is too limited for supporting the envisioned M2M applications and services with thousands of devices per cell.

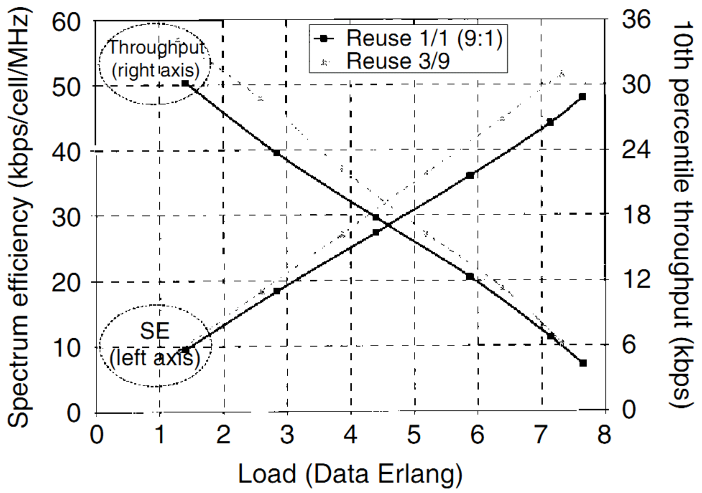

Figure 4.1: Evolution of spectrum efficiency and 10th percentile throughput in both non-hopping and RF-hopping macrocell GPRS networks. (a) GPRS with CS-1–2 and (b) GPRS with CS-1–4. Three TSL-capable terminals. One TRX (Source: [25]).

Another issue regarding GSM/GPRS networks is that it mandates that the connection is initiated by the device in the GPRS network [27]. The most usual techniques to establish a server-started connection are a wake-up call and an SMS message. Moreover, in GSM/GPRS networks there is no standard way of monitoring the state of the existing connections. Usually, the devices are programmed to report their status or the servers poll the devices on a regular basis. Both methods generate unnecessary traffic, which worsens the problem of GSM/GPRS cell capacity limitations.

Many problems are reported when implementing management servers for GSM/GPRS servers, which are expected to serve a large number of devices. A server utilizing the Remote Authentication Dial In User Service (RADIUS) protocol, is not capable of handling the information fast enough when the amount of devices is high. As an alternative, the Session Initiation Protocol (SIP) is used, but it is not memory-efficient and contains a few DoS vulnerabilities (e.g. reflection distributed DoS). In other words, the solution is based on the mature M2M module from different vendors.

4.2 3GPP LTE (Rel-8)

In recent years, the data volume requirements in cellular mobile communication have multiplied. This comes along with a gradual shift from voice to broadband data services. Enablers for this trend are flat-rate pricing, web-friendly mobile terminals, USB data modems for PCs, and an evolved network infrastructure allowing for low cost per bit. In order to cope with this demand, 3GPP has standardized LTE. Some important design criteria are high data rates (100 Mb/s mean and 300 Mb/s peak in downlink, and 50 Mb/s mean and 75 Mb/s peak in uplink transmission), increase of the cell average and cell edge spectral efficiency by a factor of 2-4 compared to High Speed Packet Access (HSPA) Release 6, flexible bandwidths for both Frequency Division Duplex (FDD) and Time Division Duplex (TDD), significant reduction of the user plane latency to less than 10 ms and control plane latency to less than 100 ms. Moreover, a flat radio network architecture has been designed to simplify operation and to reduce cost. LTE should enable smooth evolution from and coexistence with earlier 3GPP and 3GPP2 systems (Time Division Synchronous Code Division Multiple Access – TD-SCDMA, Wideband CDMA, HSPA, and CDMA 2000). First commercial LTE-systems have been put into operation by TeliaSonera in 2009 in Stockholm and Oslo. Other operators followed in 2010 and 2011. In the following, some key functions of LTE are described in more detail. Furthermore, the interested reader is referred to [24].

Evolved Packet System (EPS): To meet the design requirements above, 3GPP started in 2005 the standardization of the Evolved Packet System (EPS). In contrast to previous cellular communication systems that were based on circuit switching and developed for voice only, the EPS also includes packet-switched technology and IP-based services. The EPS consists of two new elements, the Evolved Packet Core (EPC) and the Evolved Universal Terrestrial Radio Access Network (E-UTRAN). The EPC is a multi-access core network including 3GPP 2G, 3G and 4G systems as well as non-3GPP systems like WiMAX and fixed access. The three most important design paradigms of the EPC are mobility, policy management and security. One important characteristic of the EPC is the flat architecture with only two nodes in the user plane, the base station (eNB) and the service / packet-data network gateway. Design criteria are high network performance, low cost, and low complexity. In contrast to previous systems, the EPC supports only IP packet-switched traffic, and interfaces are based on IP protocols.

Duplex Modes: In contrast to previous cellular mobile radio systems, LTE provides both Time TDD and FDD modes in one air interface, which is a strong design requirement. The applied duplex mode is transparent to the PHY-layer, enabling a low-cost implementation, only the frame structure and the control signaling are different.

Spectrum flexibility: LTE supports a wide range of bandwidths from 1.4 MHz up to 20 MHz in order to adapt to the large number of different available spectrum allocations in the different countries.

OFDMA and SC-FDMA: The LTE downlink PHY-layer adopts Orthogonal Frequency Division Multiple Access (OFDMA), i.e. the signal is composed of a multitude of narrowband sub-carriers in the frequency domain. In time domain, consecutive OFDM symbols establish a sub-frame of 1 ms duration. In combination with a cyclic prefix, OFDMA is robust to time dispersion on the radio channel and therefore allows for low-complex equalization at the mobile terminal, finally leading to reduced cost. In uplink direction, the most important design criteria are power efficiency and low complexity. Therefore, Single Carrier Frequency Division Multiple Access (SC-FDMA) has been chosen because of the lower Peak-to-Average Power Ratio (PAPR) compared to OFDMA.

Coding and modulation: Turbo coding with flexible code rates as well as higher order modulation up to 64-QAM enable high data rates and the adaptation of the radio link to the instantaneous channel conditions. Peak data rates are 300 Mb/s in the downlink with 4x4 MIMO and 75 Mb/s in the uplink.

Multiple antenna transmission: From the beginning, LTE is based on the utilization of multiple antennas at both base station and mobile terminal (Multiple Input Multiple Output, MIMO) to support the following two different aims. On one hand, with multiple antenna systems additional diversity and redundancy can be added at the transmitter and exploited at the receiver in order to improve the robustness of a radio link and to expand coverage. In LTE Space Frequency Block Coding (SFBC), Single-Layer Spatial Multiplexing (SL-SM) and non-codebook based beam forming in combination with UE specific reference signals fall in this category. On the other hand, multiple antenna systems can be utilized to transmit different data streams simultaneously to boost the data rate. This operation mode is called (multi-layer) Spatial Multiplexing (SM). The data streams can be sent either to one user (Single User, SU-MIMO) or to different users (Multi User, MU-MIMO). The choice of the operation mode depends on the properties of the radio channel.

Inter-cell interference coordination: In LTE systems, the performance is typically limited due to interference between neighboring cells. Thus, interference avoidance and coordination is one important means to improve the performance in both uplink and downlink. Well-known methods are e.g. uplink power control, fractional frequency reuse and dynamic scheduling strategies, where control information has to be exchanged among base stations. The funded FP7 project ARTIST4G is working on this topic.

Scheduling: OFDMA and SC-FDMA enable dynamic frequency- and time-selective scheduling. The scheduler that is located in the base station decides for both downlink and uplink which user gets which radio resources at which data rate. It can be seen as a key functional block of LTE, in particular if the network is highly loaded. Thereby, a trade-off between preferably high spectral efficiency and fairness among users is made. The fading property of the radio channel in both time and frequency direction is not totally a disadvantage, but can be exploited to improve the system performance. Prerequisites for this benefit are accurate channel measurements at the mobile terminals and an efficient feedback mechanism on the uplink. Scheduling is carried out on a per sub-frame basis, i.e. in a 1 ms grid.

HARQ and ARQ protocol: Important requirements for LTE are low latency and small overhead whilst providing a high reliability. The retransmission scheme therefore has been separated into two different sub-layers. A fast Hybrid Automatic Repeat Request (HARQ) protocol with only 8 ms round-trip time and one single feedback bit is part of the MAC-layer. It is based on soft combining with incremental redundancy. The HARQ is complemented by a highly reliable but more expensive ARC protocol in the Radio Link Control (RLC) sub-layer. ARQ is carried only in the rare cases where HARQ has failed.

Link-Layer Design: The LTE link layer design is distributed on three sub-layers. The Packet Data Convergence Protocol (PDCP) is responsible for IP header compression, ciphering, handover, and the integrity protection to higher-layer control protocols. The RLC takes over data segmentation and concatenation as well as the ARQ protocol, whereas the MAC mainly consists of scheduled or random medium access and the HARQ protocol. This cross-layer approach enables a scalable tradeoff between data rate, latency, overhead, and reliability according to the running application.

The standardization of LTE was a major step towards International Mobile Telephony (IMT)-Advanced. Further releases of LTE also referred to as LTE-Advanced [28] aim at even higher data rates. For this, the performance potential of carrier aggregation, enhanced multi-antenna support, improved support for heterogeneous deployments, and relaying is being investigated [29].

Reviewing the most important features of the LTE-system, we can state that it is mainly designed to support the requirements of broadband data services. For narrowband applications with only sporadic transmissions LTE is not efficient in terms of spectrum allocation, energy usage, and cost. Moreover, the limited capabilities of low-complex end-nodes with respect to RF have not been considered at all. Therefore, many requirements listed in section 3 are not yet supported.

A 3GPP study item with focus on Machine Type Communications (MTC) was primarily based on a respective configuration of the existing system without adapting the air interface itself or facilitating interfaces to capillary networks [30], [31]. Scalable and cheap because simple M2M communications is by far not enabled with these suggestions.

4.3 IEEE 802.11

In 1997 The Institute of Electrical and Electronics Engineers (IEEE) developed and released first 802.11 standard. The 802.11 standard is actually set of standards for wireless local area network (WLAN) communication, developed by the IEEE LAN/MAN Standards Committee in the 5 GHz, 2.4 GHz and 900 MHz public spectrum bands. The 802.11 standards are widely known as "WiFi".

There are various 802.11 standards but some popular ones are: 802.11a, 802.11g, 802.11b and recently 802.11n, because of its increased speed and due to MIMO technology. The speed of 802.11 systems is distance dependent.
IEEE 802.11a runs in the 5GHz spectrum, and used with the 802.11h extensions, it gives 23 non-overlapping channels. IEEE 802.11a can run up to 54Mbps, but only if the device is less than 50 feet from an access point.
IEEE 802.11b runs in the 2.4GHz range and has three non-overlapping channels. It can handle long distances, but with a maximum data rate of up to 11Mpbs.
IEEE 802.11g runs in the same 2.4GHz range, but it has a higher data rate of 54Mbps if the device is less than 100 feet from an access point.
IEEE 802.11n builds upon previous 802.11 standards by adding Multiple-Input Multiple-Output (MIMO) technology, which employs multiple transmitters and receiver antennas to increase data throughput. 802.11n can have up to 8 antennas, but most of today’s access points use 4.

Wireless connections can be made in ad-hoc mode or infrastructure mode. Ad-hoc mode (also known as "peer-to-peer" mode), or Independent Basic Service Set (IBSS), is simply a group of computers talking wirelessly to each other with no access point (AP). It is limited in range and functionality. Infrastructure mode’s BSS uses one AP to connect clients. The range of the AP’s signal, called microcell, must encompass all clients. The Extended Service Set (ESS) uses multiple APs with overlapping microcells to cover all clients. Microcells should overlap by 10–15 percent for data and 15–20 percent for voice traffic. Each AP should use a different channel. “Pico” cells, with even smaller coverage areas, can also be used. Workgroup bridges connect to devices without a wireless network interface card (NIC) to allow their access to the wireless network.

The use of wireless products falls into three categories:

- Client access, which allows mobile users to access the wired LAN resources
- Wireless connections between buildings
- Wireless mesh

Wireless mesh networks can span large distances because only the edge APs connect to the wired network. The intermediate APs connect wirelessly to multiple other APs and act as repeaters for them. Each AP has multiple paths through the wireless network. The Adaptive Wireless Path (AWP) protocol runs between APs to determine the best path to the wired network. APs choose backup paths if the best path fails.
WiFi has brought a few advantages over wired LANs, but also a few disadvantages. Main disadvantage is low coverage, usually limited to indoor or small outdoor settings in both infrastructure and ad-hoc modes. WiFi uses the unlicensed 2.4GHz spectrum, which often crowded with other devices such as Bluetooth, microwave ovens, cordless phones, or video sender devices, ZigBee and among many others. This may cause degradation in both, performance and size of covered area.

Wireless LANs (WLAN) transmit and receive data using radio or infrared signals, sent through an access point (AP), and usually does not require radio frequency (RF) licenses. WLANs are local to a building or a campus and are an extension of wired network.

Main characteristics of WLAN are the following:

- WLANs use Carrier Sense Multi-Access/Collision Avoidance (CSMA/CA) instead of Carrier Sense Multiple Access / Collision Detection (CSMA/CD)
- Wireless data is half-duplex. CSMA/CA uses Request to Send (RTS) and Clear to Send (CTS) messages to avoid collisions.
- Radio waves are susceptible to interference, multipath distortion and noise. Their coverage area can be blocked by building features, such as elevators. The signal might reach outside the building and lead to privacy issues.
- WLAN hosts have no physical network connection. They are often mobile and often battery-powered. The wireless network design must accommodate this.
- WLANs must adhere to each country's RF standards

SSID (Service Set Identifier) is a common network name for devices in a WLAN system. An SSID prevents access by any client device that does not have the SSID. SSIDs can be broadcast by an AP or statically configured on a client, but the client must have the same SSID as the AP to register with it. SSID names are case sensitive.

There are various security methods in the WLANs:

- MAC ID filtering
- Static IP addressing
- WEP (Wired Equivalency Privacy) encryption-this is deprecated algorithm secure IEEE 802.11 wireless networks,
- WPA - WiFi Protected Access (WPA) is an early version of the 802.11i security standard that was developed by the WiFi Alliance to replace WEP,
- WPA2 - WPA2 is a WiFi Alliance branded version of the final 802.11i standard. The primary enhancement over WPA is the inclusion of the AES-CCMP algorithm as a mandatory feature, LEAP - This stands for the Lightweight Extensible Authentication Protocol. This protocol is based on 802.1X and helps minimize the original security flaws by using WEP and a sophisticated key management system. This also uses MAC address authentication. LEAP is not safe from crackers,
- PEAP - This stands for Protected Extensible Authentication Protocol. This protocol allows for a secure transport of data, passwords, and encryption keys without the need of a certificate server. This was developed by Cisco, Microsoft, and RSA Security.
- TKIP - This stands for Temporal Key Integrity Protocol and the acronym is pronounced as tee-kip. This is part of the IEEE 802.11i standard. TKIP implements

per-packet key mixing with a re-keying system and also provides a message integrity check. These avoid the problems of WEP.

- RADIUS - This service provides an excellent weapon against crackers.
- WAPI - This stands for WLAN Authentication and Privacy Infrastructure. This is a wireless security standard defined by the Chinese government.
- Smart cards, USB tokens, and software tokens

WLAN is used as a capillary network technology for M2M networks. Also, WLAN is an example of M2M communications networks (enables communications between the M2M Gateway and M2M application). WLAN fulfils requirements for M2M networks. WLAN-based devices can be easily deployed in an existing WLAN network infrastructure, also these devices will provide usage of many networking protocols and web services, such as SNMP for device configuration and management, IP protocol, usage of security features for data protection and so on.

4.4 ZigBee

ZigBee is a low-power, short-distance wireless communication standard designed by ZigBee Alliance [32], based on the IEEE 802.15.4 Low-Rate Wireless Personal Area Network (WPAN) standard. It uses the license-free ISM bands either 2.4GHz or 868/915 MHz. Network standard allows unicast, broadcast and groupcast messaging in ad-hoc self-created networks. Based on that messaging scheme, ZigBee defines three different network topologies:

- Mesh: Every node has the possibility of reaching its destination through any of its neighbors. The elements use a simplified version of AODV routing protocol to construct their routing tables.
- Cluster tree: Network routing directs packets up and down the tree structure created through network formation until they reach their destination. This topology demands the links to be active at all times, since the breakage of one may cause re-formation of the tree structure.
- Star: There is a coordinator node which reaches all the other members in a single-hop way, the rest communicates with other nodes by using the coordinator as relaying node in order to deliver their messages to destination.

As can be derived from the topology descriptions, nodes within a ZigBee network can play three different roles: *Coordinator* (stores information about the network and provides connection to other networks), *router* (capable of running application functions and relaying data from other devices) and *end devices* (it only communicates the information generated to its neighbors but with no critical role in the network topology). The following figure shows different topologies identifying the actors and their positions within the network in each of the ZigBee topologies.

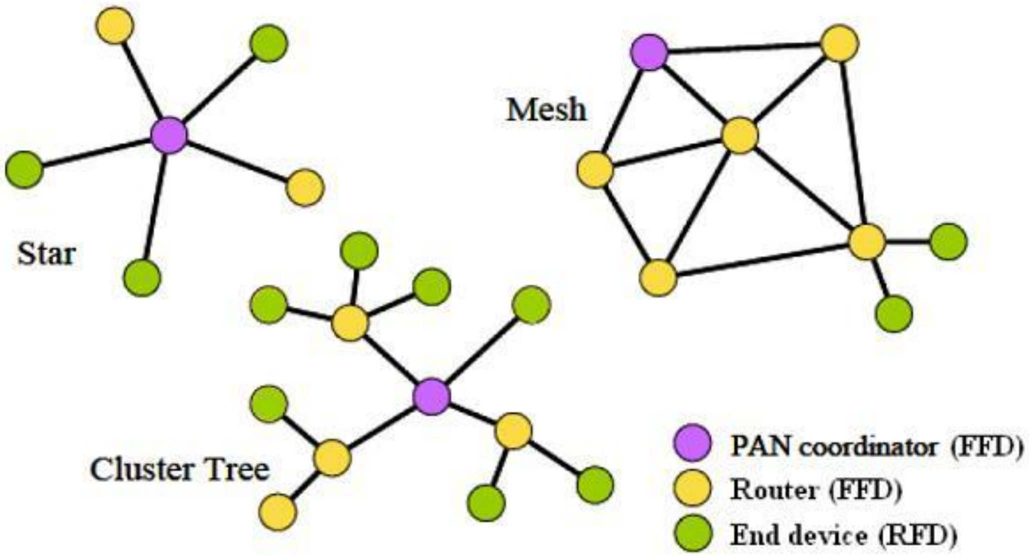

Figure 4.2: ZigBee network topologies and actors

IEEE 802.15.4 defines PHY and MAC OSI levels and ZigBee acts over these levels defining the network layer functions in charge of managing message delivery and routing. Figure 4.3 shows the different layers composing ZigBee protocol stack. An application support sub-layer for providing end manufacturers access to lower layers and a security service provider acting in these two layers are depicted.

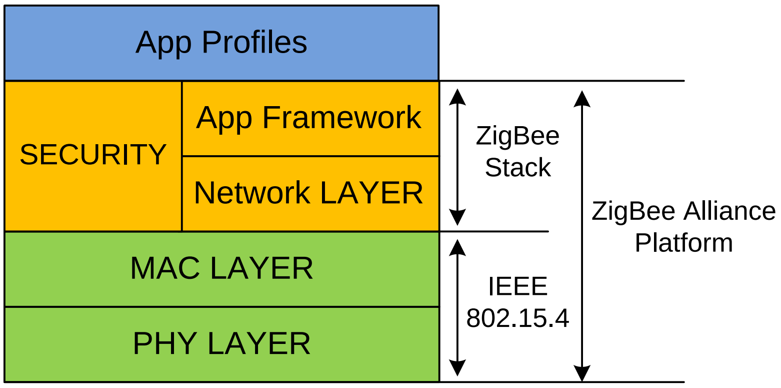

Figure 4.3: ZigBee architecture stack (source ZigBee Alliance)

Error Control in ZigBee networks includes a hand shake protocol to confirm the correct delivery of packets. Furthermore, the standard includes security aspects in each layer, for instance at the layer for network command frames and at the layer for application support sub-layer frames. It also describes two security modes:

- *Standard Mode:* Based on two network keys, application security via network key and the ability to switch these keys. Optional use of Application Link Keys for pairs of communicating devices at APL.
- *High Security Mode:* Implemented only in ZigBee Pro devices, it is composed of two network keys and separate link keys for pairs of communicating devices at the application layer. It provides a mechanism for entity authentication between all pairs of communicating devices within the network.

Regarding all features described, ZigBee has proven to be a good option to provide communication in M2M networks with low-power constraints and high-density mesh topologies. Nevertheless, there are some characteristics that make ZigBee by itself unsuitable for certain assumptions of the project.

One of the most relevant disadvantages when trying to integrate ZigBee into EXALTED is the lack of mechanisms to provide E2E connectivity of different capillary networks. Neither ZigBee nor LTE provide this capability to connect M2M devices residing in different networks. This missing feature, combined with the fact that it uses IEEE addresses instead of IP ones, disabling common routing protocols and external visibility of the M2M devices from outside the capillary network, makes the combination of ZigBee and LTE useless for proving EXALTED assumptions. Modifications on either LTE network (enabling this E2E features) and in ZigBee (providing address translation for external communications) should be done.

In addition to these two main cons, there are some other disadvantages, such as security and coverage. Security can be regarded as a disadvantage not at the level that is guaranteed by ZigBee, but at the level of complexity that necessitates the selection of the most appropriate scheme in every scenario [32]0. Coverage can be a problem in low-density networks, as distances between nodes higher than a hundred meters are not reachable with ZigBee's low-power radios systems.

5. Initial EXALTED System Concept

5.1 M2M system concept requirements and challenges

M2M has an extremely wide range of application domains covering areas like environment monitoring, remote health service provisioning, intelligent building and intelligent transport etc. In each of these domains, a plethora of potential services is envisioned, each with its own set of requirements (network quality of service, delays, etc.), with different traffic patterns generated (a few bytes once a year to MB daily) and with varying number of potential users and devices (machines) involved in each service.

The scale, i.e. the number of non-human users in M2M together with the simplification/automation of the management procedures of the machines are the most critical factors driving the activities aimed at designing modifications of mobile networks for efficient support of M2M services.

However, a number of challenges arise, if various currently envisioned services (some of them analyzed in the context of the EXALTED project) and those that are yet to be envisioned in the future are combined together and then mapped on a single mobile network and even a single radio cell,. The existing base stations (eNodeBs) are designed to serve a certain number of users. With the increase of users it is possible to some extent to expand the hardware capabilities of eNodeBs or to add additional access points in an area. However, the combined M2M scenarios can result in a large number of mobile subscribers active in an area, adding on top of the human users a number of connected cars, trucks, buses, a number of personal devices that human subscribers carry with them as well as various other machines always present in a radio cell, like connected lampposts, waste bin, vending machines, fridges, houses, buildings, etc. Expanding the network by simply adding additional hardware is not the most viable solution for cost reasons, so more efficient solutions are required. Due to the nature of the M2M services, it is possible to imagine that waste bins will report periodically about the level of garbage in each of them, traffic lights about the traffic intensity and houses/apartment blocks about the energy consumption. If notifications from all machines coincide, the number of simultaneous requests for network connections would be huge and would definitely cause problems and degradation of service for other users (one could even think of a denial of service attack on a mobile network by synchronizing a large number of machines; all house and car alarms could be triggered simultaneously during a storm). Such sudden jump in the number of connections could cause problems not just for the serving radio cell, but also for the core network, stretching its capability to serve multiple users simultaneously.

Furthermore, some M2M services are rather agnostic to the network delays and do not require high-level of guarantee that a message will be delivered in a very limited time to the destination (for example notifying the waste management company that the level of garbage in a waste bin is getting close to the maximum can be delivered inside a window of several minutes, possibly hours). On the other hand, there are M2M services with very strict delay requirements and high delivery guarantees, like fire alarms or gas leakages. The network in those cases has to ensure that such traffic is given priority over other ongoing services. While this is possible to achieve in the current networks, for example by providing private access points for certain users, such configuration implies a fair amount of manual configuration which makes such services not really economically viable, mainly due to usually small amount of data that individual M2M devices are generating.

Configuration of M2M devices and their provisioning in a mobile network is, in general, an important aspect of the M2M service chain. Due to the scale and expected revenue per device (which is much lower than the revenue per human subscriber) it is important to automate this step as much as possible and limit involvement of mobile operators in the process. This is extremely important if M2M is to expand to the mass market where various consumer electronic devices and other mass market objects might become connected. In such scenarios, the objects will come with embedded connectivity (for example a washing machine will be available with M2M connectivity already integrated, i.e. with appropriate SIM cards) and it will be up to the owners of these objects to select a (mobile) network they wish to use by simply configuring it directly on the washing machine without any need to visit mobile operators and obtain new SIM cards.

This also leads to another interesting aspect of the M2M in relation to the business cases and the way M2M services can be charged to the users. Current practice is that data services are primarily charged based on the amount of data transferred. As the majority of devices will generate small amounts of data, such a charging model might not be the most viable one for mobile operators. On the other hand, for the users of M2M services, the value of information transferred between the M2M devices is usually not measured by the amount of data transferred, but by other benefits like cost reduction or more efficient processes etc. Therefore, it could be of interest for mobile operators to investigate pricing models on the value of information as the main point rather than on the amount of data transferred.

In order to enable seamless connectivity for everyday objects, it is of great importance to reduce the cost of M2M terminals/modules. This is particularly true for LTE, as the current LTE modules are significantly more expensive than GSM/GPRS ones. The cost reduction can come from the scale of operation and the general advancements in the production technology, but can also be achieved through simplification of the functionality that such modules have to support. For example, a number of modules will be embedded in devices that are not mobile and as such will not require support for mobility. Likewise, the majority of M2M modules will be used in low throughput applications and hence do not require support for high data throughput.

Further savings can be achieved by optimizing protocols and procedures on the network side, taking into account the characteristics of the M2M services. For example, as already stated above, many M2M devices will generate data in regular intervals. This can be utilized to mobile network’s advantage by scheduling the transfers in such a way to minimize the simultaneous number of connections, while respecting the specific application requirements. Moreover, a number of M2M devices will interact with one single point on the far end (for example, all waste bins will communicate with waste management company servers) which could be used to further optimize the network resources.

Having the above in mind, the goal of the EXALTED project is to design an LTE overlay capable of providing functionality tailored to the M2M requirements without breaking the LTE procedures and protocols already in place for the regular LTE terminals. This is in analogy with GPRS’ relation to GSM or HSPA to WCDMA, where improvements of the basic technologies were introduced and were available for capable terminals, but were not disrupting functionality of mobile terminals not supporting this new functionality. While in these two cases, the improvement is visible, i.e. higher throughputs, in the case of LTE-M, it can be seen more as a downgrade of the full functionality to the bare minimum required by the M2M services thus facilitating usage of simpler and cheaper M2M modules.

5.2 High-level system architecture

Based on the consideration of the requirements and challenges for a highly scalable communication system enabling cheaper operation and services compared to existing solutions, we propose a high-level architecture of the M2M system shown in Figure 5-1. In the following, the key network elements and their functionalities as well as the types of communication within this network will be described.

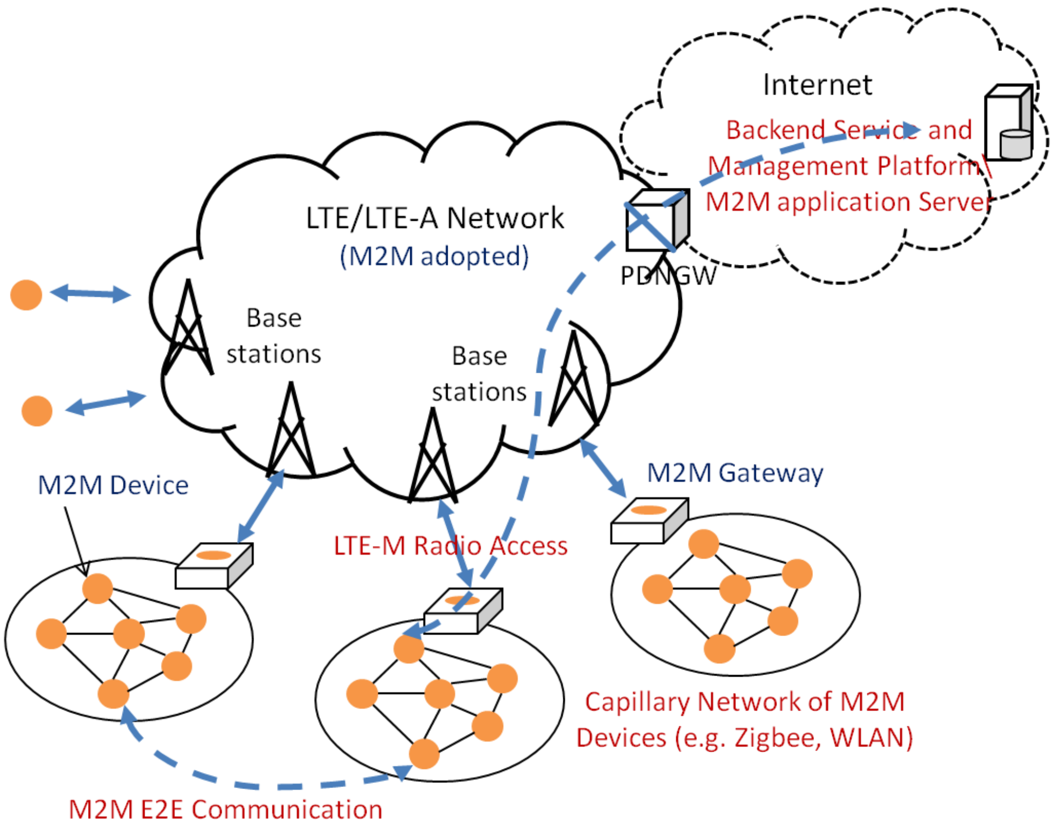

Figure 5.1: The EXALTED System concept

The main M2M system components are the M2M devices, the M2M gateway, the LTE-M enabled base station, the core network and the M2M application servers, which offer the end-to-end M2M services. We assume the core network (Evolved Packet Core, EPC) and the application server as given and do not expect further enhancements out of EXALTED.

In the following, we distinguish between two different types of communication in this network, namely direct access of the M2M devices to the base station, and access through a gateway. The functionality and the technical requirements of the individual components can differ in both cases.

1. Direct access: This type of communication is needed if the M2M devices are distributed in a wide area. This could happen in specific scenarios (e.g. E-health, ITS, SMM). In such cases, the operability of the devices and the service availability must be ensured. An LTE-M connection between the M2M devices and the base station will be established.

2. Access through a gateway: In this case the M2M devices form a capillary network with specific functionalities depending on the air interface (e.g. ZigBee, WLAN, LTE-M), such as relaying or data aggregation. The radio link between the gateway and

the BS can be either based on LTE or LTE-M, i.e. the capillary network could be handled as a unified LTE or LTE-M device according to the aggregated data rate. It is important to highlight the fact that some devices must be able to support both options depending on whether or not a gateway is available. A gateway utilizing LTE-M as air interface for both the link to the M2M devices and the link to the base station can be considered as a relay. Generally, it must be ensured that the application server is able to initiate or terminate a connection with a specific gateway or M2M device. It is also important to note that each M2M gateway may provide access to different service providers.

Beside the above mentioned two types of communication, also the option for an end-to-end connection between two M2M devices must be ensured for specific applications. This connection may be between M2M devices belonging to the same capillary network. In this case, the devices may communicate either directly with each other, depending on the capabilities offered by each air interface (e.g. ZigBee, bluetooth), or through the M2M gateway. The core network is not involved.

In summary, EXALTED aims to develop an extension of the existing LTE system addressing the particular requirements and challenges of M2M, e.g. supporting an increase in the number of connected devices of several orders of magnitude compared to today's networks. This extension is called LTE-M. The EXALTED key idea is that LTE and LTE-M will coexist, i.e. LTE-M is backward compatible with LTE. In case of high data rate communications, e.g. for the link between a gateway and a base station, LTE will be employed, while for low data rates LTE-M will be the preferred solution. LTE-M will also enable a simple interface to other air interfaces, e.g. ZigBee or Bluetooth, which may be applied in the connected capillary networks.

6. Evaluation Methodology

This section firstly describes the assessment methods that will be utilized to decide whether the technical requirements can be fulfilled with EXALTED solutions or not. Moreover, we will say which assessment method is used for which technical requirement. A second sub-section briefly defines the assessment criteria, i.e. the performance metrics needed for a quantitative evaluation of algorithms and concepts. This general description is a compilation of the intended evaluation work of all project partners. It does not mean that each single contribution will be evaluated with all assessment methods and all criteria, but only with a subset of the presented methodology.

6.1 Assessment Methodology

In EXALTED, different assessment methodologies will be used. Generally, the methods can be classified into three categories:

- Analytical assessment
- Assessment by simulations
- Assessment by measurements and trials.

The following paragraphs will briefly describe the individual categories with some examples. Ideally, all technical requirements listed in section 3 can be evaluated with at least one of the three methods. For example, backward compatibility can be assessed analytically or with a testbed, demonstrating the coexistence of a legacy terminal and an LTE-M terminal in one communication system. Energy efficiency could be assessed either analytically or with simulation, whereas successful remote software updates of devices can be only evaluated with a testbed. The complete list of technical requirements can be found at the end of this section.

6.1.1 Analytical assessment

An important example of the analytical assessment is the link budget analysis. With this method, an expectation of the range of a radio link can be given depending on the path loss model, the carrier frequency, antenna heights, antenna gains, transmit power, receiver sensitivity, noise figure, implementation loss, filter and cable losses, and wall penetration loss. Furthermore, mean SINR distributions predominantly depending on geometric parameters, not changing with time, can be derived analytically. Moreover, the efficiency of protocols often can be determined without simulation, as well as the required effort for signal processing, by counting the number of required additions and multiplications of an algorithm. Finally, upper and lower performance bounds can be expressed analytically in many cases. A very simple example is the data rate of 2x2 spatial multiplexing whose upper limit is twice the single antenna performance.

6.1.2 Simulation

Simulation is a prevalent method to assess the performance if the considered system is too complex for analytical assessment and trials. Simulation is typically based on an environment that is described by input parameters, e.g. the cell size or the number of transmitted packets. Furthermore, statistical measures, e.g. the standard deviation of a fading process, controlling other variables are typical input parameters. In addition, important inputs to a simulation are simulation models. Examples are channel model and path loss model. Generally, a model is a simplification of the reality and is often based on the results of lab and field measurements. The disadvantage of simulations is the high expenditure of time needed to obtain statistically stable results. In EXALTED, different types of simulations will be used:

(Multi-) link-level simulation: With this type, one or more isolated radio links on the PHY-layer are considered. Typically, a link-level simulator consists of a transmitter part, where the baseband signal processing (coding, interleaving, modulation, frame building etc.) is implemented, the respective receiver part (decoding, demodulation etc.), and a model of the radio channel. A link-level simulation is a good means to assess the complexity and the performance of baseband algorithms in the receiver chain, e.g. by observing the bit error ratio at the output of the decoder.

System-level simulation: In contrast to link-level, system-level simulators consist of a multitude of transmitters and receivers in a multi-cell deployment. Often the PHY-layer is considered by an abstraction model mapping SINR values to throughput values. The aim of a system level simulation is to assess the performance of the scheduler or an interference coordination concept by observing indicators like coverage and spectral efficiency.

The simulation tools that will be used in EXALTED are property of the respective project partners and might be further extended according to the needs. Although no common simulation tools will be utilized, comparability of results will be guaranteed through calibration. The calibration process is not yet defined in detail, but it will rely on reference cases. For LTE-M functionality, we would prefer reference cases from 3GPP, once they will be defined.

6.1.3 Measurements and trials

With analytical assessment and simulation, trials are the third essential method to evaluate the proposed solution. Trials have the following purposes:

- Measurements of physical quantities to be compared to the analysis or simulation results
- System integration
- Practical implementation of features for evaluation

Measurements of physical quantities: To be meaningful, the trials must setup testbeds that resemble real systems as close as possible. Hence, assuming perfect testbeds, when measuring physical quantities, substantial deviations of the measures from analysis or simulation results indicate that some key hypotheses in the system are missing or that the model used to produce the analysis or simulation results is not ideal. Examples of such physical quantities are throughput, latency, spectrum spread, etc. However, testbeds can never be perfect, that is, cannot reproduce real conditions perfectly. Reasons for that are to be found in feasibility and costs of the testbeds. For example, scalability over billions of devices cannot be practically tested in labs. Therefore, measures gained through testbeds must be accompanied with a mention of the experimental hypotheses and their validity range. Whether the conditions posed on testbeds represent meaningful hypotheses is usually left to the appreciation of the telecom community.

System Integration: For a big communication system like EXALTED, whose design requires miscellaneous skills, problems are divided into more specific ones, easier to solve. Once one or more partial solutions for a specific topic are found, the reverse path is to integrate them to get a global solution. This integration step represents a good opportunity to spot incompatibility issues not caught during the design phase. Of course, solving incompatibility issues is expected to have consequences on EXALTED architecture and may require a new design review. Among sources of incompatibility, the most common one emerges from these numerous required skills. For example, it is not obvious at first sight whether the end-to-end communication protocols will be compatible with a future LTE-M backbone because the levels addressed are not the same.

Practical implementation: Some highly desired features may prove to be too complicated for practical use when one tries to implement them. For example, self-healing systems are a neat feature whose implementation, depending on the required reliability level, may turn out to be hardly feasible because of the difficulty to access some diagnostic data. Trials may be lab trials or field trials. Lab trials occur in a controlled environment, especially for radio conditions. It is then easier to modify some key parameters in this testbed. Field trials on the contrary are closer to real conditions but with more uncontrolled parameters, results may be more difficult to interpret. Hence, field trials are the logical step after lab trials.

The following table indicates with which assessment method we will find out whether a technical requirement from section 3 is fulfilled or not.

Table 6.1: Mapping of technical requirements to the assessment methodology

ID	Title	Assessment methods
FU.1	Support of large number of devices	Analytical assessment; Simulation
FU.2	Efficient spectrum management	Analytical assessment; Simulation
FU.3	Support for diverse M2M services	Simulation;
FU.4	Network initiated packet-data communication	Simulation; Measurements and trials
FU.5	Local and remote device management	Simulation; Measurements and trials
FU.6	Unique identity for devices	Simulation; Measurements and trials
FU.7	Security and provisioning	Measurements and trials
SV.1	Overall QoS	Analytical assessment, Simulation, Measurement and trials
SV.2	Allow multiple service providers on M2M devices	Analytical assessment
SV.3	Efficient provisioning of a set of M2M equipments	Analytical assessment, Measurement and trials
SV.4	Change of subscription	Measurement and trials
SV.5	Delegation and distribution of functionality	Simulation, Measurement and trials
SV.6	Security	Analytical assessment
NT.1	Heterogeneous networks	Analytical assessment; Simulation, Measurements and trials
NT.2	LTE-M backward compatibility	Analytical assessment, Measurement and trials
NT.3	Minimum number of modifications in network infrastructure	Analytical assessment
NT.4	Support of multi-hop communication	Analytical assessment; Measurements and trials
NT.5	Half duplex operation of terminals	Analytical assessment; Measurements and trials

NT.6	End to end device to device communication	Analytical assessment; Measurements and trials
NT.7	Flexible addressing scheme	Analytical assessment; Measurements and trials
NT.8	Mobility management	Analytical assessment
NT.9	Reliable delivery of a message	Analytical assessment; Simulation
NT.10	High node density	Analytical assessment, Simulation
NT.11	Traffic aggregation	Analytical assessment; Simulation
NT.12	Self-diagnostic and self-healing operation	Analytical assessment
NT.13	Multicast and broadcast communication	Analytical assessment; Simulation, Measurements and trials
NT.14	End-to-end QoS system	Analytical assessment
NT.15	End-to-end session continuity	Analytical assessment
NT.16	Support for dual stack IPv4/IPv6	Analytical assessment; Simulation
NT.17	Reduced signaling	Analytical assessment
NF.1	Scalability	Analytical assessment
NF.2	Energy efficiency	Analytical assessment, Simulation
NF.3	Extensibility and adaptability	Analytical assessment
NF.4	Real time performance	Analytical assessment; Measurements and trials
NF.5	Congestion control mechanism	Analytical assessment
NF.6	Address space scalability	Analytical assessment
NF.7	Control signaling integrity protection and encryption	Analytical assessment; Simulation;
NF.8	Service provisioning for MNO/SP customers	Analytical assessment; Measurements and trials
NF.9	Roaming support	Analytical assessment; Simulation; Measurements and trials
DV.1	Self organized M2M equipments	Measurements and trials
DV.2	Reliable M2M equipments	Analytical assessment; Simulation; Measurements and trials
DV.3	Energy efficient duty cycles	Analytical assessment; Simulation; Measurements and trials
DV.4	Location information	Measurements and trials
DV.5	Location locked M2M equipments	Measurements and trials
DV.6	Gateway detection and registration	Measurements and trials
DV.7	Protocol translation at the gateway	Measurements and trials
DV.8	Information routing at the gateway	Measurements and trials
DV.9	M2M equipment wake-up	Measurements and trials
DV.10	Remote configuration	Measurements and trials
DV.11	Software update over the air	Measurements and trials

6.2 Assessment Criteria

In this section we list several assessment criteria that can be utilized to decide whether or not the technical requirements in section 3 can be fulfilled by applying a certain algorithm:

- **Energy efficiency:** As saving battery lifetime at the device is one major challenge in EXALTED, energy efficiency is a key criterion for the evaluation of an algorithm or a system concept. It can be given in Joule/bit or Joule/session and indicates the consumed energy at the device per transmitted information bit, and the consumed energy at the device per transmission session, respectively. The consumed energy consists of the energy needed for signal processing (uplink and downlink) and the transmission energy in uplink. An information bit is defined as the raw payload of the transmission, redundancy due to forward error coding, pilot bits and any kind of control information that are not information bits. A transmission session is defined as the sum of transmitted bits required for one activity cycle of the device including all overhead (control information, encryption etc). A simple example for such a session is the transmission of one single blood pressure measurement by an E-health sensor.

- **Number of supported devices per base station:** This is yet another assessment criterion specific for M2M is the number of supported devices per base station. In section 2, it has been elaborated that the envisaged use cases may require a lot of devices within a relatively small area, i.e. within one single radio cell. Therefore, the number of supported devices per base station is an important evaluation criterion for the EXALTED system concepts.

- **Peak-to-Average Power Ratio (PAPR)**, often referred to as crest factor: This is a PHY layer metric and defined as the peak amplitude of a waveform divided by its root mean square. The higher the PAPR, the more challenging and expensive is the design of the power amplifier, and the more severe is the distortion of the transmitted signal. For a low-cost M2M device, a waveform with high PAPR is not appropriate. Therefore, alternative waveforms with desirably low PAPR will be investigated in EXALTED. Instead of PAPR, also the Cubic Metric (CM) can be evaluated.

- **Overall latency:** This is defined as the time duration between the occurrence of an event, e.g. taking a measurement of blood pressure, and the reception of the information at the target, e.g. an application server in the hospital, where the blood pressure is observed.

- **BER, PER, SINR, throughput, and their statistics:** In particular for PHY and MAC algorithms, performance criteria like bit error rate (BER), packet error rate (PER), throughput and coverage, well known and established in the evaluation of cellular mobile radio communication systems, will be utilized in EXALTED as well.

- **Complexity:** This criterion is closely related with energy efficiency. The energy needed for signal processing increases with the complexity of the algorithms. Therefore, low-complex solutions with a predictable number of computing operations are envisaged. Low complexity will also help to keep the costs for the device and for the respective M2M services small.

7. Conclusions

This deliverable offers an overall and high-level description of the EXALTED system concept – the architecture that combines widely-deployed M2M communications with standardized core network technologies, in this case - LTE. Changes must be done, in a way that co-existence with the legacy systems is preserved, but significant level of interoperability and consolidation in this hybrid “M2M-LTE” model must also be achieved.

The following three scenarios are described as the most applicable examples of LTE-M: Intelligent Transport System (ITS), Smart Metering and Monitoring (SMM) and E-healthcare. It can be noticed that even though the scenarios seem to be different in various aspects, some common characteristics regarding topologies, types of communication, and key elements can be recognized, and many technical requirements can be applied to all.

The requirements are presented in generic and simple way, and they serve for many purposes: they are guidelines for other WPs of EXALTED; they serve as the baseline for future implementation of LTE-M; they determine a common framework and concept which covers all relevant use cases of EXALTED, also applicable to other use cases. For the purpose of convenient referencing and understanding, the requirements are grouped into several categories: functional, service, network non-functional and device requirements. Dependencies between many requirements exist and are clearly indicated. In case of a deployment of an LTE-M system, a specific set of these requirements need to be satisfied, depending on their nature and purpose.

The LTE-M system consists of an LTE-M core network and capillary networks, which can be some of the standardized ones, such as WiFi and ZigBee. The use of LTE-M to capillary networks attached to a core LTE-M network is also allowed. End devices communicate with each other within the capillary network, and the communication outside the capillary network is done via Gateways. A Gateway has at least one LTE-M interface, facing an LTE-M base station.

The final section of this document describes assessment and evaluation methodologies for future implementation of LTE-M. Three main methods are recognized: analytical assessment, simulation, and measurements and trials. They are referenced by the use cases in which they can serve as assessment tools. These methods have to be further improved in EXALTED; brief high-level explanations are provided for the sake of completeness.

Acronyms

Acronym	Meaning
3GPP	3rd Generation Partnership Project
AMM	Advanced Meter Management
AODV	Ad hoc On Demand Distance Vector
AP	Access Point
APL	Application Layer
ARQ	Automatic Repeat-reQuest
AWP	Adaptive Wireless Path
BS	Base Station
C2C	Car-to-car
CAN	Controller Area Network
CDMA	Code Division Multiple Access
CPU	Central Processing Unit
CSMA/CA	Carrier Sense Multi-Access/Collision Avoidance
CSMA/CD	Carrier Sense Multi-Access/Collision Detection
CTS	Clear to Send
DHCP	Dynamic Host Configuration Protocol
DSRC	Dedicated Short-Range Communications
DoS	Denial of Service
E2E	End-to-end
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
ECG	Electrocardiogram
EHR	Electronic Health Record
EPC	Evolved Packet Core
EPS	Evolved Packet System
ERP	Enterprise Resource Planning
ESP	Energy Service Providers
ESS	Extended Service Set
FDD	Frequency Division Duplex
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GV	Gateway Vehicle
GW	Gateway
HARQ	Hybrid Automatic Repeat-reQuest
HIMSS	Health Information and Management Systems Society
HSPA	High Speed Packet Access
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IMT	International Mobile Telephony
IP	Internet Protocol
ITS	Intelligent Transport System
LAN	Local Area Network
LLC	Logical Link Control
LTE	Long Term Evolution
LTE-A	Long Term Evolution – Advanced
LTE-M	Long Term Evolution for Machines
M2M	Machine-to-Machine

M2ME	Machine-to-Machine Equipment
MAC	Medium Access Control
MAN	Metropolitan Area Network
MIMO	Multiple Input Multiple Output
MNO	Mobile Network Operator
MSISDN	Mobile Station Integrated Services Digital Network
MTC	Machine Type Communications
MU-MIMO	Multiuser MIMO
NAT	Network Address Translation
NIC	Network Interface Card
OFDM	Orthogonal Frequency-Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OSI	Open System Interconnection
PACS	Picture Archiving and Communication Systems
PAN	Personal Area Network
PAPR	Peak-to-Average Power Ratio
PC	Personal Computer
PDCP	Packet Data Convergence Protocol
PDN	Public Data Network
PEAP	Protected Extensible Authentication Protocol
PLMN	Public land mobile network
QAM	Quadrature Amplitude Modulation
QOS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RF	Radio Frequency
RLC	Radio Link Control
RTS	Request to Send
SC-FDMA	Single Carrier Frequency Division Multiple Access
SFBC	Space Frequency Block Coding
SHO	Selected Home Operator
SIM	Subscriber Identity Module
SINR	Signal to interference and Noise Ratio
SIP	Session Initiation Protocol
SL-SM	Single-Layer Spatial Multiplexing
SM	Spatial Multiplexing
SMM	Smart Metering and Monitoring
SMP	Smart Metering Provider
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SP	Service Provider
SSID	Service Set Identifier
SU-MIMO	Single User MIMO
TDD	Time Division Duplex
TD-SCDMA	Time Division Synchronous Code Division Multiple Access
TKIP	Temporal Key Integrity Protocol
UE	User Equipment
URL	Uniform Resource Locator
USB	Universal Serial Bus
V2V	Vehicle-to-Vehicle
WAPI	WLAN Authentication and Privacy Infrastructure
WCDMA	Wideband CDMA
WEP	Wired Equivalency Privacy
WiMAX	Worldwide Interoperability for Microwave Access

WLAN	Wireless LAN
WP	Work Package
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal Area Network
WPX	Work Package X
WSN	Wireless Sensor Network

References

[1] ETSI TS 102.689, Machine-to-Machine Communications (M2M); M2M service requirements. 3GPP TR 33.812, Feasibility Study on the Security Aspects of Remote Provisioning and Change of Subscription for M2M Equipment (December 2009).
[2] ETSI TR 102 691 V1.1.1 (2010-05) Technical Report, “Machine-to-Machine communications (M2M); Smart Metering Use Cases”.
[3] European Commission Standardisation Mandate M/441: "Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability.
[4] Directive 2006/32/EC of the European Parliament and of the Council of 5 April 2006 on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC, published in the Official Journal of the European Union as OJ L 114 of 27.4.2006.
[5] ESMIG Document ESMCR003-002-1.0 (October 2009): "Smart Metering Functionality Use Cases", Engage Consulting Limited (assigned by ESMIG).
[6] 3GPP TS 22.368, Service Requirements for Machine-Type Communications (April 2010).
[7] 3GPP TR 22.868, Study on Facilitating Machine to Machine (December 2009).
[8] 3GPP TR 23.888, System Improvements for Machine-Type Communications (March 2010).
[9] ETSI TR 102 863: "Intelligent Transport System (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM); Rationale for and guidance on standardization".
[10] ETSI TS 102 637-1: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirements".
[11] ETSI TS 102 637-2: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".
[12] ETSI TS 102 637-4: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic set of applications; Part 4: Operational Requirements".
[13] ETSI TS 102 636-4-1: "Intelligent Transport System (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Subpart 1: Media independent functionalities".
[14] ETSI TR 102 638: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions".
[15] 3GPP TR 22.947, Study on Personal Broadcast Service (PBS), Release 10. 9.
[16] International Workshop on Machine-to-Machine Communications, Globecom 2011, December 2011.
[17] A Balanced Cost Cluster-Heads Selection Algorithm for Wireless Sensor Networks.
[18] Energy Efficient Clustering Algorithms for Wireless Sensor Networks, ICC Workshop, May 2008.
[19] ETSI TS 102.689, Machine-to-Machine Communications (M2M); M2M service requirements
[20] The GSMA, http://www.gsmworld.com/newsroom/press-releases/2011/6040.htm
[21] ETSI GSM Specification 02.60, Digital cellular telecommunications system (Phase2+), General Packet Radio Service; Service description, Stage 1, 1999.
[22] ETSI GSM Specification 03.60, Digital cellular telecommunications system (Phase2+), General Packet Radio Service, Service description, Stage 2, 1999.
[23] ETSI GSM Specification 03.64: Digital cellular telecommunications system (Phase2+), General Packet Radio Service, Overall description of the GPRS radio interface, Stage 2, 1999.

[24] E. Dahlman, S. Parkvall, J. Sköld, P. Beming, „3G Evolution: HSPA and LTE for Mobile Broadband," Academic Press, Oxford, UK, second edition, 2008.
[25] T. Halonen, J. Romero, J. Melero, "GSM, GPRS and EDGE Performance - Evolution Towards 3G/UMTS", John Wiley & Sons, ISBN 0470 84457 4, 2002.
[26] G. Fodor, A. Furuskar, and J. Lundsjo, "On access selection techniques in always best connected networks," in ITC Specialist Seminar on Performance Evaluation of Wireless and Mobile Systems, Aug. 2004.
[27] Martsola, M., Kiravuo, T., and Lindqvist, J. "Machine to machine communication in cellular networks", In Mobile Technology, Applications and Systems, 2005 2nd International Conference on (15-17-2005), pp. 6 pp. –6.
[28] 3GPP, "LTE-Advanced," http://www.3gpp.org/LTE-Advanced
[29] S.Parkvall, E. Englund, A. Furuskär, E. Dahlman, T. Jönsson, A. Paravati: "LTE Evolution towards IMT-Advanced and Commercial Network Performance," Proc. IEEE International Conference on Communication Systems (ICCS), pp 151-155, Singapore, November 2010.
[30] 3GPP, "TR 22.368 – Service Requirements for Machine-Type Communications," Rel-10, 2010.
[31] 3GPP, "TR 23.888 – System Improvements for Machine-Type Communications," Rel-10, 2010.
[32] Understanding ZigBee RF4CE. ZigBee Alliance 2009.
[33] Naveen Sastry and David Wagner, "Security Considerations for IEEE 802.15.4 Networks", WiSE'04, October 1, 2004, Philadelphia, Pennsylvania, USA.