International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series Y
Supplement 30
(01/2016)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

ITU-T Y.4250 series – Smart sustainable cities – Overview of smart sustainable cities infrastructure

ITU-T Y-series Recommendations – Supplement 30

ITU-T

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899

For further details, please refer to the list of ITU-T Recommendations.

Supplement 30 to ITU-T Y-series Recommendations

ITU-T Y.4250 series – Smart sustainable cities
Overview of smart sustainable cities infrastructure

Summary

Supplement 30 to the ITU-T Y-series Recommendations presents the overview of infrastructure in cities. Generally, the city infrastructure can be classified as digital/ICT infrastructure and physical infrastructure.

The intelligent improvement of physical infrastructure can be achieved through the widely adoption of information and communication technologies (ICTs). In this sense, ICT acts as an enabler to construct smart sustainable cities (SSC). Consequently using ICTs in SSC results in cost and energy saving, increased economic growth, improved quality of life (QoL), and reduced environmental footprint.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y Suppl. 30	2016-01-26	20	11.1002/1000/12756

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 30 to ITU-T Y-series Recommendations

ITU-T Y.4250 series – Smart sustainable cities
Overview of smart sustainable cities infrastructure

1 Introduction

1.1 Background

There are several definitions of a city. A city can be classified according to its population density and its level of urbanization. Both variables are related to the human intervention over a populated area. Those areas with high population density appear to be the most heavily modified when compared with their original landscapes. This reflects the intensity of human activities which have taken place in the area. However, defining a city only from a statistical point of view can be misleading.

From an economic point of view, the emergence of agglomeration economies causes an increase in productivity and efficiency in a city. Meanwhile, it reduces transportation and communications costs, stimulates the labour division and promotes the development of economies of scale and increasing returns to scale. These agglomeration economies partially explain the process of urbanization, since people move to cities when companies move business there. Historically, this process has been associated with two major structural changes; firstly, the development of the agricultural and industrial sectors and secondly, the expansion of the services sector.

Nowadays, the world is facing a third structural advancement with the development and application of the information and communication technology (ICT). In accordance with this development, there have been several novel concepts for cities based on ICT. The reputed sociologist, Manuel Castells, an influential thinker on the changes caused by ICT, developed the idea of an informational city. This concept is related to the communication flowswithin a city.

It is important to recognize that in order to be part of this ICT based metamorphosis, cities need to incorporate infrastructures that have the capacity to utilize the potential of ICT and combine them with the existing infrastructure (such as building, roads, etc.). For this reason, the "convergence" ICT idea is applied to the infrastructure for "Smart Sustainable Cities (SSC)". For instance, electricity networks serve as routes outlined to telecommunications transport networks (which also develops with better control on the electrical system using supervisory control and data management (SCADA) systems). The use of buildings for the installation of raised elements such as antennas and base stations is also required.

Therefore, ICT acts as an enabler to construct SSC with its intelligent and efficient use of resources being the focus. Consequently using ICTs in SSC results in cost and energy saving, increased economic growth, improved quality of life (QoL), and reduced environmental footprint.

1.2 Stakeholders in SSC

Stakeholders refer to the major players involved in SSC establishment and functioning. The classification of these stakeholders is diverse. In particular, the classification of interdependent and standalone stakeholders distinguishes public and private institutions, local and supra-local entities, as well as commercial and non-commercial entities. The diagram[1] in Figure 1 shows an example of the interrelationships between some key stakeholders.

---

[1] Adapted from "Broadband and Local Government: evaluation of experiences and recommendations". United Nations (CEPAL), September 2007.

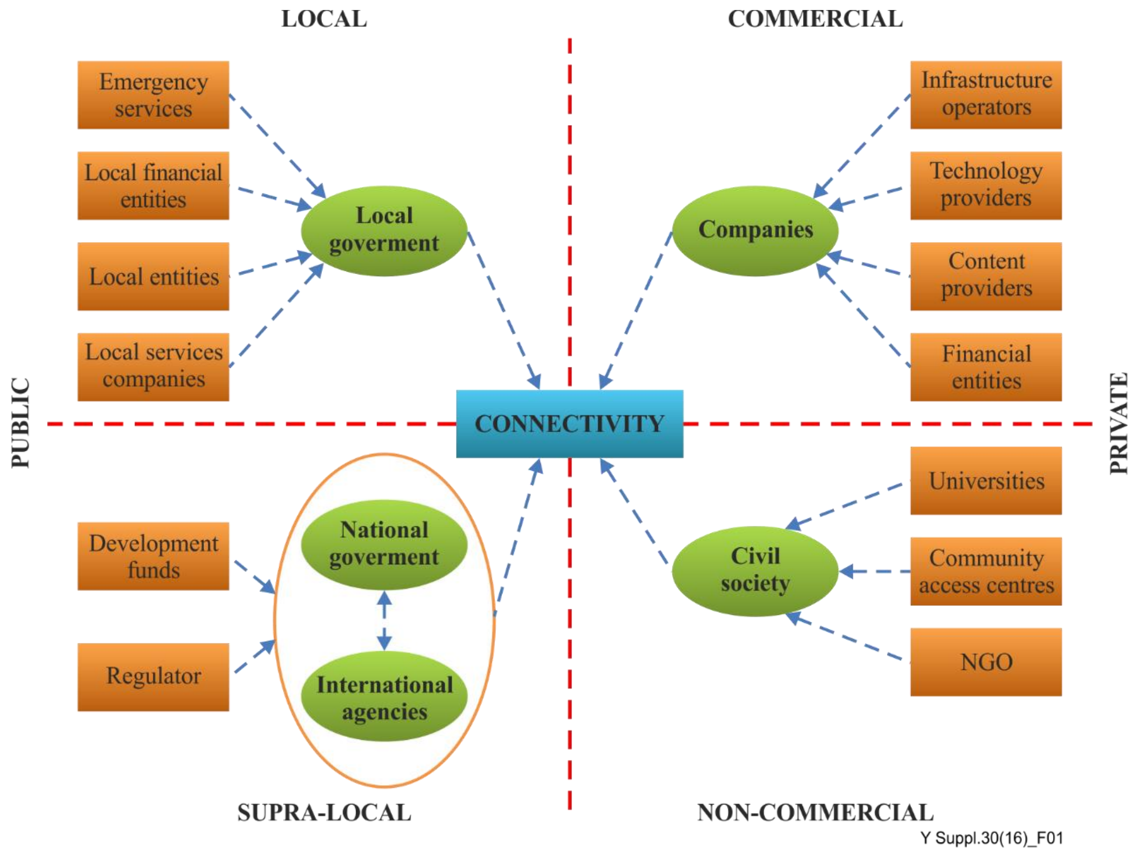


Figure 1 – Relationship between key stakeholders

Source: Ministry of Transportation and Communications of Peru.

All these actors (and other identifiable ones) will have interests linked to the idea of "Smart Sustainable City" in order to:

– Improve the quality of the citizens' life.

– Ensure sustainable economic growth to provide a better standard of life and employment opportunities for the citizens.

– Improve the welfare of the citizens, which means improving the quality of medical care, welfare, physical safety, and education, among others.

– Establish and implement a responsible and sustainable approach to environmental management.

– Strengthen measures for the prevention and management of natural disasters, including the ability to reduce the impacts of climate change.

– Provide an effective mechanism for regulatory compliance and well balanced governance, with policies and standardized processes.

A detailed analysis of stakeholders is available in the Technical Report on setting the stage for stakeholders' engagement in smart sustainable cities.

1.3 Architecture of a smart sustainable city

The architecture of SSC has been defined in the corresponding Supplement "Smart Sustainable Cities – Setting the framework for an ICT architecture",

At a high level, a meta-architecture consists of five layers as depicted in Figure 2.

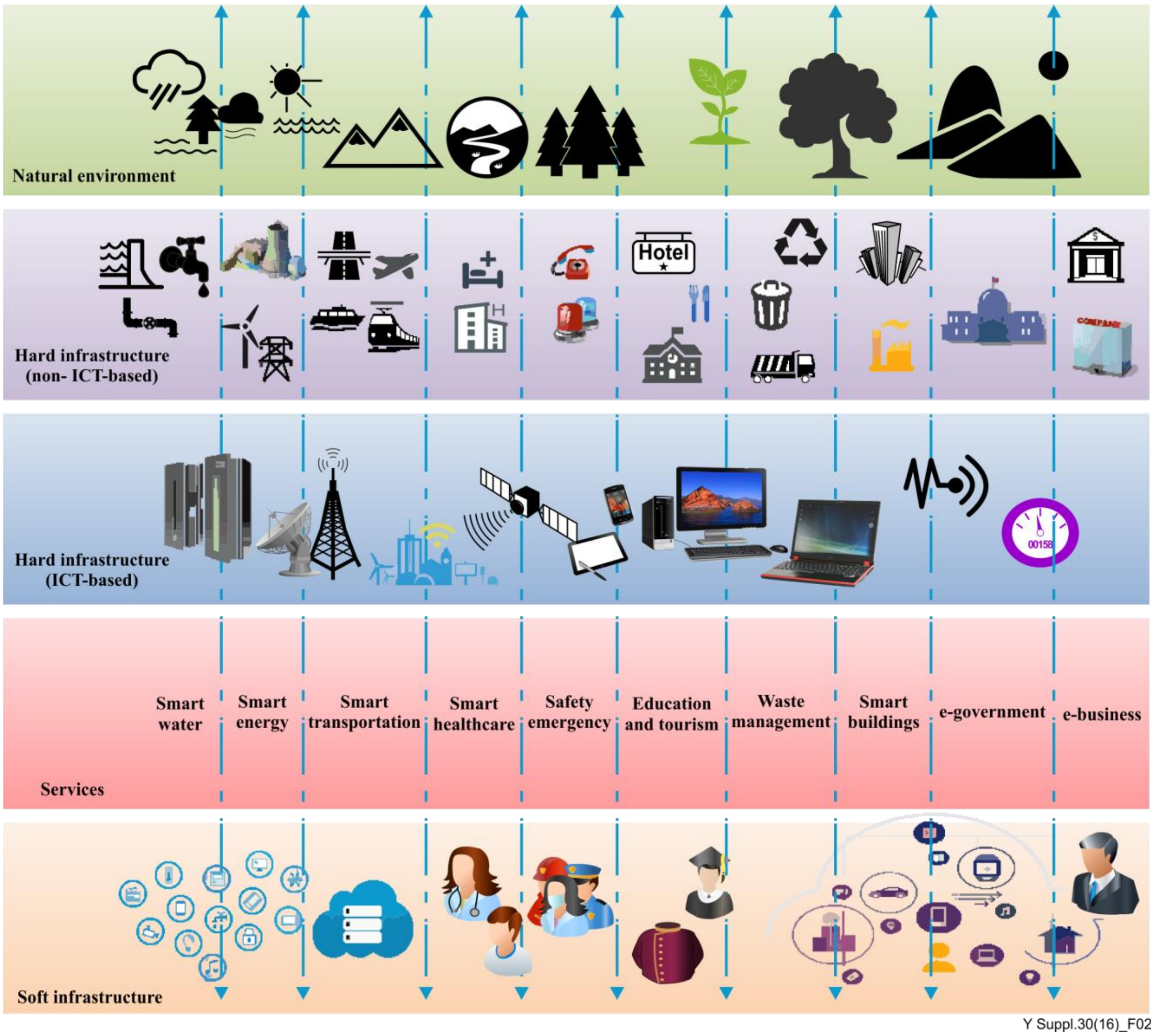


Figure 2 – Multi-tier SSC ICT meta-architecture[2]

A smart sustainable city can also be considered as a system comprising subsystems and, its ICT architecture (as depicted in Figure 3), where each subsystem addresses a different smart sustainable city service category. Finally, with regard to its technical definition, it has been seen from different views. Figures 4 and 5 demonstrate the communication view of the SSC ICT architecture, from a physical and an information flow perspective respectively. Please note that both perspectives of this view are multi-tier.

[2] According to the Supplement "Smart Sustainable Cities – Setting the framework for an ICT architecture" [ITU-T Y-Sup. 27].

Figure 3 – Subsystems of SSC ICT architecture[2]

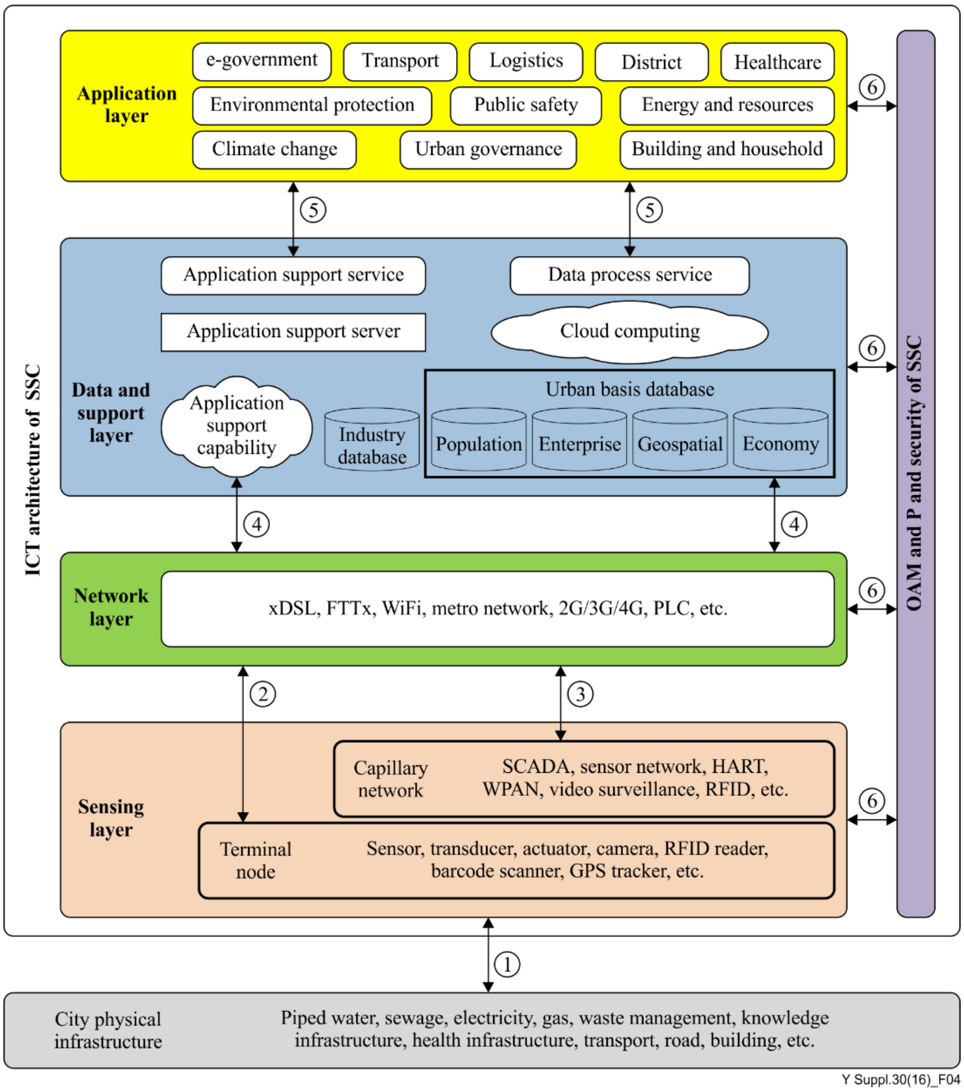


Figure 4 – A multi-tier SSC ICT architecture from communication view (physical perspective)

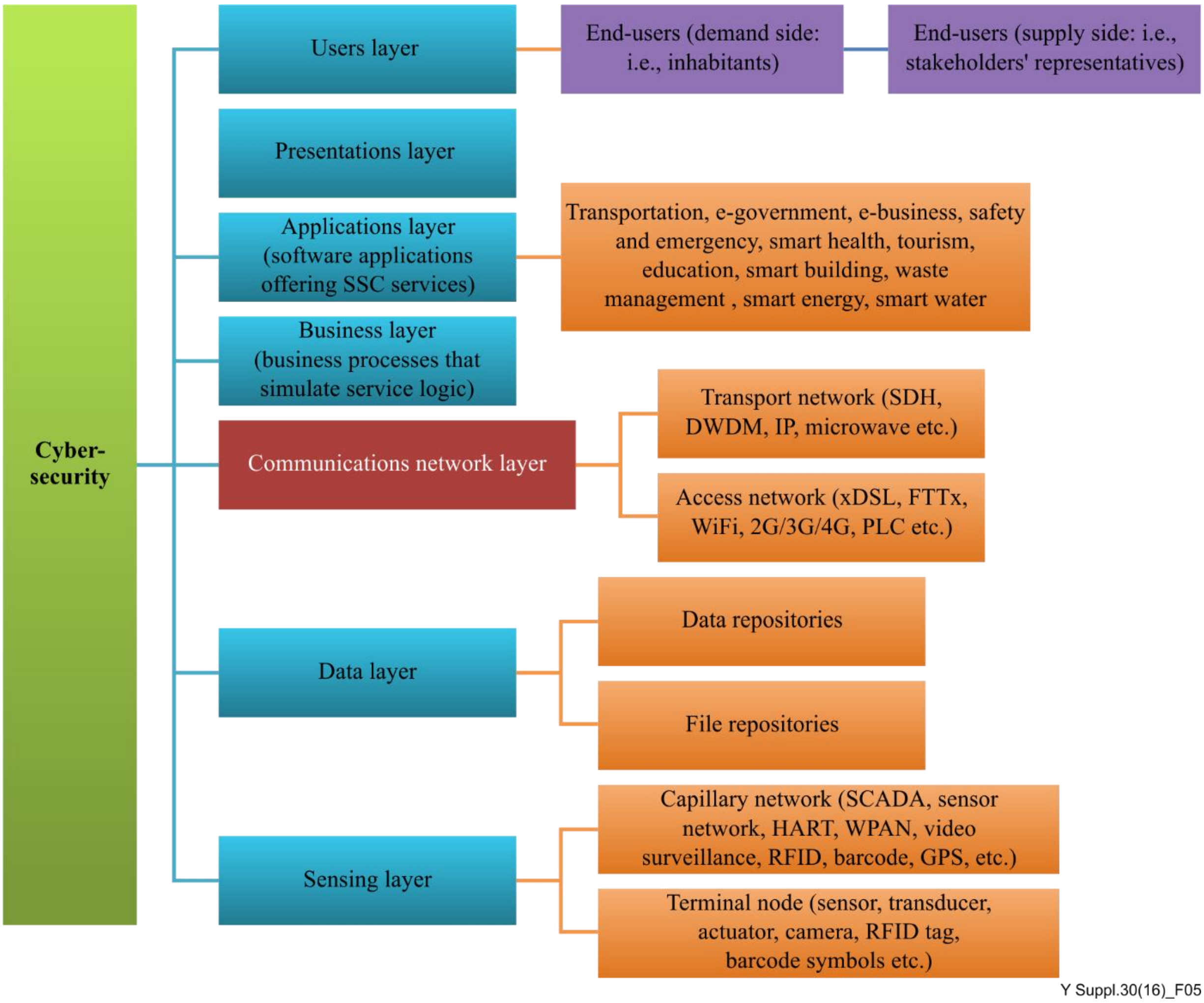


Figure 5 – A multi-tier SSC ICT architecture from communications view (information flow perspective)

Both these perspectives concern valid representations of the same architecture, one closer to the language of infrastructure developer the second more in line with the context required for information system developers. The architecture consists of the following layers (illustrated in Figure 4):

– Sensing layer: This layer consists of a terminal node and capillary network. Terminals (sensor, transducer, actuator, camera, RFID reader, barcode symbols, GPS tracker, etc.) are capable of sensing the physical world. They provide the superior "environment-detecting" ability and intelligence for monitoring and controlling the physical infrastructure within the city. The capillary network (including SCADA, sensor network, HART, WPAN, video surveillance, RFID, GPS related network etc.) connects various terminals to the network layer, providing ubiquitous and omnipotent information and data.

– Network layer: The network layer indicates various networks provided by telecommunication operators, as well as other metro networks provided by city stakeholders and/or enterprise private communication network. It is the "infobahn", the network layer data and support layer: The data and support layer makes the city "smarter". Its main purpose is to ensure the support capabilities of various city-level applications and services. Data and support layer contain data centres from industries, departments, enterprises, as well as the municipal dynamic data centre and data warehouse, established for the realization of data processing and application support.

– Application layer: This layer includes various applications that manage SSC and deliver the SSC services.

– Operation automation monitoring & protection & security framework: This framework provides the operation, administration, maintenance, provisioning, and security function for the ICT systems of SSC.

Compared to Figure 5, Figure 4 also uses the following layers:

– Users layer: It organizes SSC service end-users into groups from both the demand and the supply sides;
– Presentations layer: It contains the user interfaces (web, Apps, voice commands etc.), which stand between end-users and SSC services;
– Applications layer: It contains all corresponding software applications that realize the SSC services;
– Business layer: It consists of the business processes, which lie behind each SSC service execution;
– Communications layer: It contains the above mentioned networks, over which the SSC services are performed and transactions and data flow are realized;
– Data layer: It contains the data and file repositories, where data are created or retrieved;
– Sensing layer: This consists of terminal node and capillary network. The terminals (sensor, transducer, actuator, camera, RFID tag, barcode symbols etc.) sense the natural environment where the smart sustainable city is located and the corresponding hard infrastructure and utilities (water, transport etc.). It provides the superior 'environment-detecting' ability and intelligence for monitoring and controlling the physical infrastructure within the city. The capillary network connects various terminals to communication layer, or directly to data layer and/or application layer providing ubiquitous and omnipotent information and data.

Discussions on ICT architecture and architecture framework, as well as security aspect of smart sustainable cities are ongoing and the outcomes will be published in the relevant ITU-T document as soon as the process is completed.

2 References

[ITU-T L.1300] Recommendation ITU-T L.1300 (2014), *Best practices for green data centres.*

[ITU-T L.1310] Recommendation ITU-T L.1310 (2014), *Energy efficiency metrics and measurement methods for telecommunication equipment*.

[ITU-T L.1320] Recommendation ITU-T L.1320 (2014), *Energy efficiency metrics and measurement for power and cooling equipment for telecommunications and data centres.*

[ITU-T L.1340] Recommendation ITU-T L.1340 (2014), *Informative values on the energy efficiency of telecommunication equipment.*

[ITU-T L.1400] Recommendation ITU-T L.1400 (2011), *Overview and general principles of methodologies for assessing the environmental impact of information and communication technologies.*

[ITU-T L.1410] Recommendation ITU-T L.1410 (2014), *Methodology for environmental life cycle assessments of information and communication technology, goods, networks and services.*

[ITU-T L.1500]	Recommendation ITU-T L.1500 (2014), *Framework for information and communication technologies and adaptation to the effects of climate change.*
[ITU-T L.1501]	Recommendation ITU-T L.1501 (2014), *Best practices on how countries can utilize ICTs to adapt to the effects of climate change.*
[ITU-T L.1502]	Recommendation ITU-T L.1502 (2015), *Adapting information and communication technology infrastructure to the effects of climate change*
[ITU-T Y.4900]	Recommendation ITU-T Y.4900/L.1600 (2016), *Overview of key performance indicators in smart sustainable cities.*
[ITU-T Y.4901]	Recommendation ITU-T Y.4901/L.1601 (2016), *Key performance indicators related to the use of information and communication technology in smart sustainable cities.*
[ITU-T L.1602]	Recommendation ITU-T Y.4902/L.1602 (2016), *Key performance indicators related to the sustainability impacts of information and communication technology in smart sustainable cities.*
[ITU-T L-Sup.19]	ITU-T L.1600-series Recommendations—Supplement 19 (2015), *Key performance indicators definitions for smart sustainable cities.*
[ITU-T Y-Sup.27]	ITU-T Y.4400-series Recommendations – Supplement 27 (2016), *Smart Sustainable Cities – Setting the framework for an ICT architecture.*
[ITU-T Y-Sup.34]	ITU-T Y.4000-series Recommendations – Supplement 34 (2016), *Smart sustainable cities – Setting the stage for stakeholders' engagement.*
[ITU-T Y-Sup. 36]	ITU-T Y-series Recommendations – Supplement 36 (2015), *ITU-T Y.4550-Y.4699 - Smart water management in cities.*
[ITU-T K-Sup. 4]	ITU-T K-series Recommendations – Supplement 4 (2015) *ITU-T K.91 - Electromagnetic field considerations in smart sustainable cities*.

3 Definitions

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

3GPP	3rd Generation Partnership Project
ADC	Analog to Digital Converter
ADSL	Asymmetrical Digital Subscriber Line
AISUWRS	Assessing and Improving Sustainability of Urban Water Resources and Systems

AMI	Advanced Metering Infrastructure
ARM	Architecture Reference Model
ATM	Asynchronous Transfer Mode
BAT	Bouyant Airborne Turbine
BEMS	Building Energy Management System
BSC	Base Station Controller
BTS	Base Transmitter Station
CAGR	Compound-annual-growth
CALM	Continuous Air interface Long and Medium range
CAP	Common Alerting Protocol
CBC	Cell Broadcast centre
CDMA	Code Division Multiple Access
Cell ID	Cell Identifier
CME	CALM Management Entity
CMSP	Common Mapping Production System
CO	Central Office
CO	Communication Operator
CPU	Central Processing Unit
CRM	Customer Relationship Management
DAB	Digital Audio Broadcasting
DC	Direct Current
DCIM	Data Centre Infrastructure Management
DER	Distribution Energy Sources
DG	Diesel Generator
DNS	Directory Name Server
DSL	Digital Subscriber Loop
DSLAM	Digital Subscriber Line Access Multiplexer
DSRC	Dedicated Short-Range Communications
DWDM	Dense Wavelength Division Multiplexing
EC	European Commission
EDGE	Enhanced Data for GSM Evolution
EFC	Electronic Fee Collection
EMS	Emergency Management System
EPR	Electronic Patient Records
ERP	Enterprise Resources Planning
ETSI	European Telecommunications Standards Institute
EV	Electrical Vehicle

EVDO	Evolution Data Only
FTTB	Fibre to the Building, Business, or Basement
FTTC/FTTK	Fibre to the Curb/Closet/Cabinet/Kerb)
FTTD	Fibre to the Desktop
FTTE/FTTZ	Fibre to the Telecom Enclosure
FTTH	Fibre to the Home
FTTLA	Fibre to Last-Amplifier
FTTN	Fibre to the Neighbourhood/Node
FTTP	Fibre to the Premises
FTTx	Fibre to the x
FTTZ	Fibre to the Zone
GEPON	Gigabit Ethernet Passive Optical Network
GHG	Greenhouse Gases
GPON	Gigabit Passive Optical Network
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	General System for Mobile communication
GW	Gateway
HAN	Home Area Network
HAPS	High-Altitude Platform Station
HDR	High Data Rate
HEMS	Home Energy Management System
HSDPA	High Speed Data Packet Access
HSPA	High Speed Packed Access
HVAC	Heating, Ventilation, & Air Conditioning
IaaS	Infrastructure as a Service
IBMS	Intelligent Building Management Systems
ICT	Information and Communication Technologies
IEEE 1901	It is a standard from IEEE
IME	Interface Management Entity
IMT	International Mobile Telecommunications
IO	Infrastructure Operator
IP	Internet Protocol
IPS	Intrusion Prevention System
IPTV	Internet Protocol based Television
IR	Infrared
ITS	Intelligent Transport System

ITU	International Telecommunication Union
LAN	Local Area Network
LDR	Low Data Rate
LEDs	Light Emitter Diodes
LMU	Location Measure Units
LTE	Long Term Evolution
M2M	Machine to Machine
MAC	Medium Attachment Control
MAN	Metropolitan Area Network
MANET	Mobile Ad-hoc Network
MDR	Medium Data Rate
MELT	Metallic Loop Test
MEMS	Micro-Electromagnetic Devices
MPLS	Multiprotocol Label Switching
MPLS-TP	Multi-Protocol Label Switching – Transport Profile
MSAN	Multi-Service Access Code
MV/LV	Medium Voltage Low Voltage
NEM	Network Management Entity
NO	Network Operator
OBU	On Board Unit
OEM	Original Equipment Manufacturing
OLN	Optical Line Terminal
OLT	Optical Line Termination
ONUs	Optical Network Units
OSI	Open Systems Interconnection
PAN	Personal Area Network
PC-LAN	Personal Computer Local Area Network
PHY	Robust radio
PM2.5	Particulate Matter air pollution
PON	Passive Optical Network
POTS	Plain Old Telephone Service
PSTN	Public Switch Telephone Network
PtP	Point to point
PUE	Power Usage Effectiveness
QoL	Quality of Life
QoS	Quality of service
QR	Quick Response

RF	Radio Frequency
RF-ICs	Radio Frequency-Integrated Circuits
RFID	Radio Frequency Identification Devices
RNC	Radio Network Controller
ROADM	Remote Optical Add-Drop Multiplexing
ROI	Return on Investment
RSP	Retail Service Provider
RSSI	Receive Signal Strength Indicator
RSU	Road Side Unit
SaaS	Software as a Service
SAP	Service Access Protocol
SCADA	Supervisory Control and Data Management
SDDC	Software-Defined Data Centre
SDH	Synchronous Data Hierarchy
SGTF	Smart Grid Task Force
SMARTIE	Secure and Smarter Cities Data Management
SME	Small and medium enterprises
SMW	Smart water management
SNS	Social Networking Site
SONET	Synchronous Optical Network Technologies
SSB	Sensor service bus
SSC	Smart Sustainable Cities
STaaS	Storage as a Service
TA	Timing Advance
TMN	Telecommunication Management Network
TP	Transport Profile
UGROW	Urban GROundWate
UMTS	Universal Mobile Telecommunications System
U-TDOA	Uplink-Time Difference of Arrival
UWB	Ultra-Wide Band
VDSL	Very high bit rate Digital Subscriber Line
VoIP	Voice over IP
VPN	Virtual Private Networks
VPP	Virtual Power Plant
WAN	Wide Area Network
W-CDMA	Wideband - Code Division Multiple Access
WDM	Wavelength Division Multiplexing

WG	Working Group
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
XDSL	X Digital Subscriber Line
XML	Extensible Mark-up Language

5 Digital/ICT infrastructure for SSC

ICT infrastructure plays a crucial role in all SSC subsystems (Figure 3) and they deliver the SSC services, which were presented in SSC meta-architecture (Figure2). This section demonstrates technical aspects with regard to the ICT Infrastructure, which is utilized in the SSC ICT architecture.

5.1 Network facilities

The network services describe both data and communications layers depicted in Figures 4 and 5.

5.1.1 Data layer

The data layer concerns, the distributed nodes that require intelligent management and are integrated into the network. This layer has components that are described in the following subsections.

5.1.1.1 Data/content centre

These are centralized repositories, for the storage, management, and dissemination of data and information organized around the objective of creating SCC. It is recommended that data warehouses use a platform that is scalable, reliable and high performance that allows for growth as the number of sensors installed is increased in the territory or the city.

5.1.1.2 Data centre characteristics and the evolution of infrastructure architecture

The infrastructure must be designed and provisioned including the specific volumetric considerations for supporting the business applications and considering the peak load transaction in jobs per second, availability and scalability requirements. When volumetric and projected growth do not manifest as envisaged, this method of sizing infrastructure computation and storage could lead to either under sizing or oversizing the footprint. Often, having such islands of computer infrastructure and storage, leads to underutilization of resources. This has a cascading effect on investment and effort spent on energy consumption, management overheads, software licenses and data centre costs.

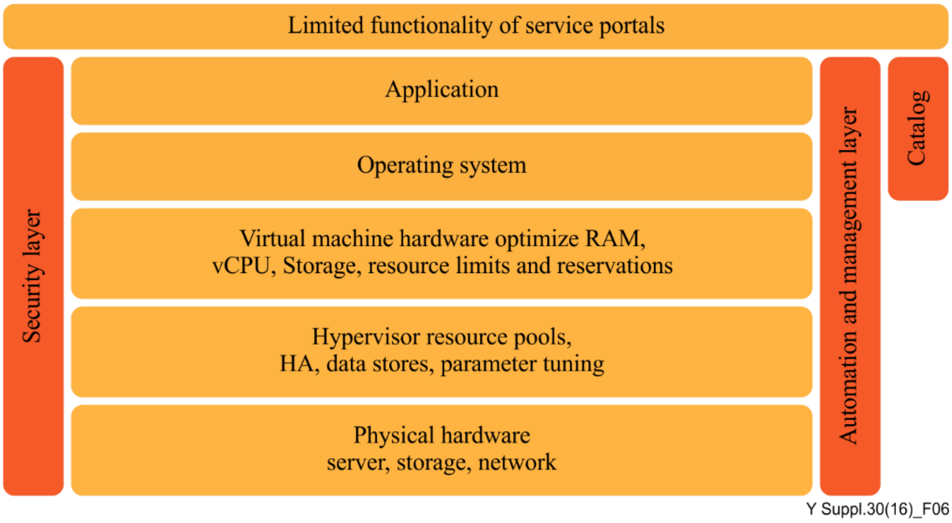


Figure 6 – Data centre infrastructure architecture: A conceptual view

Figure 6 depicts a conceptual view of today's infrastructure architecture in a traditional data centre. The surrounding data centre components such as data centre facilities and legacy infrastructure would exist in this case as individual components in the data centre.

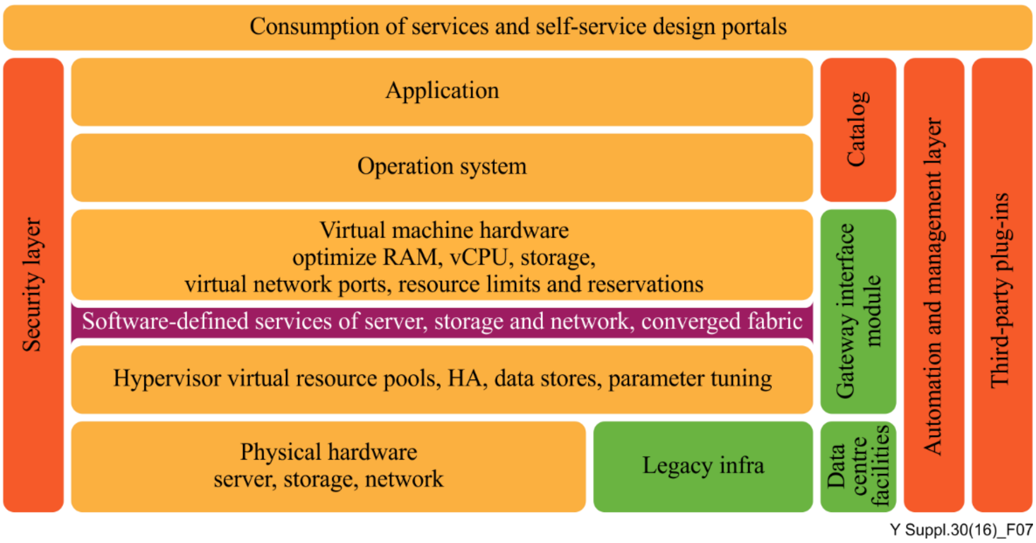


Figure 7 – Legacy infrastructure surrounding software-defined data centre: A conceptual view

Figure 7 illustrates the infrastructure architecture surrounding software-defined data centre (SDDC)[3], where software is deployed to meet applications for dynamic workloads. SDDC blocks the need to be holistic for integration across physical, legacy and data centre facilities. This requires third-party vendors with plug-ins to provide the interfaces.

Based on Figure 7, the following aspects can be emphasized on:

– Physical hardware and legacy infrastructure:

[3] The term SDDC, or software-defined data centre, was coined in 2012 by VMware's former chief technology officer (CTO), Dr. Steve Herrod. At first, it may seem unusual to define a data centre in terms of software, rather than hardware infrastructure, that programmatically turns on and off devices, or shrinks and expands computing resource consumption as business requirements dictate.

- This constitutes the bare metal hardware and data centres that can be virtualized across physical or legacy systems. The ability of these to be involved and controlled via software, programmatically, will be based on the evolution of technology or business needs, depending on the abstraction of server, storage, network components and legacy integration requirements. Original equipment manufacturing (OEMs) and converged infrastructure vendors are key players since they design, fabricate and integrate to make this happen.

– Automation and management layer:

  - This consists of an integrated suite of management and monitoring solutions for the data centre estate, comprising operations and performance engineering capabilities.

– Gateway interface module:

  - For SDDCs to be mainstream, they must be integrated with existing data centre components. This gateway module will comprise of multi-vendor OEM plug-ins connecting with the existing data centre footprint. OEM partners and service system integrators need to drive this.

Figure 8 shows a logical depiction of SDDC to explain the challenges foreseen in mainstream adoption.

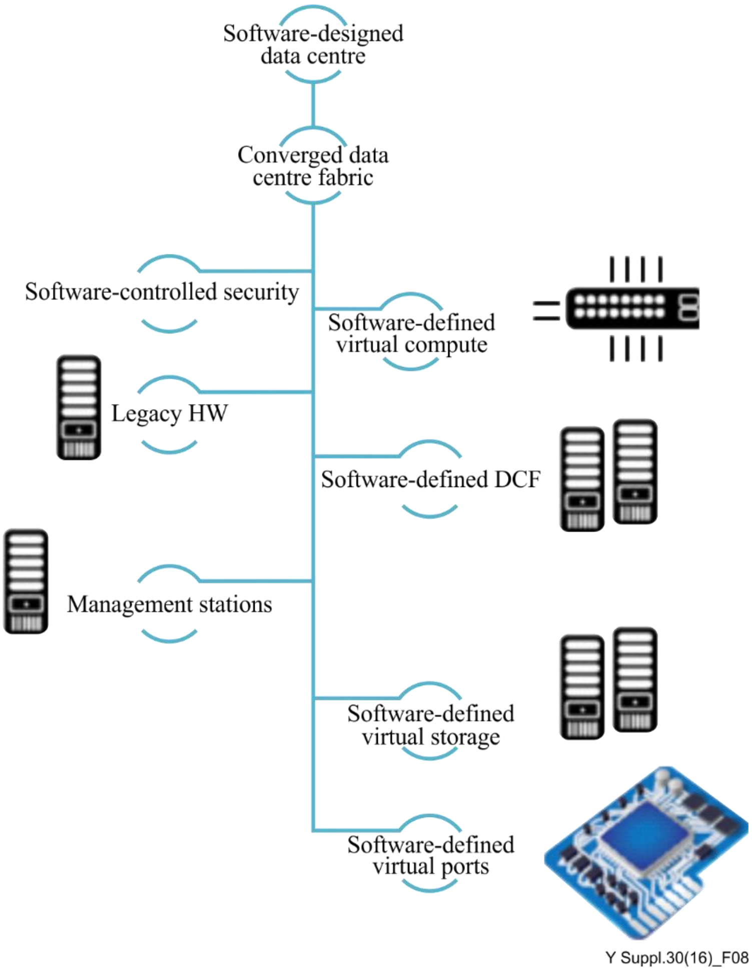


Figure 8 – A logical view of future SDDC

For a data centre, the facilities play an important role in ensuring that the SLAs are aligned and met. Given the mix of data centre categories in use (such as tier 1, 2, 3 or 4, with tier 4 data centres built for maximum resiliency and uptime), data centre providers must develop integrated and adaptable power and cooling solutions in line with the infrastructure capacity planned and provisioned.

5.1.1.3 Design considerations of data centre

A data centre is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and various security devices.

A data centre can occupy one room of a building, one or more floors, or an entire building itself. Most of the equipment is often in the form of servers mounted in 19 inch rack cabinets (see Figure 9), which are usually placed in single rows forming corridors (so-called aisles) between them. This allows people access to the front and rear of each cabinet. Servers differ greatly in size from 1U servers to large freestanding storage silos which occupy many square feet of floor space. Some equipment such as mainframe computers and storage devices are often as big as the racks themselves, and are placed alongside them. Very large data centres may use shipping containers packed with 1000 or more servers each. When repairs or upgrades are needed, whole containers are replaced (rather than repairing individual servers).

Figure 9 – Cabinet aisle in a data centre

5.1.1.4 Technology infrastructure design

Technology infrastructure design addresses the telecommunications cabling systems that run throughout data centres (see Figure 10). There are cabling systems for all data centre environments, including horizontal cabling, voice, modem, and facsimile telecommunications services, premises switching equipment, computer and telecommunications management connections, keyboard/video/mouse connections and data communications. Wide area, local area, and storage area networks should link with other building signalling systems (e.g., fire, security, power, HVAC, EMS).

Figure 10 – Under floor cable runs

5.1.1.5 Electrical power

A bank of batteries (see Figure 11) in a large data centre, used to provide power until diesel generators can start backup power, consists of one or more uninterruptible power supplies including battery banks, and/or diesel/gas turbine generators.

To prevent single points of failure, all elements of the electrical systems, including backup systems, are typically fully duplicated, and critical servers are connected to both the "A-side" and "B-side" power feeds. This arrangement is often made to achieve N+1 redundancy in the systems. Static transfer switches are sometimes used to ensure instantaneous switchover from one supply to the other in the event of a power failure.

Figure 11 – Bank of batteries

5.1.1.6 Network infrastructure

Communications in data centres today are most often based on networks running the IP protocol suite. Data centres contain a set of routers and switches that transport traffic between the servers, like the one shown in Figure 12, and to the outside world. Redundancy of the Internet connection is often provided by using two or more upstream service providers as multihoming. Multihoming refers to a computer or device connected to more than one computer network. It can be used, for example, to increase the reliability of an Internet protocol network, such as a user served by more than one Internet service provider. Also SAN solutions are recommended for redundant storage management.

Some of the servers at the data centre are used for running the basic internet and intranet services needed by internal users in the organization, e.g., e-mail servers, proxy servers, and DNS servers.

Network security elements are also usually deployed: firewalls, VPN gateways, intrusion detection systems, intrusion prevention system (IPS) is also widely used. Monitoring systems for the network and some of the applications are also common. Additional off site monitoring systems are also typical, in case of a failure of communications inside the data centre.

Figure 12 – Rack mounted servers

5.1.1.7 Environmental control

The physical environment of a data centre must be rigorously controlled. Air conditioning is used to control the temperature and humidity in the data centre. Some guidelines recommend a temperature range of 18-27 °C (64-81 °F), a few point range of 5-15 °C (41-59 °F), and a maximum relative humidity of 60% for data centre environments. The temperature in a data centre will naturally rise because of the electrical power used that heats the air. Unless the heat is removed, the ambient temperature will rise, resulting in malfunctioning of the electronic equipment. By controlling the air temperature, the server components at the board level are kept within the manufacturer's specified temperature/humidity range. Air conditioning systems help control humidity by cooling the return space air below the dew point. Too much humidity and water may begin to condense on internal components. In case of a dry atmosphere, ancillary humidification systems may add water vapour if the humidity is too low, which can result in static electricity discharge problems which may damage components. Subterranean data centres may keep computer equipment cool while expending less energy than conventional designs.

Figure 13 – Air conditioning equipment

5.1.1.8 Power saving system control technology to maintain temperature and humidity of container-type data centres[4]

Power saving system control technology shall be included to maintain temperature and humidity of container-type data centres by closely coordinating the operation of servers and air-conditioning systems as elemental technology for ICT infrastructure of smart sustainable cities.

Data centres are used in smart sustainable cities in order to collect necessary data, process those data and provide and manage application services using them.

With container-type data centres rather than data centres in buildings, one can expand the scale of data centres according to increases in demand. It facilitates the achievement of a balance between investment and return for data centre providers as well as a reduction of environmental burden.

To reduce the environmental burden of the container-type data centres themselves, the technology is required to reduce the amount of electricity consumed to maintain proper temperature and humidity levels.

There is technology that maintains temperature and humidity of container-type data centre using external ambient air and air-conditioning equipment (see Figure 13) attached to the inside of the container, instead of an internal fan equipped to each server. The use of external ambient air reduces the amount of electricity used by the air conditioning.

By eliminating the use of internal fans of servers, the amount of electricity used by air conditioning is also reduced. Generally speaking, when external ambient air is used to cool servers, the higher the ambient temperature is, the larger the amount of electricity consumption of internal fans becomes. However, this technology allows the use of internal fans by maintaining temperature and humidity with air-conditioning equipment attached to the inside of the container.

The main composing elements of the air-conditioning equipment attached to the inside of the container are the fans. They are controlled to achieve optimum temperature of central processing units (CPUs) using information of location, temperature and electricity consumption of each CPU.

If the temperature of each CPU is too high, the performance of the CPU gets lower (Figure 14). The technology controls the container air-conditioning fan to ensure that the system never reaches an operating temperature where CPU performance is compromised.

In addition, there is optimum temperature of the CPU to minimize the total power consumption (Figure 15). When a CPU's operating temperature becomes too high, the amount of electricity

[4] Corresponds to a contribution of FUJITSU (Japan).

consumed by a server increases as a result of the impact of the CPU's leakage current. Conversely, by trying to lower the temperature of the CPU, greater power is consumed by the container air-conditioning fan. The technology controls the container air-conditioning fan to achieve an optimal CPU temperature that will enable the amount of power consumed by the entire container data centre to be minimized.

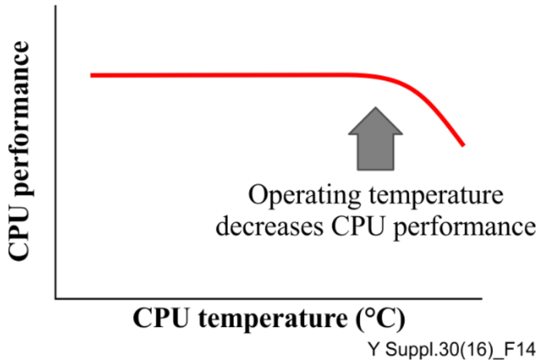


Figure 14 – Control technology to prevent overheating

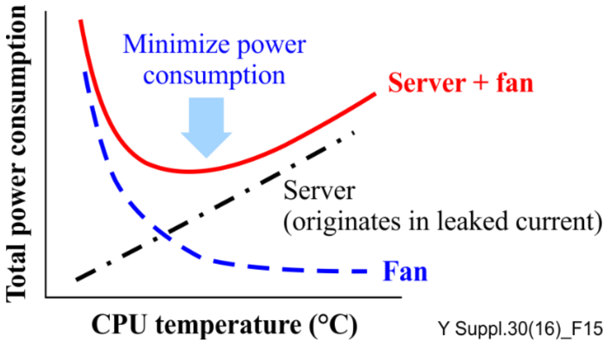


Figure 15 – Control technology to minimize decreased CPU performance overall energy consumption

Source: Fujitsu (2012), Fujitsu Develops Power Saving System Control Technology for Container Data Centres[5].

When the external temperature is between 10 °C and 35 °C, the container's air conditioning fan takes air through the external intake vent and moves it inside the racks. The warm air from inside the racks is then released from the exhaust vent.

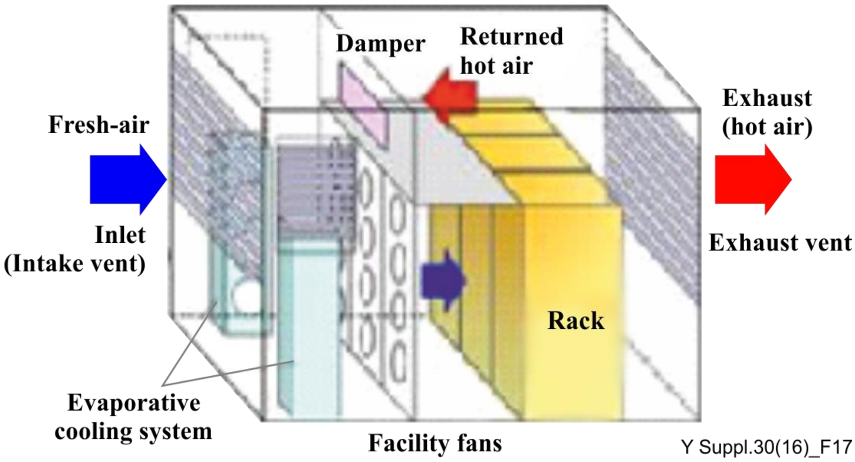
When the external temperature exceeds 35 °C, an evaporative cooling system cools the air to 35 °C or lower before moving it with the fan. This ensures that the temperature of the moving air into the racks does not exceed the favourite range of temperature for servers.

Conversely, when the outside temperature is below 10 °C, warm air being released from the racks is passed through a damper and returned to the air intake vent side where it is warmed to 10 °C or higher before being moved into the racks by the fan. This prevents dew condensation.

5 http://www.fujitsu.com/global/news/pr/archives/month/2012/20120404-02.html.

Y Suppl.30(16)_F16

Figure 16 – Prototype container data centre



Y Suppl.30(16)_F17

Figure 17 – Container data centre's contents

Figure 16 is a photo of a prototype container data centre and Figure 17 is a schematic of the container's contents.

The effect of reduction of electricity consumption with the prototype container data centre was as depicted in Figure 18. It shows that energy consumption is reduced by approximately 40% compared with conventional container data centres using internal fans equipped to servers.

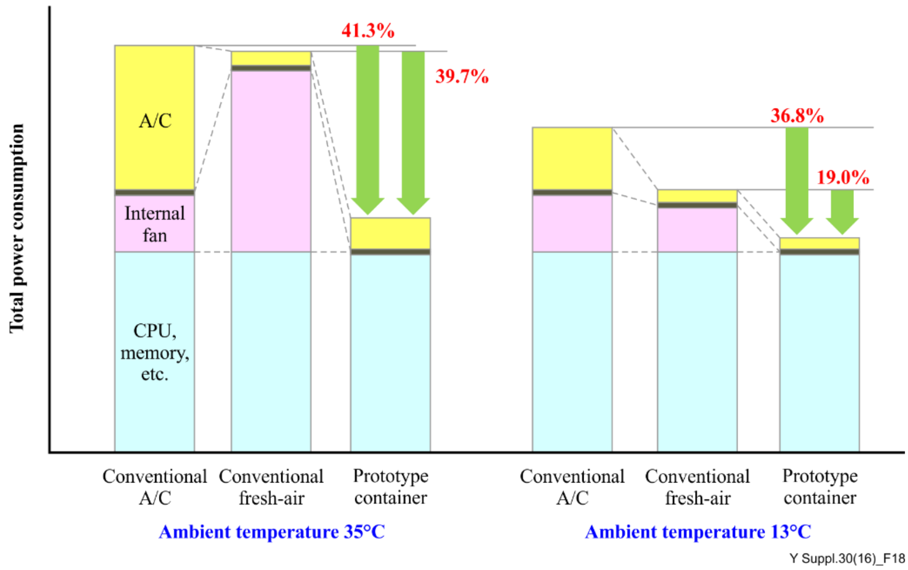


Figure 18 – Power reduction effectiveness

5.1.1.9 Requirements of the technology

i) Reduction of overall power consumption

Power usage effectiveness (PUE)is often used as an indicator to measure the energy effectiveness of air-conditioning of data centres. PUE is the ratio between the power consumption of overall data centre and that of ICT equipment in the data centre. If the figure of PUE gets lower, it means the effectiveness improves. As electricity consumption for internal fans is counted as that of ICT equipment, the larger the internal fans are, the smaller the PUE is, and the better the energy effectiveness. In contrast to this, it is required to reduce the overall power consumption of data centres, not only to lower PUE values.

ii) Usage regardless of climate conditions

Temperature or humidity of external ambient air varies according to locations and seasons. It is required to be able to reduce power consumption in a wide range of temperatures and humidity levels. Figure 19 shows an example of climate data for 2010 observed locations.

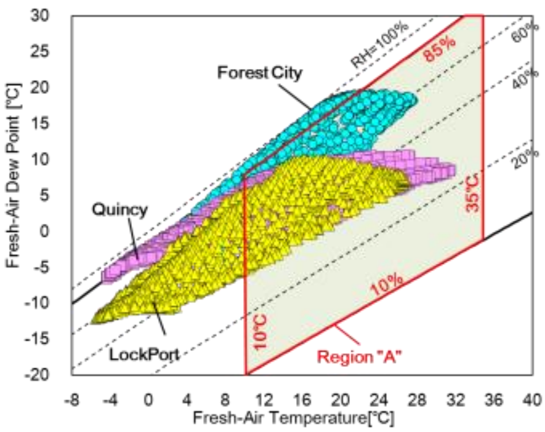


Figure 19 – Hourly climate data for 2010 observed at locations of direct fresh-air-cooled data Centres

Source: Hiroshi Endo et.al. (2013), Effect of climatic conditions on energy consumption in direct fresh-air container data centers; IEEE.

5.1.1.10 Data centre infrastructure management

Data centre infrastructure management (DCIM) is the integration of information and communication technology (ICT) and facility management disciplines to centralize monitoring, management and intelligent capacity planning of a data centre's critical systems. Achieved through the implementation of specialized software, hardware and sensors; DCIM enables common, real-time monitoring and management platform for all interdependent systems across IT and facility infrastructures.

Depending on the type of implementation, DCIM products can help data centre managers identify and eliminate sources of risk to increase availability of critical IT systems. DCIM products can also be used to identify interdependencies between facility and IT infrastructures to alert the facility manager of gaps in system redundancy, and provide dynamic, holistic benchmarks on power consumption and efficiency to measure the effectiveness of "green IT" initiatives.

In order to measure and understand important data centre efficiency metrics, a lot of discussion in this area has been focused on energy issues, but other metrics can give a more detailed picture of the data centre operations. Server, storage, and staff utilization metrics can contribute to a more complete view of an enterprise data centre. In many cases, disc capacity goes unused and in many instances the organizations run their servers at 20% utilization or less. More effective automation tools can also improve the number of servers or virtual machines that a single admin can handle.

Recommendation [ITU-T L.1300] "Best practices for green data centres", recommended a possible methodology for cooling data centres with high density ICT devices.

The Recommendation [describes best practices aimed at reducing the negative impact of data centres on the climate. It is commonly recognized that data centres will have an ever-increasing impact on the environment in the future. The application of the best practices defined in [ITU-T l.1300] can help owners and managers to build future data centres, or improve existing ones, to operate in an environmentally responsible manner. Such considerations will strongly contribute to a reduction in the impact of the information and communication technology (ICT) sector on climate change.

5.1.2 Communication layer

This is one of the main aspects of the ICT infrastructure. Particular attention should be paid in both the national and urban infrastructure, since the backhauls will feed the backbones that are bound to the international links. Access networks are key for the development of SSC. However they are issues related to the deployment of antennas which pose problems in setting up access networks. Figure 20 shows an example of the infrastructure of a communication layer.

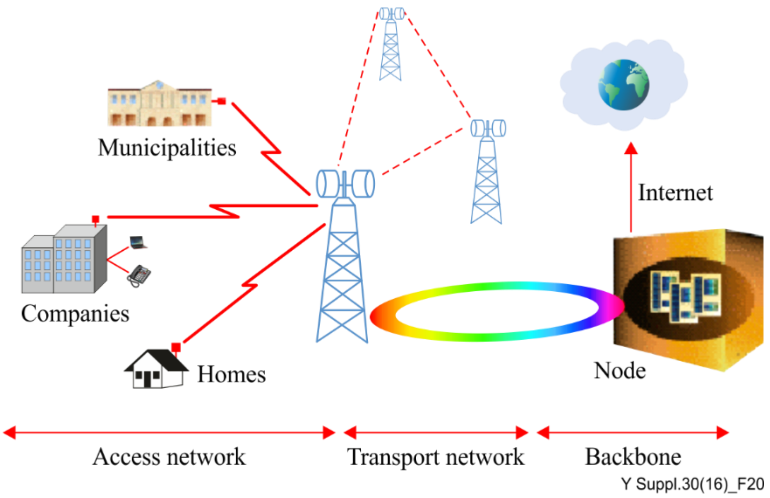


Figure 20 – Communication layer

5.1.2.1 Transport networks

The convergence of infrastructure already introduced earlier should be carefully considered for this type of transport of data networks in urban environments.

To transport the large amount of data handled by smart sustainable cities it will be necessary for local governments to implement national policies for the deployment broadband networks.

Optical transport

Fibre is the optimum physical medium to transmit large amounts of data over long distances. The bandwidth-over-distance capabilities of fibre by far exceed those of any other medium such as copper or wireless technologies. Fibre-optic transport is therefore the unchallenged foundation for all high-speed networks. See Figure 21 for an image of fibre optic networks worldwide.

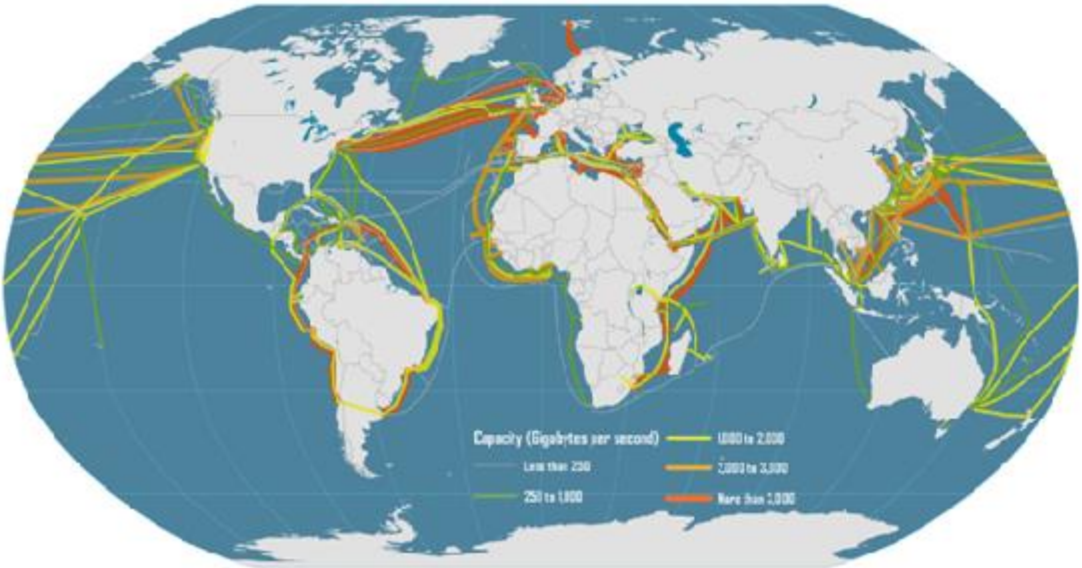


Figure 21 – Fibre optic networks worldwide

Dense wavelength division multiplexing (DWDM)

This is an optical multiplexing technology used to increase bandwidth over existing fibre networks. DWDM works by combining and transmitting multiple signals simultaneously at different wavelengths on the same fibre. The technology creates multiple virtual fibres, thus multiplying the capacity of the physical medium.

Wavelength division multiplexing (WDM) has revolutionized the cost per bit of transport. Owing to DWDM, fibre networks are capable of carrying multiple terabits of data per second over thousands of kilometres – at cost points unimaginable less than a decade ago. State-of-the-art DWDM systems support up to 192 wavelengths on a single pair of fibre, with each wavelength transporting up to 100Gbit/s capacity – 400Gbit/s and one terabit/s on the horizon.

DWDM provides ultimate scalability and reach for fibre networks. Without the capacity and reach of DWDM systems, most Web 2.0 and cloud-computing solutions today would not be feasible. Establishing transport connections as short as tens of kilometres to enabling nationwide and transoceanic transport networks, DWDM is the workhorse of all the bit-pipes keeping the data highway alive and expanding.

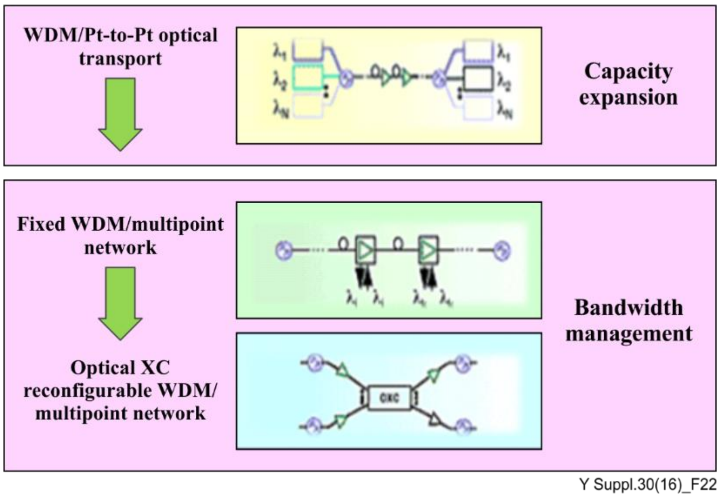


Figure 22 – Optical transport to optical networking: Evolution of the photonics layer

Use of DWDM allows providers to offer services such as e-mail, video, and multimedia carried Internet protocol (IP) data over asynchronous transfer mode (ATM) and voice carried over SONET/SDH. Despite the fact that these formats, that is, IP, ATM, and SONET/SDH-provide unique bandwidth management capabilities, all these can be transported over the optical layer using DWDM. This unifying capability allows the service provider the flexibility to respond to customer demands over one network.

Figure 22 depicts the evolution of the photonics layer.

Ethernet data link

In a world that is moving to a packet-based future, Ethernet is the dominant data-link protocol for today's networks (see Figure 23), supporting a multitude of communication applications. Also, Ethernet is one of the key protocols used to interconnect routers and to carry applications in high-speed optical networks to backhaul access traffic.

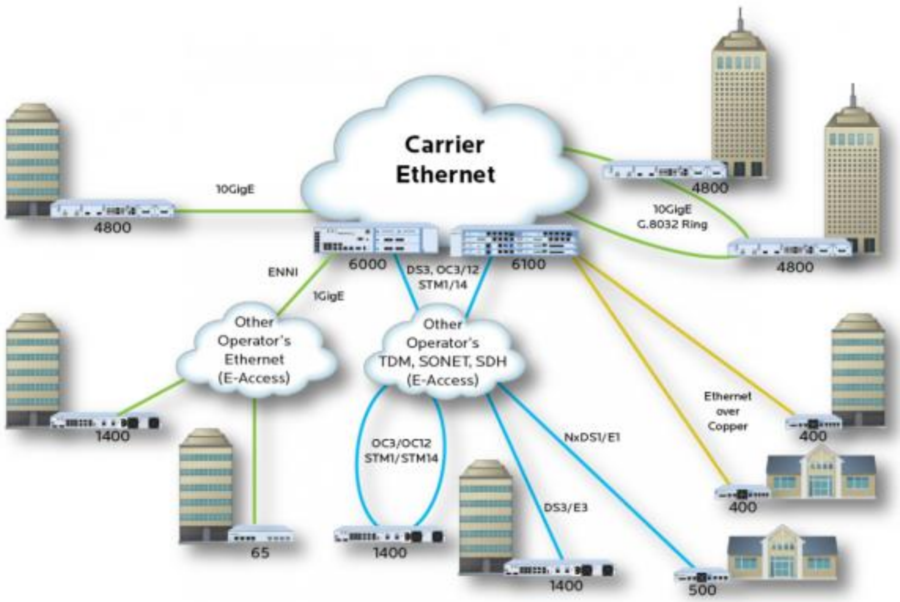


Figure 23 – Ethernet is the dominant data-link protocol (Source: Overture[6])

6 http://www.overturenetworks.com/solutions/business-services/deliver-consistent-ethernet-service-over-any-access.

Optical + Ethernet (foundation for high-speed networks)

The combination of fibre-optic transmission technology and Ethernet-optimized data processing (Optical+Ethernet) is the perfect solution to deliver high-speed connectivity for data, storage, voice and video applications (see Figure 24).

Optical+Ethernet innovation enables us to advance the transformation of packet-oriented optical networking and increase the efficiency of existing network infrastructures. Wavelength division multiplexing technology provides more capacity, higher speeds, longer reach and a greater utilization of optical networks. As a result, networks become more manageable, operate more efficiently and transport considerably higher bandwidth for high-volume data transmission.

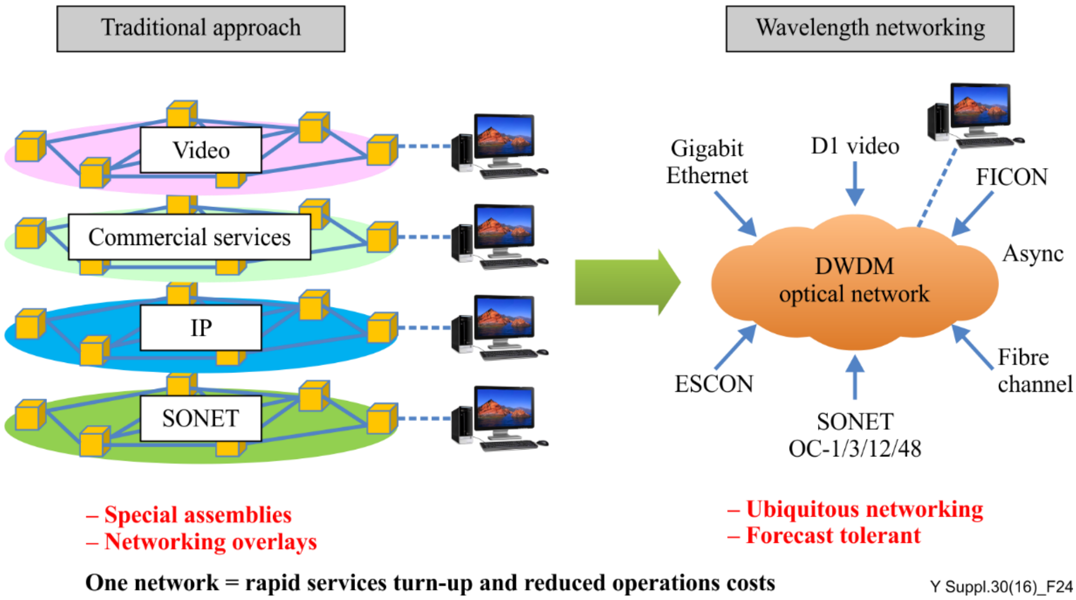


Figure 24 – Convergence at the optical layer

Multiprotocol label switching (MPLS)

In MPLS, the traffic engineering capabilities are integrated into OSI Layer 3, which optimizes the routing of IP traffic through the guidelines established by the topology and the trunk capacities.

MPLS IP VPN gives a network separate and independent communication for all its offices in the telecommunications network. Its benefits are:

– Access to all information wirelessly.
– Stable, private and secure connection.
– Availability for teleconferencing, video-calls and unlimited exchange of information in real time.
– Total availability of corporate headquarters from a single point.
– Implementation of loyalty systems and databases such as CRM, SAP, ORACLE, ERP, etc.
– Transmission of data, images and voice.

MPLS could be divided into two categories, MPLS for user access network, MPLS-TP (Transport Profile) for transport network.

5.1.2.2 Access networks

These are shaped by fixed and mobile access, preferably by broadband communication networks. Mobile networks are especially important for a smart sustainable city to permit permanent and wireless connection of objects, people and environments. Figure 25 provides examples of elements in the sensor and network layers.

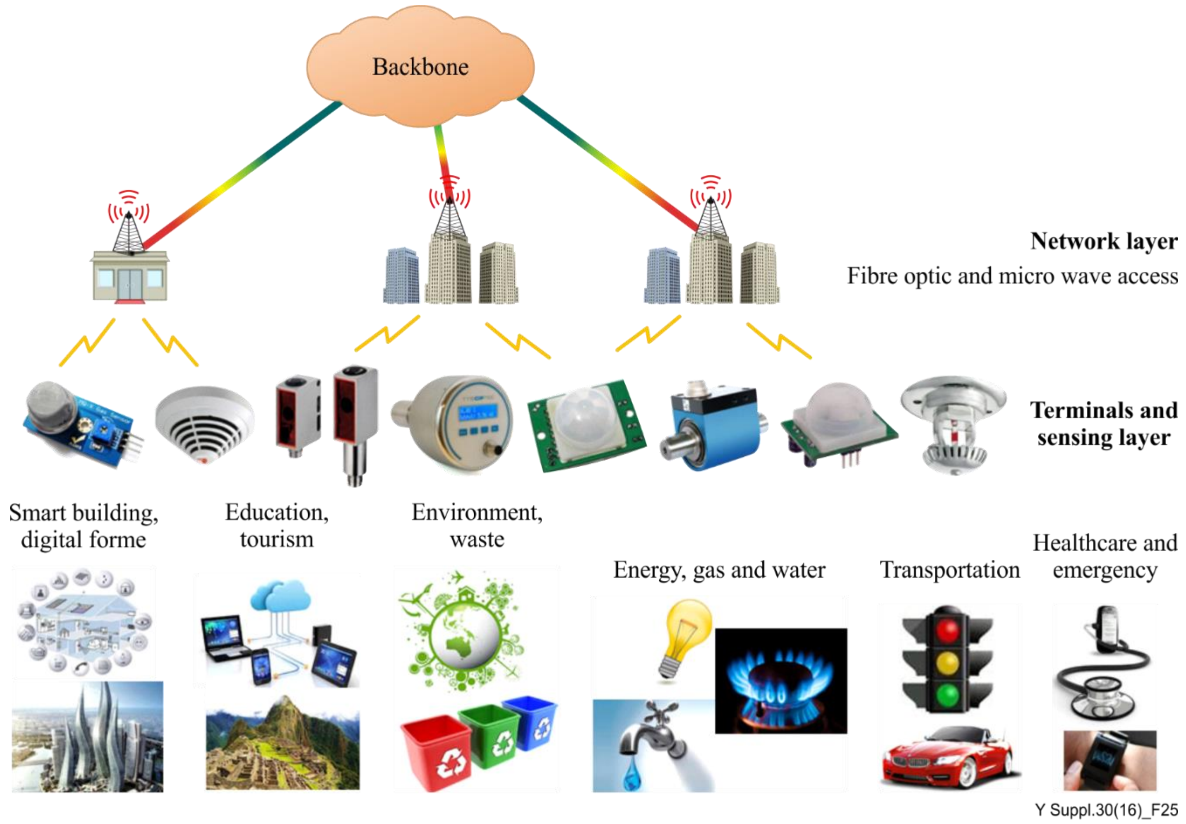


Figure 25 – Sensing and network layer

Source: Ministry of Transportation and Communications of Peru.

MPLS and Ethernet as access networks

These types of networks are used mainly as part of the transport facilities inside telecommunication networks; but can also be used as access networks for the connectivity of branch offices, for example, specifically in business environments.

FTTx access networks

Fibre to the X (FTTx) is a generic term for any broadband network architecture using optical fibre to provide all or part of the local loop used for last mile telecommunications. The term is a generalization for several configurations of fibre deployment, ranging from fibre to the neighbourhood (FTTN) to fibre to the desktop (FTTD). See Figure 26.

One of the most used technologies for FTTx is the passive optical network (PON). It is a point-to-multipoint fibre to the premises network architecture in which unpowered optical splitters utilizing Brewster's angle principles are used to enable a single optical fibre to serve multiple premises, typically 32 to 128. A PON consists of an optical line terminal (OLT) at the service provider's central office (CO) and a number of optical network units (ONUs) near end users. A PON configuration reduces the amount of fibre and CO equipment required compared with point to point architectures.

The telecommunications industry differentiates between several distinct FTTx configurations. The terms most widespreadly used today are:

1) Fibre-to-the-node, -neighbourhood, or -last-amplifier (FTTN/FTTLA): Fibre is terminated in a street cabinet, possibly miles away from the customer premises, with the final

connections being copper. FTTN is often an interim step toward full FTTH and is typically used to deliver advanced triple-play telecommunications services.

2) Fibre-to-the-curb/kerb, -closet, or -cabinet (FTTC/FTTK): This is very similar to FTTN, but the street cabinet or pole is closer to the user's premises, typically within 1 000 feet (300 m), within range for high-bandwidth copper technologies such as wired Ethernet or IEEE 1901 power line networking and wireless Wi-Fi technology. FTTC is occasionally ambiguously called fibre-to-the-pole (FTTP), leading to confusion with the distinct fibre-to-the-premises system.

3) Fibre-to-the-premises (FTTP): This term is used either as a blanket term for both FTTH and FTTB, or where the fibre network includes both homes and small businesses.

   a) Fibre-to-the-building, -business, or -basement (FTTB): Fibre reaches the boundary of the building, such as the basement in a multi-dwelling unit, with the final connection to the individual living space being made via alternative means, similar to the curb or pole technologies.

   b) Fibre-to-the-home (FTTH): Fibre reaches the boundary of the living space, such as a box on the outside wall of a home. Passive optical networks and point-to-point Ethernet are architectures that deliver triple-play services over FTTH networks directly from an operator's central office.

4) Fibre-to-the-desktop (FTTD): Fibre connection is installed from the main computer room to a terminal or fibre media converter near the user's desk.

5) Fibre-to-the-telecom-enclosure or fibre-to-the-zone (FTTE/FTTZ) is a form of structured cabling typically used in enterprise local area networks, where fibre is used to link the main computer equipment room to an enclosure close to the desk or workstation. FTTE and FTTZ are not considered part of the FTTx group of technologies, despite the similarity in name.

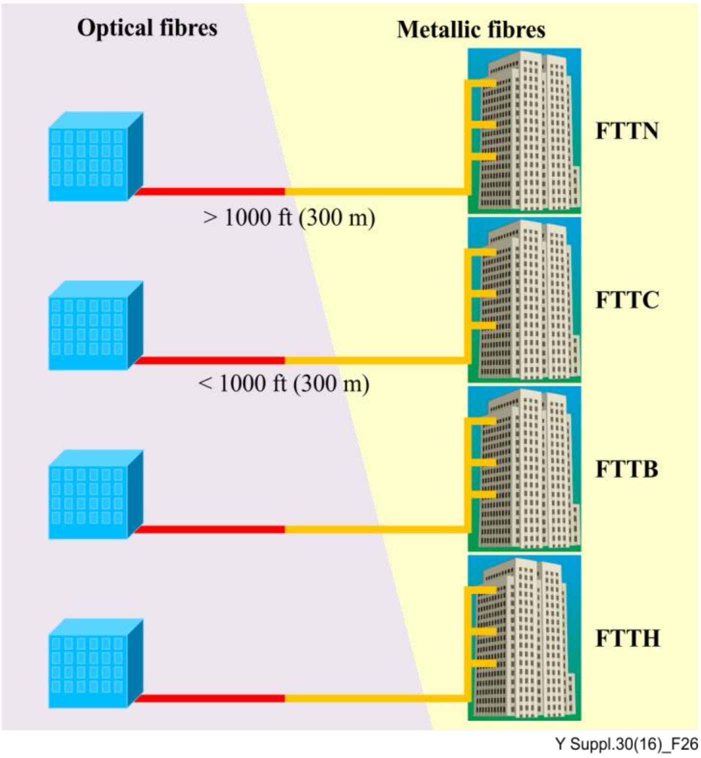


Figure 26 – FTTx access networks

Increased competition from multiple system operators (MSOs), telcos, and Internet protocol television (IPTV) service providers worldwide are driving the deployment of quadruple-play services over next-generation access networks. As a result, service providers are faced with many new business and service delivery challenges. New optical access networks deliver higher bandwidths for increased service offerings.

Whether the access network is purely optical fibre-to-the home (FTTH) or based on a mixed fibre/copper technology (fibre-to-the curb [FTTC], fibre-to-the business [FTTB]), the requirements for operation and maintenance are changing dramatically compared to pure digital subscriber loop (DSL)-based access. At the same time, expectations have been set to reduce the maintenance effort especially on the fibre network, because it is regarded as more reliable than copper.

X digital subscriber line (XDSL)

This is a family of technologies that allows access to provide broadband access network over conventional telephony (PSTN). Therefore, in the copper, the data are transmitted in a frequency range higher than that used for voice, while avoiding the mutual interference. Implementation of DSL modem requires placing a client (Modem) at home and an equipment called digital subscriber line access multiplexer (DSLAM) in the central operator. One of the main considerations in the deployment of this technology is the length of the local loop, as given band width is inversely proportional to this length.

The example in Figure 27 shows how the different access networks connect homes:

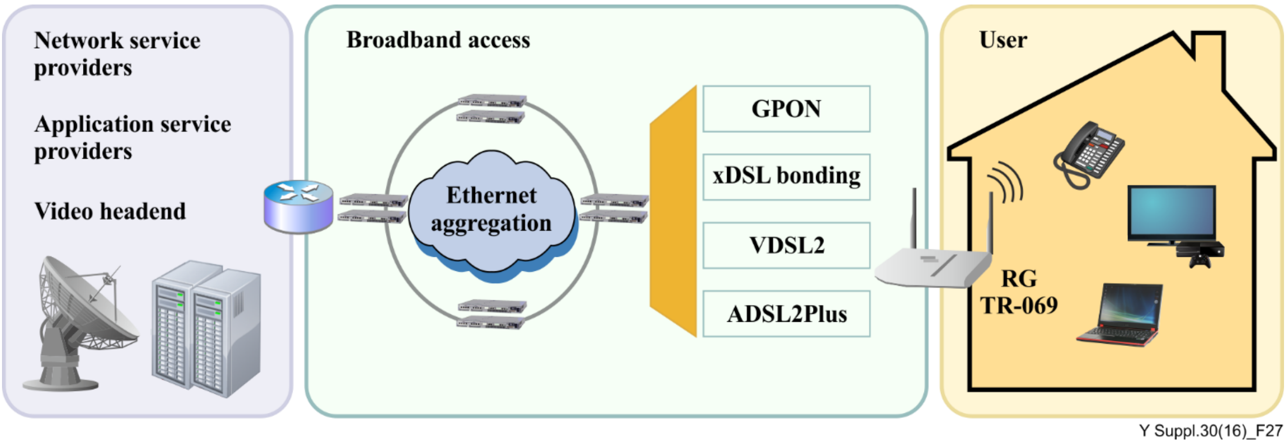


Figure 27 – Broadband access

Mobile broadband wireless access technologies

Wireless broadband technologies provide ubiquitous broadband access to mobile users and to all kind of terminal equipment, enabling consumers with a broad range of mobility and a variety of wireless multimedia services and applications. Broadband wireless access technologies provide broadband data access through wireless media to consumer and business markets.

There have been continued efforts to deliver ubiquitous broadband wireless access by developing and deploying advanced radio access technologies such as 3GPP UMTS and LTE, as well as mobile WiMAX systems; commercially known as 3G and 4G technologies. In the future, it is expected that 5G will deliver higher speeds.

The broadband wireless access is also an attractive option to network operators in geographically remote areas with limited or no wired network. The advantages in terms of savings in speed of deployment and installation costs are further motivation for broadband wireless access technologies.

There are various types of broadband wireless access technologies that are classified based on the coverage area and user mobility as follows:

1) Personal area network (PAN) is a wireless data network used for communication among data devices/peripherals around a user. The wireless PAN coverage area is typically limited to a few meters with no mobility. Examples of PAN technologies include Bluetooth or IEEE 802.15.1 and ultra-wideband (UWB) technology.

2) Local area network (LAN) is a wireless or wireline data network used for communication among data/voice devices covering small areas such as home or office environments with limited or no mobility. Examples include Ethernet (fixed wired LAN) and Wi-Fi or IEEE 802.11 (wireless LAN for fixed and nomadic users).

3) Metropolitan area network (MAN) is a data network that connects a number of LANs or a group of stationary/mobile users distributed in a relatively large geographical area. Wireless infrastructure or optical fibre connections are typically used to link the dispersed LANs.

   Examples include the IEEE 802.16-2004 (fixed WiMAX) and Ethernet-based MAN.

4) Wide area network (WAN) is a data network that connects geographically dispersed users via a set of inter-connected switching nodes, hosts, LANs, etc., and covers a wide geographical area.

   Examples of WAN include the Internet and national cellular networks.

The user demand for broadband wireless services and applications are continuously growing. Also the connection of the elements for SSC will increase this demand. Offering customized and ubiquitous services based on diverse individual and SSC needs through versatile communication systems will require certain considerations in the technology design and deployment.

The 4th generation of mobile broadband wireless access technologies

International mobile telecommunications-advanced (IMT-Advanced) or alternatively 4th Generation (4G) cellular systems are mobile systems that extend and improve upon the capabilities of the IMT-2000 family of standards. Such systems are expected to provide users with access to a variety of advanced IP-based services and applications, supported by mobile and fixed broadband networks, which are predominantly packet-based. The IMT-Advanced systems can support a wide range of data rates, with different quality of service requirements, proportional to user mobility conditions in multi-user environments.

Millimetre wave communication[7]

High capacity wireless communication technology using impulse radio operating in the millimetre wave E-band

Expanding use of applications of sensor networks and/or Internet of things (IoT) for SSC requires huge amount of data to be transferred on the telecommunication networks of the cities.

Moreover, due to the popularity of smartphones and tablets in recent years, along with the growing volumes of content handled by such devices, there has been a sharp increase in traffic passing through mobile networks and other communications channels.

Mainly, optical cables are used for backbone broadband network. However, wireless broadband technology complement to the optical cables is also required to meet the telecommunication demand for more flexibly.

In some cases, it is difficult to lay cables. Such cases include providing services around waterway crossings and between buildings. In other cases, it is not efficient to lay cables. Such cases include providing services for use at temporary events and for rapid network recovery in emergency occasions like big natural disasters.

---

7 Corresponds to a contribution of FUJITSU (Japan).

Figures 27a and 28 show use cases of the technology:

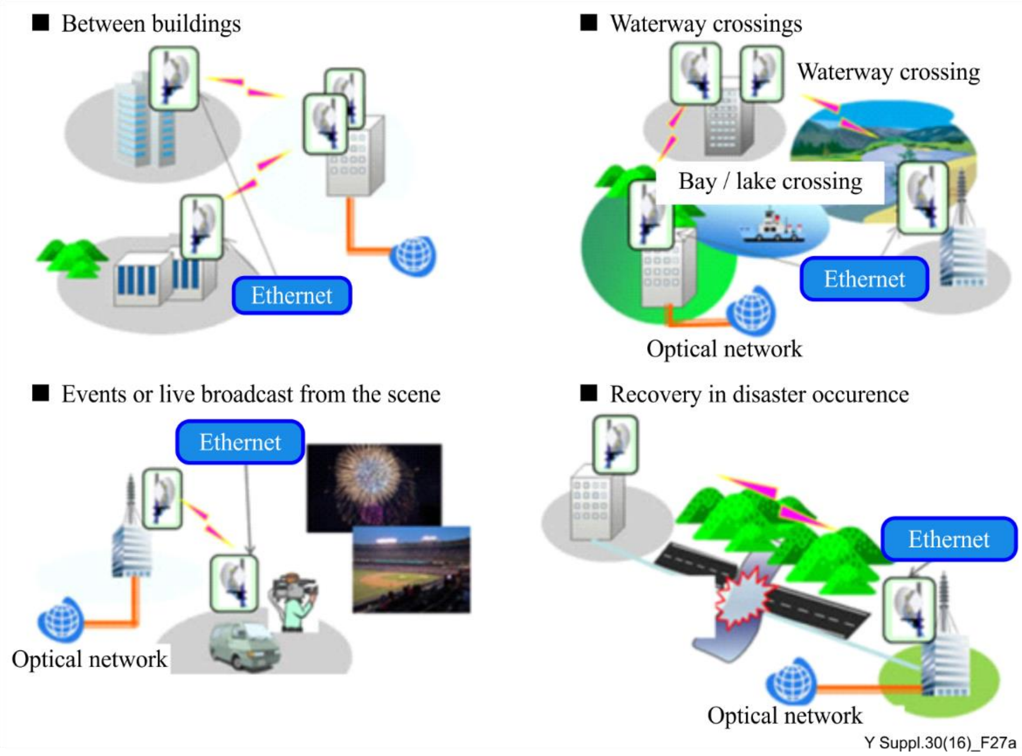


Figure 27a – Example use cases of millimetre wave communications

Setting transmission equipment at each of two sites (Figure 28), the distance between them is several kilometres; data is to be transmitted between them wirelessly. Operating in the millimetre wave allows the system access to a wider radio frequency spectrum and prevents the radio wave from interfering with other radio waves as a result of the rectilinear propagation characteristic. Transmission rate of few Gbps comparable to optic cables is achieved.

Figure 28 – Example installation

From an environmental point of view, to consume less electricity:

– It is required to consume less electricity per unit for the amount of transmission of data in order to reduce the environmental burden.

– It is also required to use less electricity when some data is transmitted along the same distance.

– It is preferable to be able to obtain electricity autonomously using natural energy such as wind power and energy from sunlight.

To be small and lightweight:

– It is required to be easily installed and used for temporary radio relays or live broadcast from the events sites as well as the means of rapid network recovery in an emergency where mobility characteristic is required.

– It is preferable to be able to lessen the number of component parts or the amount of volume to contain in order to reduce the environmental burden. For example, impulse radio wireless technology does not allow the system to use oscillators which are likely to be large-size.

Connectivity to Internet

Internet connections through the many access networks listed before, are a solution for SSC data transmission. As security is an extremely important element, virtual private networks (VPN) are necessary to send data over the Internet. Encryption in these VPN is vital for the safe transport of data. A VPN is a private network in logical terms, mounted potentially on a shared medium.

The Internet solution is a very economical option compared to using private channels from MPLS or Ethernet networks, but depends on the speed and availability of broadband Internet access. The virtual private network perfectly fits the requirements: security, data encryption, transparency and lower monthly costs.

Tasks that must satisfy a VPN are:

– Remote access to databases, servers, etc.

– Authentication of both ends of the connection (main office and remote office).

– Ability to send IP packets through a tunnel in the public network (Internet), so that the two segments of the network interconnecting remote LAN does not appear to be geographically separated.

– Encryption of data traveling over a public network (Internet) so that nobody can decipher its contents.

– National coverage.

– Massive transfer of information.

5.2 ICT facilities: over the top, services, applications and contents

This section addresses the application and security layers illustrated in Figures 4 and 5, and contains specifications for corresponding ICT facilities.

5.2.1 ICT integrated services capacity

The capacity of integration of services has a direct relationship with interoperability, which is decisive. Every entity involved in the development SSC applications shall adopt open standards that enable interoperability between information systems with the systems of other actors, public and private, and for data captured through smart devices of citizens serve as a basis for open and reuse data and generate new services and platforms.

5.2.2 Data management

5.2.2.1 Data security

As stated in the European Commission Project SMARTIE (Secure and Smarter Cities Data Management)[8]: "A secure, trusted, but easy to use (…) system for a smart city will benefit the various

[8] Security and Privacy Challenge in Data Aggregation for the IoT in Smart Cities (from http://www.smartie-project.eu/publication_bohli2013a.html).

stakeholders of a smart city. This also holds true for SSC. The city administration will find it easier to get information from their citizens while protecting their privacy. Furthermore, the services offered will be more reliable if quality and trust of the underlying information is ensured".

There are numerous risks to be addressed involving all levels of data of the system itself, and considering citizens' concerns about data intrusion, then security becomes a key concept in the adoption and sustainability of a smart city, some of these risk are[9]:

– Event-driven agents to enable an intelligent/self-aware behaviour of networked devices.
– Authentication and data integrity.
– Models for decentralized authentication and trust.
– Security and trust for cloud computing.
– Data ownership, repository data management, privacy policies management and privacy preserving technologies.
– Legal and liability issues (etc.).

5.2.2.2 Integration of heterogeneous data

The sensing of urban spaces and the participation of society in the generation of content and social networks exponentially increases the volume of information available. There are three "Vs" of interest in large data volumes (i) the Volume or the amount of processed information, (ii) the Variety of the types of data that can be represented, and (iii) the Velocity (speed) at which these data are captured, transferred and processed..

Technology to create, integrate and search the heterogeneous and multi-domain data, and deliver the unified information[10]

A large-scale electronic data is generated constantly by the progress of ICT utilization and application in various sectors such as environment, medical care, administration, and education.

It reduces environmental impact, and promotes the sustainable development of the city to utilizing these heterogeneous and multi-domain data effectively in an integrated manner.

Therefore, it is proposed to include a specific type of technology to create, integrate, and search the heterogeneous and multi-domain data, and deliver the unified information as a fundamental technology for ICT infrastructure of smart sustainable cities.

The role of the technology

In smart sustainable cities, environmental monitoring with a large number of sensing devices generates a large-scale electronic data. A large scale electronic data is also generated constantly by the progress of ICT utilization and application in various sectors such as medical care, administration and education sector.

Large amounts of generated data is integrated in various forms in each domain, and utilized in cloud environment with huge data centres and high-speed networks. It can realize sustainable improvement of environment, energy, economy, and society to utilize these heterogeneous and multi-domain data efficiently.

Thus, the technology is required to create, integrate, and search efficiently and transversely the heterogeneous and multi-domain data, and deliver the unified information. The technology can realize not only the environmental impact reduction but also the community revitalization, the reinforcement of disaster prevention, and the improvement of citizens' life.

---

[9] Taken from "Internet of Things Strategic Research Roadmap" Page 34.

[10] Corresponds to a contribution of FUJITSU (Japan).

This technology helps to extract the highly correlated data set group from enormous data, and is applicable to the environment impact reduction, the energy management, the remote medical care, the disaster monitoring, e-Government, etc.

There are applications of this technology that can support disaster prevention and monitoring; ICT utilization in smart sustainable city is one of the solutions for this key role in future cities.

During disasters it is very difficult to recognize the extent of overall damage. In trying to cope with and manage disasters, the lack of information sharing among various organizations and individuals can create complications.

The technology can solve these issues by providing the appropriate information from various information accumulated including science, administrative, and SNS information.

Requirements of the technology

To be able to recognize the damage situation, and make a decision appropriately with the technology to create, integrate, and search the heterogeneous and multi-domain data and deliver unified information.

Highly correlated data set group can be discovered by searching and integrating transversely the huge heterogeneous and multi-domain data with the combination of spatio-temporal correlation, ontological correlation and citational correlation analysis. These huge data include real sensing data, social sensing data from SNS, Web archive, and scientific database, which are collected and accumulated via the Internet from various individuals and organizations such as victims, rescuers, and media.

For example, when one analyses the potential effects of environmental damage such as particulate matter air pollution (PM2.5), it is a crucial to find correlated datasets from a wide variety of sensor data individually disseminated from heterogeneous sensing sources through the Internet and sensor networks. Related to the PM2.5 sensor data, the highly correlated environmental sensor data (wind speed and direction, rainfall, temperature, humidity) and social sensor data (SNS data with the keyword about climate and the health) can be found with the spatio-temporal correlation (near, overlapping in time and location, same movement and so on) and ontological correlation (atmospheric pollution, weather, respiratory disease, and so on). These data set and their correlations are forwarded for further analysis to create and verify the correlative hypothesis with up-to-date and/or unknown PM2.5 effects.

Other possible effect(s) of the technology (To be applicable to climate change adaptation and mitigation)

To sort and analyse the information of some event in depth, it is generally important to collect the information not only in the particular field concerned but also in the various derived and affected fields.

For example, in order to sort and analyse the issue on "global warming", without the technology, it is necessary to search various information one by one to recognize the relationship among various fields, but using this technology it is easy to obtain horizontal search results including various industry, economy, energy problem, hygiene and education as well as natural disaster using climate change as search key. The technology can support the data-intensive science and give a very good sketch of various events of the real world based on many heterogeneous and multi-domain information.

5.2.3 Cloud computing and data platform

Cloud computing is another technology that is being used to build SSC, in line with the policies of green technologies to be adopted. In all cases the public administration shall ensure protection of people's privacy. Cloud computing is also one of the main forms of Green IT that refers to the efficient use of computing resources thus minimizing the environmental impacts and contribute to the reduction in energy consumption or greenhouse gas emissions.

The need of "the cloud approach, in which providers outside city government deliver a technological platform for gathering and mining data and producing city applications over the public Internet or a virtual private network, has become the favoured means for municipalities to move to the next level"[11], and that is because it is a cost effective and time and effortless solution. The infrastructure of most cities is not equipped to work with the levels of infrastructure in a smart sustainable city. On the other hand, cloud service suppliers are capable of sorting, in a good manner, many of the risks involved.

The convergence of cloud technologies should be well utilized. These include Software as a Service (SaaS), Storage as a Service (STaaS), Infrastructure as a Service (IaaS) and more, to increase availability, reliability and security, and deliver optimum quality of service applications for the large number of heterogeneous devices and platforms.

An example of IaaS cloud computing architecture is shown in Figure 29[12]:

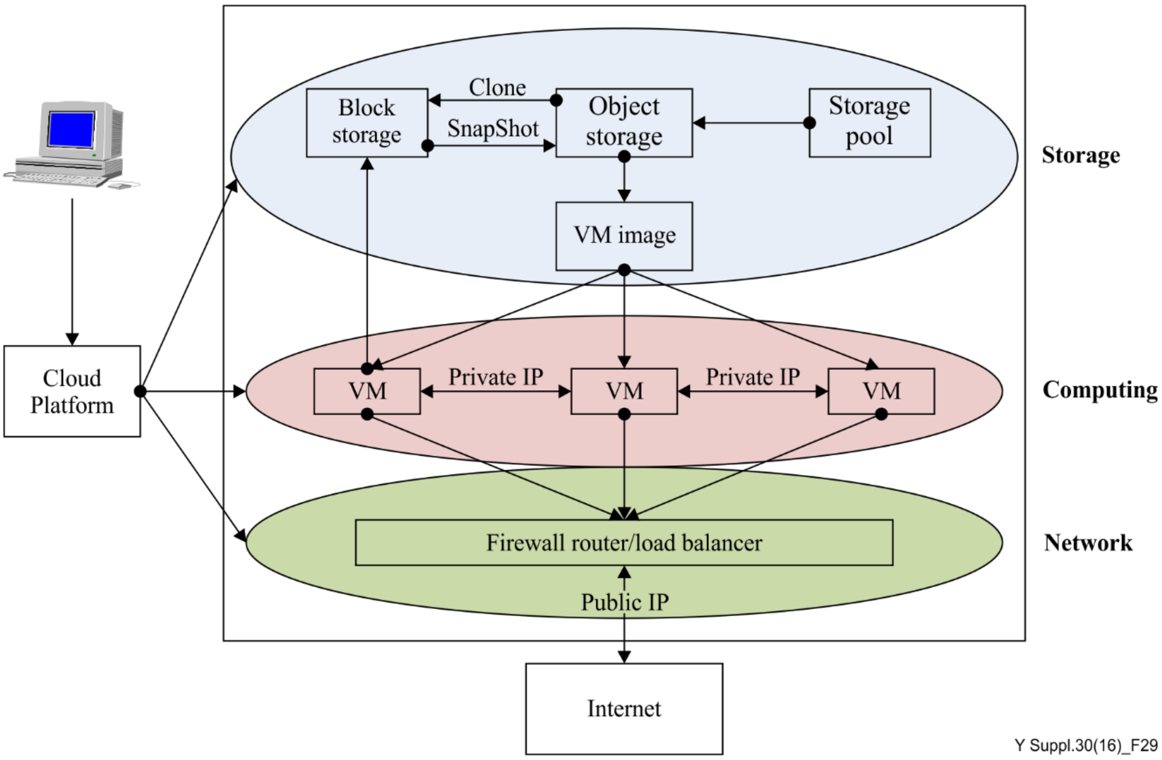


Figure 29 – Example of IaaS cloud computing architecture

The facility of storage, computing and network can be virtualized, and managed in a unified manner. So the allocation and scheduling of resources will allow for more agility, and the efficiency of resource is also higher than traditional architecture.

The secondary use of various data (so-called big data), such as individuals, companies, organizations is very useful for SSC and the information will be made available as soon as the technical report of Anonymization Infrastructure and Open Data for Smart Sustainable Cities is finalized and published in the usual manner.

Example 1: HEMS/BEMS data

The electricity demand prediction using the real-time data from smart meters enables the balancing of electricity supply-demand.

---

[11] Why Smart Cities Need Cloud Services (http://www.ubmfuturecities.com/author.asp?section_id=234&doc_id=526607).

[12] Examples extracted from recent progress of ITU-T SG13.

Example 2: Movement history data

The collection and analysis of data concerning individual movement histories provides congestion expectation information and detour information at the time of an accident outbreak.

Example 3: Medical examination history data

The collection and analysis of medical examination histories enables the identification of the infection route and decision on the necessary countermeasures against the spread/growth of the infection.

On the other hand, as far as it concerns distributing the data, there is a problem of the invasion of privacy and the leakage of confidential information.

Therefore the protocol for the secondary use of data, as shown in Figure 30, with anonymity techniques is necessary. Moreover, even if an authorized anonymity technique is repeatedly used to anonymize private data for its publication, it may cause the leak of private data when the anonymization process was accomplished independently. To prevent the leak and certify the published privacy data, anonymization infrastructure is indispensable for the future SSC applications including big-data business.

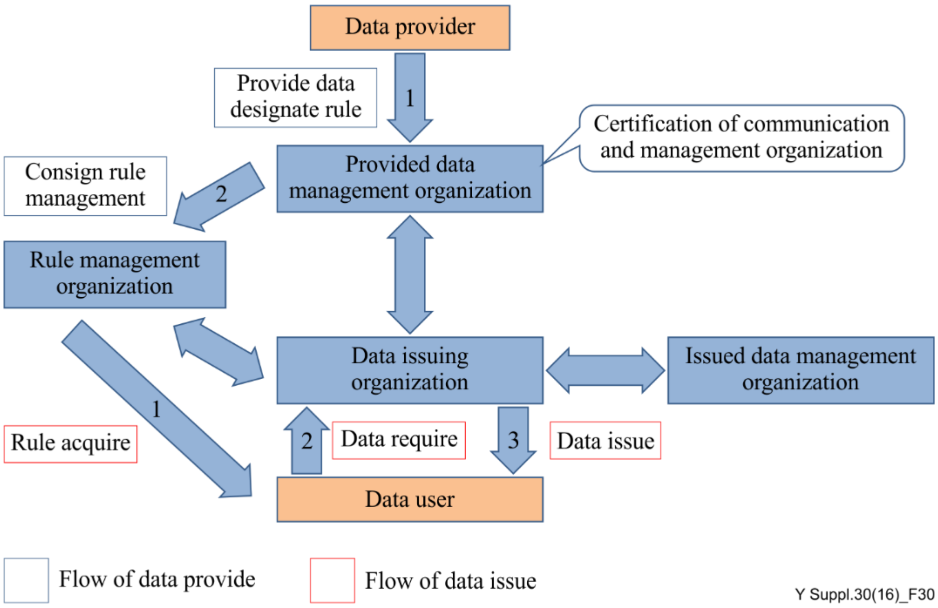


Figure 30 – Proposed protocol for the secondary use of various data

5.2.4 Augmented reality

The potential of the use of augmented reality is infinite and they are still discovering many of their applications, for example, new augmented reality technology takes designs of proposed building developments and transposed them onto a smartphone or similar device. Using this, the inhabitants of a smart sustainable city can visualize how the final result would be to make informed planning decisions. Police services can use viewers of augmented reality with facial recognition for identification of criminals, and tourists can be guided and can also display information of the attractions or monuments of the city, etc.

5.3 Terminals, sensing and multi-device layer

This section contains specifications for the users layer (Figure 5) and sensing layers (Figures 4 and 5).

5.3.1 Terminals (Gateways)

The network is not complete without interconnection equipment on the one hand and on the other with their ends that reach users and things. Sensors are one of the most important types of terminals, which are discussed in the next section.

5.3.2 Sensors

They can be categorized in sensors of resources, security, lighting, presence, weather, transportation, movement or position installed on the physical infrastructure of the SSC. These devices make it possible to meet and study the phenomena of public and private interest such as climate, congestion of the roads, air pollution, the behaviour of criminals or those attending sporting, cultural events and entertainment.

5.3.2.1 System architecture for wireless sensor networks

The emerging field of wireless sensor networks combines sensing, computation, and communication into a single tiny device. Through advanced mesh networking protocols, these devices form a sea of connectivity that extends the reach of cyberspace out into the physical world. As water flows to fill every room of a submerged ship, the mesh networking connectivity will seek out and exploit any possible communication path by hopping data from node to node in search of its destination. While the capabilities of any single device are minimal, the composition of hundreds of devices offers radical new technological possibilities.

The power of wireless sensor networks lies in the ability to deploy large numbers of tiny nodes that assemble and configure themselves. Usage scenarios for these devices range from real-time tracking or monitoring of environmental conditions, to ubiquitous computing environments, in situ monitoring of the health of structures or equipment, among others. While often referred to as wireless sensor networks, they can also control actuators that extend control from cyberspace into the physical world.

The concept of wireless sensor networks is based on a simple equation:

Sensing + CPU + Radio = Thousands of potential applications

However, actually combining sensors, radios, and CPU's into an effective wireless sensor network requires a detailed understanding of both the capabilities and limitations of each of the underlying hardware components, as well as a detailed understanding of modern networking technologies and distributed systems theory. Each individual node must be designed to provide the set of primitives necessary to synthesize the interconnected web that will emerge as they are deployed, while meeting strict requirements of size, cost and power consumption. A core challenge is to map the overall system requirements down to individual device capabilities, requirements and actions. In order to make the wireless sensor network vision a reality, an architecture that synthesizes the envisioned applications out of the underlying hardware capabilities must be developed.

5.3.2.2 Sensor network application classes

The three application classes, which have been selected, are: environmental data collection, security monitoring, and sensor node tracking. It is believed that the majority of wireless sensor network deployments will fall into one of these class templates.

Environmental data collection

An environmental data collection application is to collect several sensor readings from a set of points in an environment over a period of time in order to detect trends and interdependencies. The idea is to collect data from hundreds of points spread throughout the area and then to analyse the data offline.

At the network level, the environmental data collection application is characterized by having a large number of nodes continually sensing and transmitting data back to a set of base stations that store the data using traditional methods. These networks generally require very low data rates and extremely long lifetimes. In typical usage scenario, the nodes will be evenly distributed over an outdoor environment (see Figure 31). This distance between adjacent nodes will be minimal yet the distance across the entire network will be significant.

Environmental data collection applications typically use tree-based routing topologies where each routing tree is rooted at high-capability nodes that sink data. Data is periodically transmitted from child node to parent node up the tree-structure until it reaches the sink. With tree-based data collection each node is responsible for forwarding the data of all its descendants. Nodes with a large number of descendants transmit significantly more data than leaf nodes. These nodes can quickly become energy bottlenecks. Once the network is configured, each node periodically samples its sensors and transmits its data up the routing tree and back to the base station. For many scenarios, the interval between these transmissions can be on the order of minutes. Typical reporting periods are expected to be between 1 and 15 minutes; while it is possible for networks to have significantly higher reporting rates. The typical environment parameters being monitored, such as temperature, light intensity, and humidity, do not change quickly enough to require higher reporting rates.

In addition to large sample intervals, environmental monitoring applications do not have strict latency requirements. Data samples can be delayed inside the network for moderate periods of time without significantly affecting application performance. In general the data is collected for future analysis, not for real-time operation.

The most important characteristics of the environmental monitoring requirements are long lifetime, precise synchronization, low data rates and relatively static topologies. Additionally it is not essential that the data be transmitted in real-time back to the central collection point. The data transmissions can be delayed inside the network as long as necessary in order to improve network efficiency.

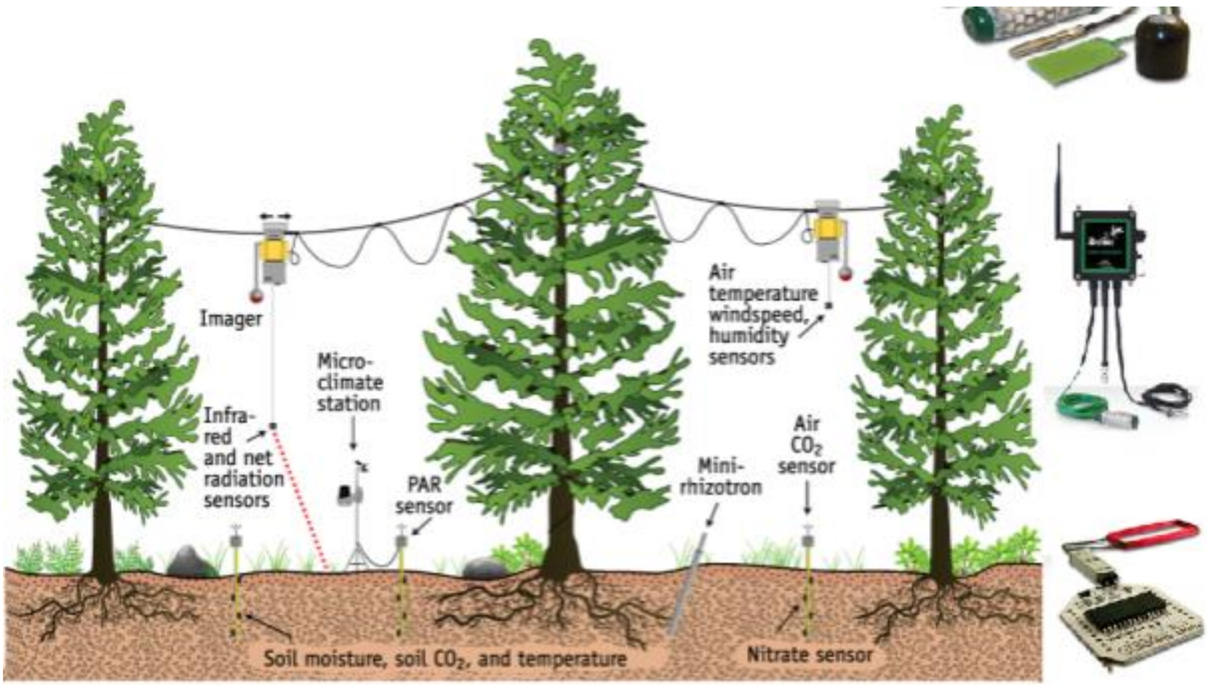


Figure 31 – Environmental data collection

Security monitoring

Security monitoring networks are composed of nodes that are placed at fixed locations throughout an environment that continuously monitor one or more sensors to detect an abnormality. A key difference between security monitoring and environmental monitoring is that security networks are not actually collecting any data. This has a significant impact on the optimal network architecture. Each node has to frequently check the status of its sensors but it only has to transmit a data report when there is a security violation. The immediate and reliable communication of alarm messages is the primary system requirement. Additionally, it is essential to confirm that each node is still present and functioning. If a node was to be disabled or failed, it would represent a security violation that should be reported. For security monitoring applications, the network must be configured so that nodes are responsible for confirming the status of each other. One approach is to have each node assigned to peer that will report if a node is not functioning. The optimal topology of a security monitoring network will look quite different from that of a data collection network.

It is reasonable to assume that each sensor should be checked approximately once per hour. Combined with the ability to evenly distribute the load of checking nodes, the energy cost of performing this check would become minimal. A majority of the energy consumption in a security network is spent on meeting the strict latency requirements associated with the signalling of the alarm when a security violation occurs.

Once detected, a security violation must be communicated to the base station immediately. The latency of the data communication across the network to the base station has a critical impact on the application performance. Users demand that alarm situations be reported within seconds of detection. This means that network nodes must be able to respond quickly to requests from their neighbours in order to forward data.

Currently there is a new generation of autonomous 3G sensors equipped with video cameras (see Figure 32) that enable the development of new security, surveillance and military applications, the wireless sensor network platform for the Internet of things.

These new video camera sensors, in conjunction with the 3G communication module, allow the creation of sensor nodes that transmit both discrete data gathered by analog and digital sensors and complex streams of real time information, such as photos and video, to servers in the cloud.

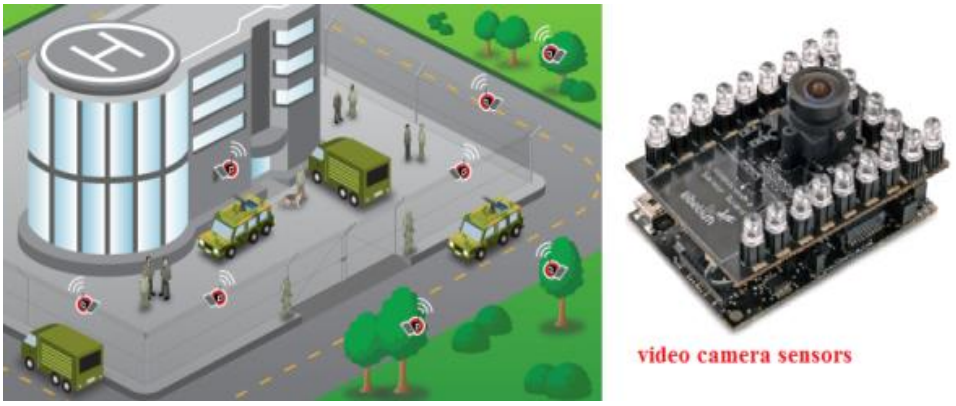


Figure 32 – 3G Sensors stream photo and video to the cloud for new security applications

This type of sensors uses ZigBee, Bluetooth and Wi-Fi protocols to send low bandwidth data such as temperature, humidity and CO2 levels, and high speed W-CDMA and HSPA mobile networks to upload video.

For security applications that require night vision mode, the new video camera sensor nodes include dozens of high-power infrared (IR) LEDs, making it possible to take pictures in total darkness. The 3G module is equipped with an internal GPS that adds geolocation information to all multimedia files.

Node tracking scenarios

This indicates tracking of a tagged object through a region of space monitored by a sensor network. There are many situations where one would like to track the location of valuable assets or personnel. Current inventory control systems attempt to track objects by recording the last checkpoint that an object passed through. With wireless sensor networks, objects can be tracked by simply tagging them with a small sensor node. The sensor node will be tracked as it moves through a field of sensor nodes that are deployed in the environment at known locations. Instead of sensing environmental data, these nodes will be deployed to sense the radio messages of the nodes attached to various objects. The nodes can be used as active tags that announce the presence of a device. A database can be used to record the location of tracked objects relative to the set of nodes at known locations. With this system, it becomes possible to request the exact location of the object and not just the last location where it was last scanned.

There are two main ways of performing outdoor location tracking when sensor devices are located in a large area such as a city. The most extensive one is to use a GPS module to get the information sent by the satellites and extract all the information possible (latitude, longitude, speed, direction). However, this methodology is not effective when requiring mobile scenarios where the nodes can change from an outdoor environment to an indoor one, such as going inside buildings, garages and tunnels.

For these cases an alternative method is used which consists of taking the information sent by the mobile phones cells and looking for their location in a previously saved data base. This information can include cell ID, RSSI and timing advance (TA) of any of the base stations which are located in the surroundings (see Figure 33).

Both GPS and GPRS technologies are complementary to each other as a system where both technologies allow the tracking of position inside buildings, garages, and even inside tunnels (e.g., subway railway system) while maintaining accurate precision of where the information from the GPS satellites can reach the sensor device. There are many technologies to obtain location information; some of them have been reviewed in chapter 3 (geo-localization for public safety and emergencies).

Figure 33 – Example of localization

Hybrid networks

Complete application scenarios generally contain aspects of all three categories. For example, in a sensor network designed to track vehicles (see Figure 34), the network may switch between being an alarm monitoring network and a data collection network. During a long period of inactivity when no vehicles are present, the network will simply perform an alarm monitoring function. Each node will monitor its sensors while waiting to detect a vehicle. Once an alarm event is detected, all or part of the network, will switch into a data collection network mode and periodically report sensor readings to a base station, where tracking of the vehicles would be in progress. As a result of this multi-modal network behaviour, it is important to develop a single architecture that can handle all the three aforementioned application scenarios.

Figure 34 – Tracking vehicles

5.3.2.3 Radio network infrastructure

The radio subsystem is the most important system on a wireless sensor node, since it is the primary energy consumer among the three highlighted application scenarios. Modern low power, short range transceivers consume between 15 and 300 milliwatts of power when sending and receiving. A key hardware observation is that low power radios consume approximately the same amount of energy when in receive or transmit mode. This energy is consumed if the radio is on, whether or not it is receiving actual data. The actual power emitted out of the antenna only accounts for a small fraction of the transceiver's energy consumption. A significant fraction goes to internal operation. As a result, the overall cost of radio communication can be dominated in some cases by the receiver power consumption – a metric that is often ignored in wireless studies.

Transmission range

The transmission range of a wireless system is controlled by several key factors. The most intuitive factor is that of transmission power. The more energy put into a signal, the farther it should travel. The relationship between power output and distance travelled is a polynomial with an exponent of between 3 and 4 (non-line of sight propagation). So to transmit twice as far through an indoor environment, 8 to 16 times as much energy must be emitted.

Other factors in determining range include the sensitivity of the receiver, the gain and efficiency of the antenna and the channel encoding mechanism. In general, wireless sensor network nodes cannot exploit high gain, directional antennas because they require special alignment and prevent ad-hoc network topologies. Omni-directional antennas are preferred in ad-hoc networks because they allow nodes to effectively communicate in all directions.

Both transmission strength and receiver sensitivity are measured in dBm. Typical receiver sensitivities are between −85 and −110 dBm. Transmission range increases can be achieved by either increasing sensitivity or by increasing transmission power. When transmitting at 0 dBm, a receiver sensitivity of −85 dBm will result in an outdoor free space range of 25-50 meters, while a sensitivity of −110 dBm will result in a range of 100 to 200 meters. The use of a radio with a sensitivity of −100 dBm instead of a radio with −85 dBm will allow you to decrease the transmission power by a factor of 30 and achieve the same range[13].

Bit rate

Unlike many high performance data networks, wireless sensor networks do not require high bit rates. 10-100 Kbps of raw network bandwidth is sufficient for many applications. Radio bandwidth has a

---

[13] The dB scale is a logarithmic scale where a 10 dB increase represents a 10x increase in power. The baseline of 0 dBm represents 1 milliwatt, so 1 watt is 30 dBm.

more significant impact on node power consumption and its lifetime in case of a battery powered node. As bit rates increase, transmission times decrease. As the highest instantaneous energy consumer, it is essential that the radio remain off as much as possible. By increasing the bit rate without increasing the amount of data being transmitted, the radio duty cycle is decreased.

Table 1 – Comparison of various hardware platforms for use in wireless sensor networks[14]

Node Type	Sample "Name" & Size	Typical Application Sensors	Radio Bandwidth (Kbps)	MIPS	FLASH	RAM	Typical Active Energy (mW)	Typical Sleep Energy (uW)	Typical Duty Cycle (%)
Generic Sensing Platform	Mote 1-$10cm^3$	General Purpose Sensing and Communications Relay	<100 kb/s	< 10	< 0.5 Mb	< 10 Kb	3V * 10-15mA	3V*10uA	1-2%
High Bandwidth Sensing	Imote 1-$10cm^3$	Rich Sensing (Video, Acoustic, and Vibration)	~ 500 kb/s	< 50	< 10 Mb	< 128 Kb	3V*60mA	3V*100uA	5-10%
Gateway	Stargate >$10cm^3$	High Bandwidth Sensing and Communications Aggregation. Gateway node.	> 500 kb/s – 10 Mb/s	> 100			3V*200mA	3V*10mA	> 50%

The last decade has seen an explosion in sensor technology (see Table 1). There are currently thousands of potential sensors ready to be attached to a wireless sensing platform. Additionally, advances in micro-electromechanic devices (MEMS) and carbon nano-tubes technology are promising to create a wide array of new sensors. They range from simple light and temperature monitoring sensors to complex sensors able to monitor more parameters and work as "digital noses" for electronic air quality control etc.

5.3.2.4 Interfaces

There are two general ways to interface with sensors that can be used in sensor networks: analogue and digital. Analog sensors generally provide a raw analogue voltage that corresponds to the physical phenomena that they are measuring. Generally these produce a continuous waveform that must be digitized and then analysed. While seemingly straightforward to integrate, raw analogue sensors often require external calibration and linearization. It is common for the sensor to have non-linear response to stimuli. The host controller must then compensate in order to produce a reading in meaningful units. Depending on the characteristics of the sensor this can be a complex process. In many cases the translation may depend on other external factors such as temperature, pressure, or input voltage. A second difficulty in interfacing with raw analogue sensors is that of scale. Each sensor will have different timing and voltage scales. The output voltage will generally contain a DC offset combined with a time-varying signal. Depending on the ratio of signal to DC component, an array of amplifiers and filters may be required to match the output of the sensor to the range and fidelity of the ADC being used to capture it.

Digital sensors have been developed to remove many of these difficulties. They internally contain a raw analogue sensor, but provide a clean digital interface to it. All required compensation and linearization is performed internally. The output is a digital reading on an appropriate scale. The interface to these sensors is via one of a handful of standard chip-to-chip communication protocols.

---

14 Extracted from http://www.isi.edu/~johnh/PAPERS/Conner04a.pdf.

5.3.2.5 Wireless platforms

In addition to the themes discussed earlier, there are a collection of other wireless networking platforms that are relevant (see Table 2).

ZigBee (IEEE 802.15.4)

ZigBee got its name from the way bees "zig and zag" while tracking between flowers and relaying information to other bees about where to find nectar resources. ZigBee is a new global standard for wireless connectivity, focusing on standardizing and enabling interoperability of products. It is a communications standard that provides a short-range cost effective networking capability; it has been developed with the emphasis on low-cost battery powered applications.

ZigBee is built on the robust radio (PHY) and medium attachment control (MAC) communication layers defined by the IEEE 802.15.4 standard. In contrast to standards like Bluetooth and Wi-Fi that address mid to high data rates for voice, PC LANs, video, etc., ZigBee meets the unique needs of sensors and control devices.

Sensors and controls do not need high bandwidth but they do need low latency and very low energy consumption for long battery lives and for large device arrays.

It is now widely recognized that standards such as Bluetooth and WLAN are not suited for low power applications, which is due to these standards' high node costs as well as complex and power demanding RF-ICs and protocols. With ZigBee, the case is different, it is the only standard that specifically addresses the needs of wireless control and monitoring applications.

Future sensor networks will be characterized by a large number of nodes/sensors which necessitate wireless solutions, very low system/node costs, they need to operate for years on inexpensive batteries; this requires low power RF-ICs and protocols, reliable and secure links between network nodes, easy deployment and no need for high data rates. Future sensor networks is a topic which is being discussed in ITU-T and other standards developing organizations that address issues surroundingM2M communications and IoT.

Table 2 – Wireless standards comparisons

Standard	ZigBee 802.15.4.	Bluetooth 802.15.1	Wi-Fi 802.11b	GPRS/GSM
Application	Monitoring & control	Cable replacement	Web, video e-mail	WAN, voice/data
System resource	4 kb-32 kb	250 kb+	1 Mb+	16 Mb+
Battery life (days)	100-1 000+	1-7	0.1-5	1-7
Nodes per network	256/65 k+	7	30	1 000
Bandwidth (kbps)	20-250	720	11 000+	64-128
Range (m)	1-75+	1-10+	1-100	1 000+
Key attributes	reliable, low power, cost effective	cost, convenience	speed, flexibility	reach, quality

This technology includes application segments in home control: wireless home security, remote thermostats, remote lighting, drape controller, automated meter reading, personal healthcare and advanced tagging, call button for elderly and disabled, universal remote controller to TV and radio, lighting, wireless keyboard, mouse and game pads, wireless smoke, CO detectors, etc.

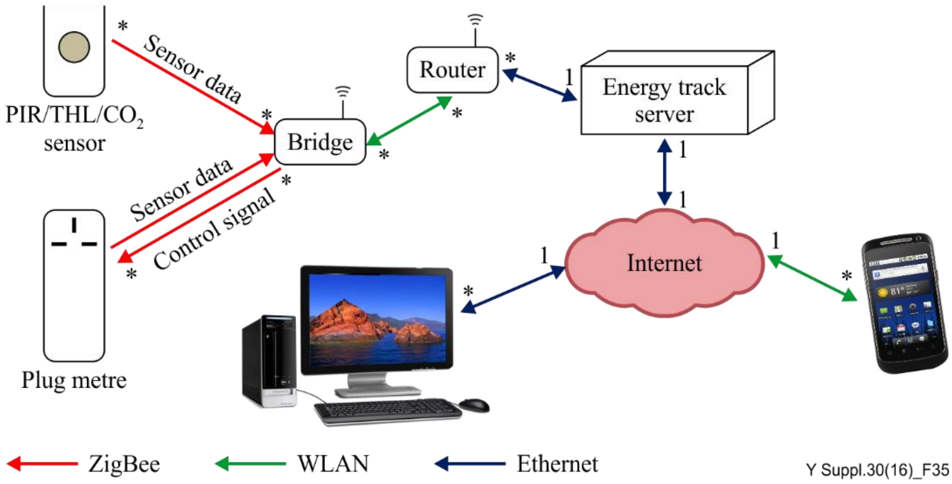


Figure 35 – ZigBee, WLAN and Ethernet

ZigBee has been widely used for its low-power consumption feature in real situations.

Figure 36 shows one of the water monitoring system by ZigBee.

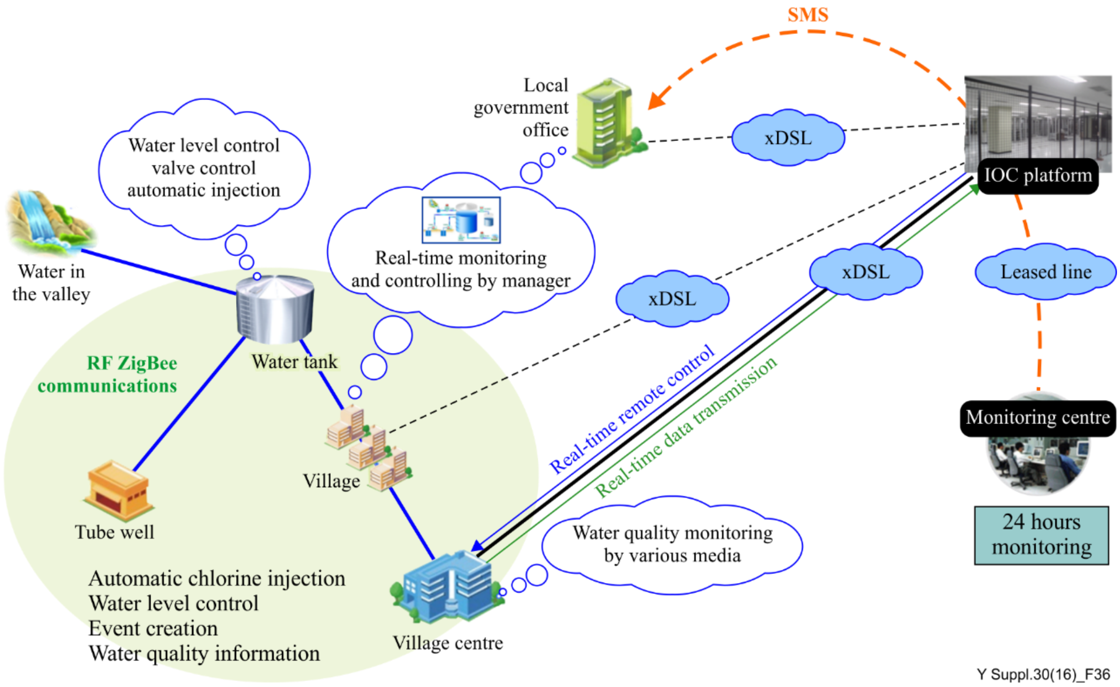


Figure 36 – Water monitoring system by ZigBee

Radio frequency identification (RFID) technology

Radio frequency identification (RFID) is a technology that is used for identification in everything from shop tagging to vehicle tracking and many more applications.

RFID technology is a simple method of exchanging data between two entities namely a reader/ writer and a tag. This communication allows information about the tag or the element carrying the tag to be determined and in this way, it enables processes to be managed more easily.

A RFID system comprises a number of elements:

– RFID reader/writer: The reader writer is used to communicate with the tags that may pass within range. The RFID reader writer will normally be located in a fixed position and will be used to interrogate an RFID tag. Dependent upon the application and the format of the system and the RFID reader/writer, data may also be written to the RFID tag.

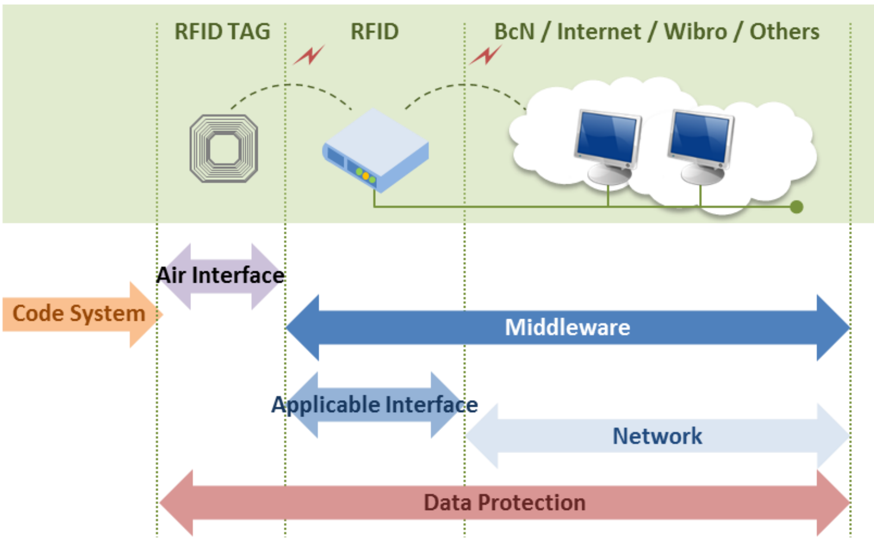
– RFID tag: RFID tags may also be called RFID transponders and are typically located on items that are mobile. They are small and generally cheap so that they can be attached to low cost (or high cost) items that need to have information associated with them. They are also generally considered as being disposable. The RFID tag contains data that is relayed to the reader, and in some systems it may also be possible to update the data within the tag to indicate that the tag and hence the item has undergone a specific stage in a process, etc.

– RFID application software: Like all systems these days, RFID systems need application software to run the overall system. With many systems there will be a number of different reader/writers and the data to and from these needs to be coordinated and analysed. A specific application software will be required for these.

Although each RFID system will vary according to its requirements, the aforementioned are the main elements which can be found.

RFID technology has become widespread in its use. It offers many advantages and RFID is a particularly versatile system, being able to be used in many areas from shops, to manufacturing plants and also for general asset tracking, as well as a host of other innovative applications.

Figure 37 describes the RFID elements:



Type	Details
Air Interface	Technical specifications regarding the wireless connection interface between the RFID tag and the reader
Code System	System of identifier codes to be recorded on RFID tags
Middleware	Common processing function of the applicable middleware system to apply various RFID
Applicable Interface	Interface for communication between the RFID reader and the applicable server system
Network	Network service function required in the applicable RFID service operation
Data protection	Data protection function required in the RFID tag/reader and applicable systems

Figure 37 – RFID elements

5.3.3 Energy harvesting

Taking advantage of different forms of energy, or through strategies of collecting the passage of people, cars, differences in salinity, currents of air through small devices, etc., is something that should happen in a smart sustainable city. Energy harvesters also provide a very small amount of power for low-energy electronics. Many sensors related to IoT, for example could feed themselves the required energy units.

Role of the technology[15]

Environmental monitoring or reducing environmental burden of application areas using ICT in SSC requires sensing network to collect data used in those areas.

To reduce the environmental burden of the sensing network itself, it is required to lessen environmental burden of the sensing devices. Sensing networks generally use an enormous number of sensing devices.

Definition of the technology

Energy harvesting technology is the technology that derives energy from the surrounding environment (environmental energy), such as light, vibrations, heat and radio waves, and converts it into electricity in order to move sensing devices, process signals and convey data through wireless networks without being supplied with electricity from any external sources such as batteries. Using environmental energy allows us to save maintenance costs for power cables and the replacement of batteries.

Energy harvesting technology includes technology for generating electricity from environmental energy and technology for storing the electricity that enables it to be used stably. See Figure 38.

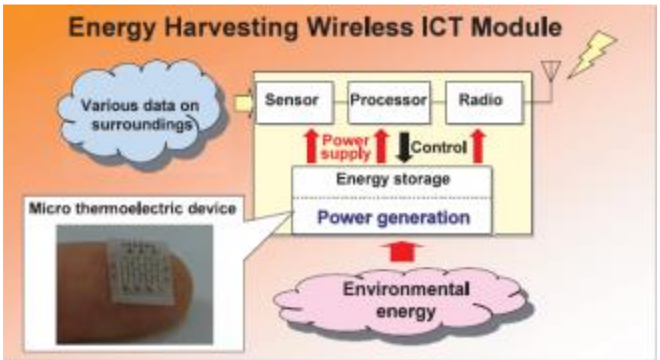


Figure 38 – Control technology to prevent decreased CPU performance

Requirements of the technology

i) To be able to harvest energy efficiently

It is required to be able to get a sufficient amount of electricity to move sensing devices, to process signals and to convey data through wireless networks. For instance, the amount of electricity produced is relatively small when only one kind of environmental energy source is used among light, vibrations, heat and radio waves. In contrast to this, when energy is derived from multiple environmental energy sources, a larger amount of electricity can be acquired.

---

[15] Corresponds to a contribution of FUJITSU (Japan).

ii) To be small and thin

Sensing devices are required to be small and thin in order to be able to adapt to a wide range of objects and to lessen the environmental burden even if used in large quantities. Notwithstanding the dimension of sensing devices, it is also required that the output power be sufficient to make them performant. Large numbers of sensing devices can be attached to various mobile objects including the human body.

iii) To be more durable

Since sensing devices are to be attached to various mobile objects including the human body, they are likely to be exposed to various environmental conditions. It is required that they do not malfunction easily even if they are moved or subject to a wide range of temperatures or moisture ranges.

iv) Not to use hazardous substances

The thermoelectric conversion is the direct conversion of temperature differences to electric voltage. A thermoelectric material creates a voltage when there is a different temperature on each side. The heavy metals such as bismuth telluride (Bi-Te) that have been used widely as the thermoelectric materials are toxic and not environmentally friendly. Such materials with large negative environmental impacts are not suitable for use in wireless ICT that is widely distributed to the environment. In contrast to this, for example, some oxide materials can be used as thermoelectric material with a small negative environmental impact.

Examples of application area

i) Environmental monitoring area

To detect environmental change and occurrence of disasters using environmental sensors.

ii) Facility management area

To detect troubles in airplanes, automobiles or plants instantaneously.

iii) Healthcare area

To monitor the user's physical condition constantly by attaching a device to the user's skin, to provide health guidance from a Cloud application, and to automatically call for an ambulance in an emergency.

5.3.4 Internet of things

The reality described in the next paragraph reflects the importance of creating mega-connection for future cities: "In 2012, there were 8.7 billion connected objects globally, constituting 0.6% of the 'things' in the world. In 2013, this number is exceeding 10.0 billion. Driven by reducing price per connection and the consequent rapid growth in the number of machine-to-machine (M2M) connections, one expects the number of connected objects to reach 50bn by 2020 (2.7% of things in the world). The connectivity costs are expected to reduce at a rate of 25% CAGR during 2012-20, which is approximately equal to the growth in number of connected objects (implying price-elasticity demand of 1). Lastly, it is believed that more than 50% of the connected objects added during 2013-20 will be added in the last 3 years of the decade. This also implies that the maximum connected objects are likely to be added when the connectivity costs are the lowest"[16].

Internet of things (IoT) is a network constituted of all kind of devices, sensors, terminals which can be part of a smart home, building, companies and SSC; which connect to each other mainly through the Internet (see Figure 39).

16 Cisco Connections Counter

The IoT will constitute the nervous system of SCC, support the interconnection and the continuous flow of information between the environment, machines, urban or rural infrastructure, and people. Besides the technology subjects discussed earlier, in this particular case, the availability of IP numbers that can be assigned to each "host" in the network is also of importance. Hence this requires a closer view to IPV6 protocol.

The IoT is a widely used term for a set of technologies, systems and design principles associated with the emerging wave of Internet-connected things that are based on the physical environment. In many respects, it can initially appear to be the same as M2M communication – connecting sensors and other devices to information and communication technology (ICT) systems via wired or wireless networks.

In contrast to M2M, however, IoT also refers to the connection of such systems and sensors to the broader Internet, as well as the use of general Internet technologies. In the longer term, it is envisaged that an IoT eco-system will emerge not dissimilar to today´s Internet, allowing things and real world objects to connect, communicate, and interact with one another in the same way humans do via the web today. Increased understanding of the complexity of the systems in question, economies of scale, and methods for ensuring interoperability, in conjunction with key business drivers and governance structures across value chains, will create wide-scale adoption and deployment of IoT solutions.

No longer will the Internet be only about people, media, and content, but it will also include all real-world assets as intelligent creatures exchanging information, interacting with people, supporting the business processes of enterprises, and creating knowledge. The IoT is not a new type of Internet network; it is an extension to the existing Internet.

IoT is about the technology, the remote monitoring, and control, and also about where these technologies are applied. IoT can have a focus on the open innovative promises of the technologies at play, and also on advanced and complex processing inside very confined and close environments such as industrial automation. When employing IoT technologies in more closed environments an alternative interpretation of IoT then is "Intranet of Things".

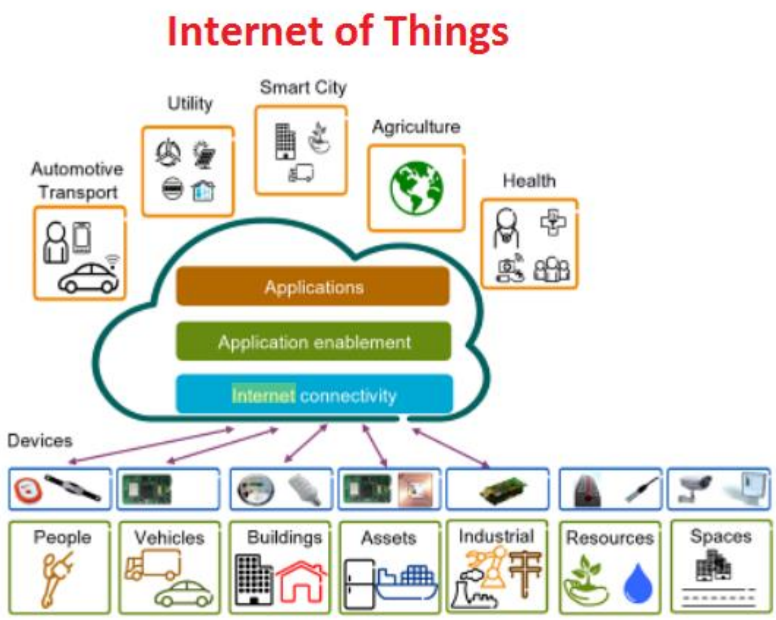


Figure 39 – Internet of things[17]

[17] Source: "From Machine-to Machine to the Internet of Things: Introduction to a New Age of Intelligence". By: Jan Holler, Vlasios Tsiatsis, Catherine Mulligan, Stefan Avesand, Stamatis Karnouskos, David Boyle.

These components could be summarize appealingly with a help of a simple equation:

Physical Object

+

Controller, Sensor, and Actuators

+

Internet

=

Internet of Things

An equation for the Internet of Things

Source: "Designing the Internet of Things". By Adrian MCEwen, Hakim Cassimaly

The IoT together with the other emerging Internet developments such as the Internet of Energy, Media, People, Services and Business/Enterprises, are the backbone of the digital economy, the digital society. The IoT developments show that there will be 16 billion connected devices by the year 2020, which will average out to six devices per person on earth and to many more per person in digital societies. Devices like smart phones and machine to machine (M2M) (or thing to thing – ToT) communications will be the main drivers for further IoT development.

By 2015, wirelessly networked sensors in everything one owns will form a new Web. However, it will only be of value if the "terabyte torrent" of data it generates can be collected, analysed and interpreted.

The first direct consequence of the IoT is the generation of huge quantities of data, where every physical or virtual object connected to the IoT may have a digital twin in the cloud, which could be generating regular updates. As a result, consumer IoT related messaging volumes could easily reach between 1 000 and 10 000 per person per day.

The IoT contribution is in the increased value of information created by the number of interconnections among things and the transformation of the processed information into knowledge for the benefit of mankind and society.

The IoT could allow people and things to be connected "Anytime, Anyplace, with Anything and Anyone", ideally using any path/network and any service. This is also stated in the ITU vision of the IoT.

The vision of what exactly the Internet of things will be, and what its final architecture will be, is still diverging and being researched on.

Figure 40 depicts the IoT smart object dimensions.

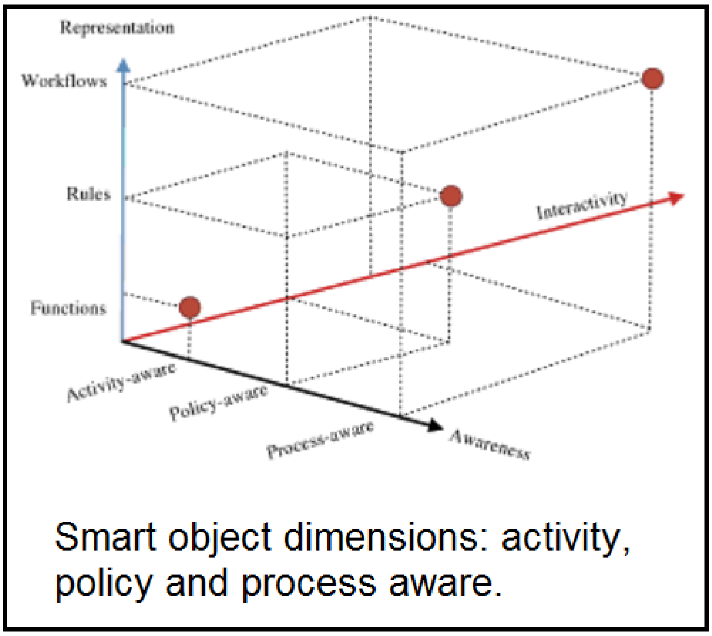


Figure 40 – Smart object dimensions[18]

Internet-of-things architecture (IoT-A)[19]

The main aim of IoT-A can be explained using the pictorial representation t shown in Figure 41.

Figure 41 – Pictorial representation of the aim of IoT-A

[18] Extracted of: Book: Internet of Things-Global Technological and Societal Trend, by Dr. Ovidiu Vermesan and Dr. Peter Friess.

[19] Extracted of document: Internet-of-Things Architecture IoT-A. Deliverable D1.3 – Updated reference model for IoT v1.5. Project co-funded by the European Commission within the Seventh Framework Programme (2007-2013).

As in any metaphoric representation, this tree does not claim to be fully consistent in its depiction, hence, it should therefore not be taken too strictly. On the one hand, the roots of this tree are spanning across a selected set of communication protocols (6lowpan, ZigBee, IPv6,…) and device technologies (sensors, actuators, tags) while on the other hand, the flowers/leaves of the tree represents the whole set of IoT applications that can be built from the sap (information/knowledge) coming from the roots. The trunk of the tree is of the utmost importance here, beyond the fact it represents the IoT-A project. This trunk represent the architectural reference model (which means here reference model + reference architecture a.k.a. ARM), the set of models, guidelines, best practices, views and perspectives that can be used for building fully interoperable IoT Concrete architecture (and therefore systems). Using this tree, one aims at selecting a minimal set of interoperable technologies (the roots) and proposing the potentially necessarily set of enablers or building blocks, etc. (the trunk) that enable the creation of a maximal set of interoperable IoT systems (the leaves).

Reference model and reference architecture

The IoT reference model provides the highest abstraction level for the definition of the IoT-A architectural reference model. It promotes a common understanding of the IoT domain. The description of the reference model includes a general discourse on the IoT domain, a domain model as a top-level description, an information model explaining how IoT knowledge is going to be modelled, and a communication model in order to understand interaction schemes for smart objects. The definition of the IoT reference model is conforming to the OASIS reference model definition [MacKenzie, 2006]. A more detailed description of the IoT reference model is provided in http://www.iot-a.eu/arm.

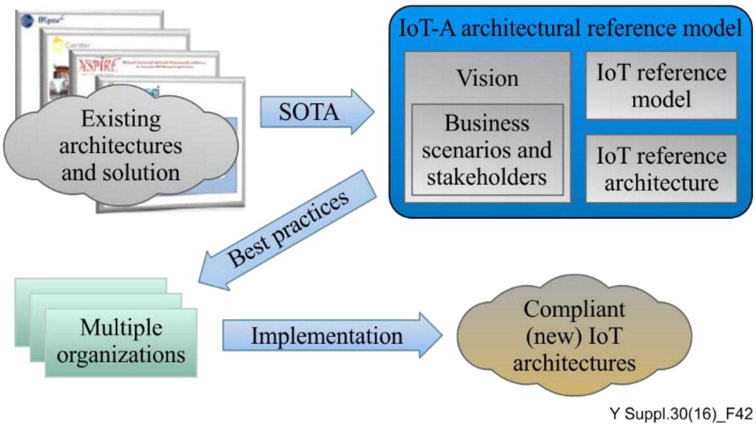


Figure 42 – IoT-Architectural reference model building blocks

Figure 42 shows an overview of the process used for defining the different parts that constitute the IoT architectural reference model (ARM). Notice that definitions of terms such as reference architecture, etc. The IoT-A ARM consists of four parts:

i) **Vision**: The vision summarizes the rationale for providing an architectural reference model for the IoT. At the same time it discusses underlying assumptions, such as motivations.

ii) **Business scenarios & stakeholders**: These are the drivers of the architecture work. With the knowledge of businesses aspirations, a holistic view of IoT architectures can be derived. Furthermore, a concrete instance of the reference architecture can be validated against selected business scenarios. A stakeholder analysis contributes to understanding which aspects of the architectural reference model need to be described for the different stakeholders and their concerns.

iii) **IoT reference model**: The IoT reference model provides the highest abstraction level for the definition of the IoT-A architectural reference model. It promotes a common understanding of the IoT domain. The description of the IoT reference model includes a general discourse on: (a) the IoT domain, (b) an IoT domain model as a top-level description, (c) an IoT information model explaining how IoT knowledge is going to be modelled, and (d) an IoT communication model in order to understand specifics about communication between many heterogeneous IoT devices and the Internet as a whole.

iv) **IoT reference architecture**: The IoT reference architecture is the reference for building compliant IoT architectures. As such, it provides views and perspectives on different architectural aspects that are of concern to stakeholders of the IoT.

The IoT domain model[20]

The relation between virtual and physical entity is usually achieved by embedding into, by attaching to, or by simply placing in close vicinity of the physical entity one or more ICT devices that provide the technological interface for interacting with or gaining information about the physical entity. By so doing the device actually enhances the physical entity and allows the latter to be part of the digital world. This can be achieved by using devices of the same class, as in the case of body-area network nodes, or by using devices of different classes, as in the case of an RFID tag and reader. A device thus mediates the interactions between physical entities (that have no projections in the digital world) and virtual entities (which have no projections in the physical world), generating a paired couple that can be seen as an extension of either one. Devices are thus technical artifacts for bridging the real world of physical entities with the digital world of the Internet. This is done by providing monitoring, sensing, actuation, computation, storage and processing capabilities. It is noteworthy that a device is also a physical entity and can be regarded as such, especially in the context of certain applications.

An example for such an application is device management, whose main concern is the devices themselves and not the objects or environments that these devices monitor.

From an IoT point of view, the following three basic types of devices are of interest:

– **Sensors**: These provide information about the physical entity they monitor. Information in this context ranges from the identity of the physical entity to measures of the physical state of the physical entity. Like other devices, they can be attached or otherwise embedded in the physical structure of the physical entity, or be placed in the environment and indirectly monitor entities. An example for the latter is a face-recognition enabled camera. Information from sensors can be recorded for later retrieval.

– **Tags**: These are used to identify physical entities to which they are usually attached to. The identification process is called "reading" and it is carried out by specific sensor devices, which are usually called readers. The sole purpose of tags is to facilitate and increase the accuracy of the identification process. This process can be optical, as in the case of barcodes and QR code, or it can be RF-based, as in the case of microwave car-plate recognition systems and RFID. The actual physics of the process as well as the many types of tags are however irrelevant for the domain model as these technologies vary and change over time. These are important however when selecting the right technology when implementing a concrete system.

– **Actuators**: They can modify the physical state of a physical entity, like changing the state (translate, rotate, stir, inflate, switch on/off.) of simple physical entities or activating/deactivating functionalities of more complex ones.

Figure 43 shows the relationship between augmented, physical and virtual entities, together with other terms and concepts.

Hardware concepts are shown in blue, software in green, animated objects in yellow, and concepts that fit into either multiple or neither categories in brown.

20 http://www.iot-a.eu/arm/120613.

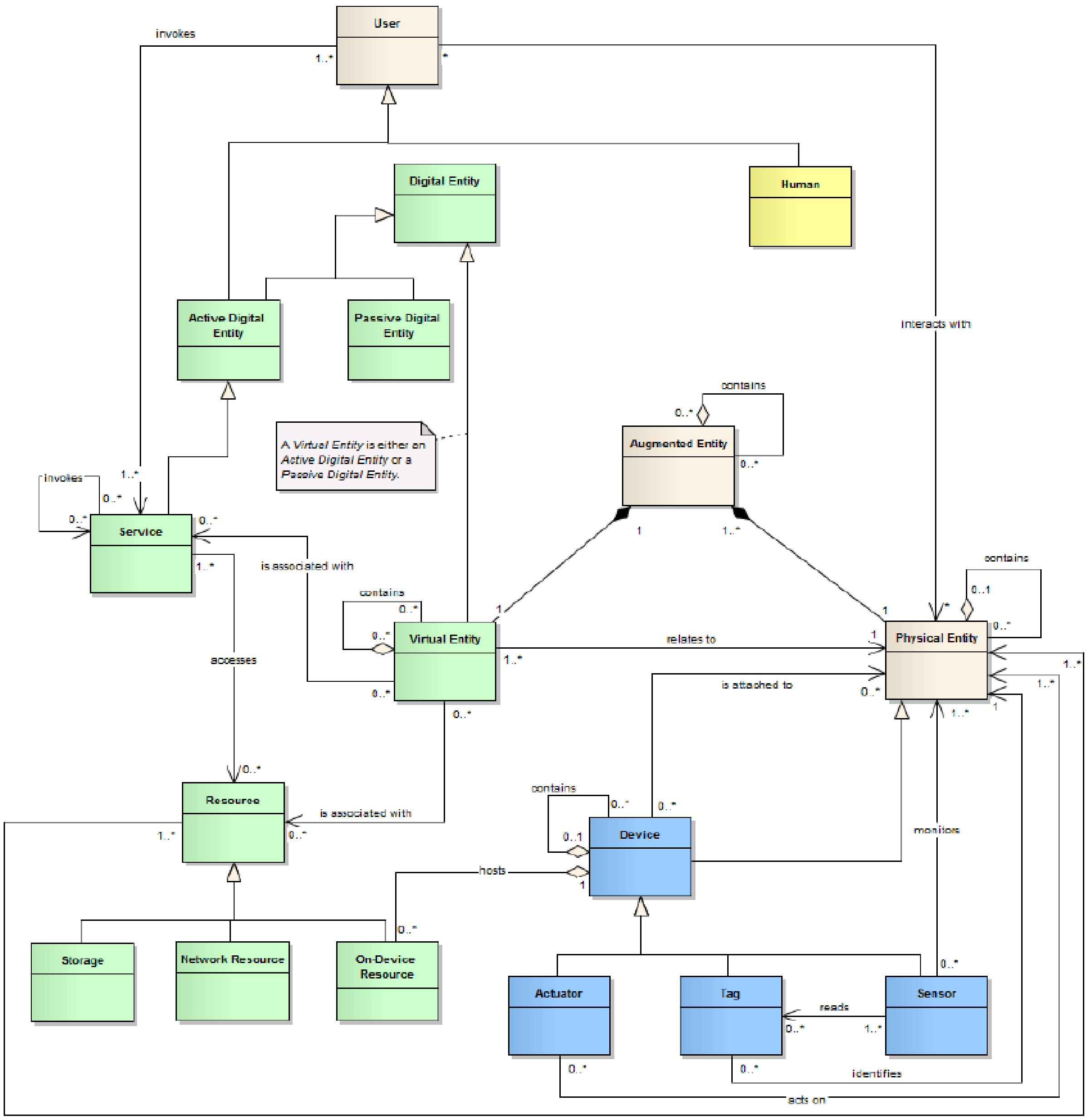


Figure 43 – IoT domain model[21]

IEEE P2413™ Working Group (WG), Internet of things (IoT)[22]

Scope and purpose

IEEE P2413™ Standard for an architectural framework for the Internet of things (IoT) defines an architectural framework for the Internet of things (IoT), including descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains. The architectural framework for IoT provides a reference model that defines relationships among various IoT verticals (e.g., transportation, healthcare, etc.) and common architecture elements.

It also provides a blueprint for data abstraction and the quality "quadruple" trust that includes protection, security, privacy, and safety. Furthermore, this standard provides a reference architecture

[21] www.iot-a.eu/public/public-documents/d1.2.

[22] http://standards.ieee.org/email/2014_06_cfp_p2413_web.html.

that builds upon the reference model. The reference architecture covers the definition of basic architectural building blocks and their ability to be integrated into multi-tiered systems. The reference architecture also addresses how to document and, if strived for, mitigate architecture divergence. This standard leverages existing applicable standards and identifies planned or ongoing projects with a similar or overlapping scope.

This standard will help to reduce current fragmentation in the various IoT verticals. By addressing the need for an IoT architectural framework, IEEE will fulfil its mission to benefit humanity by increasing the interoperability and portability of IoT solutions to both the industry and the end consumer.

IP for things

If, in a future Internet of things, everyday objects are to be addressed and controlled via the Internet, then one should ideally not be resorting to special communications protocols as is currently the case with RFID. Instead, things should behave just like normal Internet nodes. In other words, they should have an IP address and use the Internet protocol (IP) for communicating with other smart objects and network nodes.

The benefits of having IP-enabled things are obvious, even if the objects in question are not going to be made globally accessible but instead used in a controlled intranet environment. This approach enables us to build directly on existing functionality such as global interoperability, network-wide data packet delivery (forwarding and routing), data transport across different physical media, naming services (URL, DNS) and network management. The use of IP enables smart objects to use existing Internet services and applications and, conversely, these smart objects can be addressed from anywhere since they are proper Internet participants. Last but not least, it will be easy to use important application layer protocols such as HTTP.

5.4 Energy efficiency of ICT infrastructure

ICT infrastructure needs to be built considering the environmental impact of the ICT itself in a way that the environmental benefit of using ICT in other sectors will not be lower that the impact ICT infrastructure generates.

Technological solutions like power sources for infrastructure equipment using sustainable sources need to be considered when possible.

For example, a solution as shown in Figure 44 can be implemented considering the impact on fossil generated energy reduction and also the impact on operation cost.

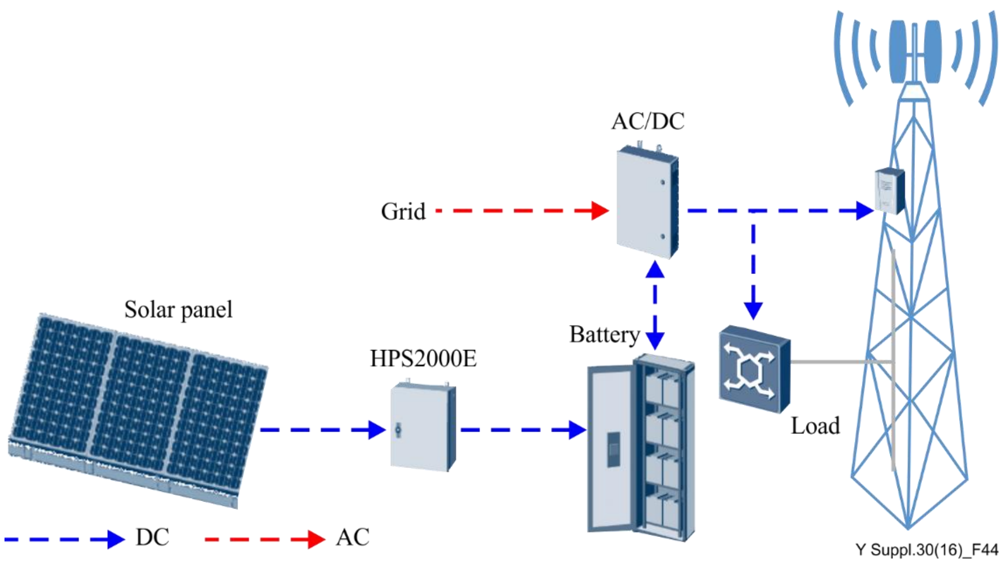


Figure 44 – Example of radio site powered by AC main and solar energy

The equipment used to build the ICT infrastructure need to be high efficiency equipment to reduce their impact and energy consumption with respect to their use.

A definition of energy efficiency metrics for ICT is available in [ITU-T L.1310] "Energy efficiency metrics and measurement methods for telecommunication equipment[23]". This Recommendation also specifies the principles and concepts of energy efficiency metrics and measurement methods for small networking equipment used in the home and small enterprise locations. The Recommendation defines that when transmission time and frequency bandwidth are fixed, a telecommunication system that can transport more data (in bits) with less energy (in joules) is considered to be more energy efficient.

The efficiency of infrastructure equipment is considered in [ITU-T L.1320]: "Energy efficiency metrics and measurement for power and cooling equipment for telecommunications and data centres[24]". The methodologies defined in this Recommendation are applied at single equipment level. The efficiency of power conversion and cooling in the data centre or telecommunication facility is only partially attributed to the equipment. The architecture and organization of the space and equipment to deliver the power or cooling to the systems is an equal, if not a more significant factor to energy efficiency. Another general factor will be the interoperability, management, and response of these systems across the demand and operational range.

Some reference values for the metrics defined in ITU-T are available in L.1340: "Informative values on the energy efficiency of telecommunication equipment[25]".

The growing demand for Internet connections from both governments and citizens is driving the rapid increase in worldwide deployment of broadband and ultra-broadband networks. Depending on the specific geographic, demographic and economic conditions, such networks can be either fixed (based on FTTx architectures and implementing technologies such as ADSL, ADSL2plus, VDSL2, GPON, GEPON, etc.) or mobile (based on HSPA, LTE, UMTS, etc.).

The increasing deployment of broadband and ultra-broadband networks has a real impact on energy consumption and, in more general terms, on the carbon footprint. To address the critical issue of energy efficiency, it is essential that particular attention be given to the choice of specific technologies during the planning phase. An informed choice of available energy-efficient telecommunication equipment is fundamental to reducing energy consumption while guaranteeing the desired level of quality of service (QoS) and reliability.

---

[23] Recommendation [ITU-T L.1310] contains the definition of energy efficiency metrics test procedures, methodologies and measurement profiles required to assess the energy efficiency of telecommunication equipments. Energy efficiency metrics and measurement methods are defined for telecommunication network equipment and small networking equipment. These metrics allow for the comparison of equipment within the same class, e.g., equipment using the same technologies.

[24] Recommendation [ITU-T L.1320] contains the general definition of metrics, test procedures, methodologies and measurement profiles required to assess the energy efficiency of power and cooling equipment for telecommunications and data centres. More detailed measurement procedures and specifications can be developed in future related ITU-T Recommendations. Metrics and measurement methods are defined for power equipment, alternating current (AC) power feeding equipment (such as AC uninterruptible power supply (UPS), direct current (DC/AC) inverters), DC power feeding equipment (such as AC/DC rectifiers, DC/DC converters), solar equipment, wind turbine equipment and fuel cell equipment. In addition, metrics and measurement methods are defined for cooling equipment such as air conditioning equipment, outdoor air cooling equipment and heat exchanging cooling equipment.

[25] Recommendation [ITU-T L.1340] provides informative values on the energy efficiency of different types of telecommunication network equipment and small networking equipment in use in both the fixed and mobile networks. These values are related to energy efficiency metrics, test procedures, methodologies and measurement profiles that have been defined in Recommendation [ITU-T L.1310]. These informative values are intended to be a valued reference resource for those in the process of choosing the most energy-efficient technologies for network upgrade and deployment and, in so doing, reducing the carbon footprint of the Information and Communication Technology (ICT) sector.

Recommendation [ITU-T L.1340] provides informative values on the energy efficiency of different types of telecommunication network equipment and small networking equipment used in both the fixed and mobile networks.

Informative values for digital subscriber line access multiplexer (DSLAM), multi-service access code (MSAN) and optical line termination (OLT) equipment[26]

This clause defines the informative values with respect to the energy efficiency metrics defined for the specific technologies used by DSLAM, MSAN and OLT equipment. More precisely, this clause covers the:

– DSLAM equipment and MSAN equipment implementing ADSL2plus, VDSL2 and POTS technologies.

– OLT equipment implementing the gigabit passive optical network (GPON), gigabit Ethernet passive optical network (GEPON) and point-to-point (PtP) technologies.

For these equipment typologies, the most commonly used metric is the Pport, which considers the number of ports at a fixed load as a functional unit.

$$\boxed{P_{port} = P_{EQ} / N_{ports} \qquad [\mathrm{W/port}]}$$

Where:

PEQ is the power (in Watts) of a fully equipped wireline network equipment with all its line cards working in a specific profile or state (e.g., all VDSL2 subscriber lines in L0 state, all ADSL2plus subscriber lines in L2 state). For DSL line cards that have additional functions (e.g., MELT, vectoring, test access and channel bonding, etc.), in addition to the bare DSL functionality, the informative value for such boards refers to a normal DSL mode of operation with any additional functions being disabled.

In [ITU-T L.1340], 5 Nports is the maximum number of ports served by the broadband network equipment under test.

Tables 3 to 5 provide informative values for these technologies.

[26] Recommendation [ITU-T L.1340]

Table 3 – Informative values for DSLAM/MSAN

Informative values for DSLAM/MSAN in L0 mode

Specific technology for DSLAM/MSAN (L0 mode)	Informative value in L0 for equipment with more than 96 ports (W/port)	Informative value in L0 for equipment with less than 96 ports (W/port)
ADSL2plus (including ADSL and ADSL2 and with transmission power of 19.8 dBm)	1.2	1.5
VDSL2 (profile 8b) transmission power 19.8 dBm	1.8	2.1
VDSL2 (profile 12a and 17a) transmission power 14.5 dBm	1.6	1.9
VDSL2 (profile 30a) transmission power 14.5 dBm	2.0	2.3
POTS (off-hook) (see Note)	2.0	2.3
NOTE – It is assumed that power consumed by the MSAN functionality which is common to both DSL and POTS is split appropriately across the two functions. For those boards, such as combo interface board and combo main control board, which integrate DSL and POTS functions, the informative values of these boards are assumed to be measured separately for each function, i.e., measure broadband with POTS disabled and vice versa.		

Informative values for DSLAM/MSAN in L2 mode

Specific technology for DSLAM/MSAN (L2 mode)	Informative value in L2 for equipment with more than 96 ports [W/port]	Informative value in L2 for equipment with less than 96 ports [W/port]
ADSL2plus (including ADSL and ADSL2)	0.8	1.1
VDSL2 (profile 8b, 12a, 17a and 30a)	1.2	1.5
POTS (on-hook)	0.5	0.8

Informative values for DSLAM/MSAN in L3 mode

Specific technology for DSLAM/MSAN (L3 mode)	Informative value in L3 for equipment with more than 96 ports [W/port]	Informative value in L3 for equipment with less than 96 ports [W/port]
ADSL2plus (including ADSL and ADSL2)	0.4	0.7
VDSL2 (profile 8b, 12a, 17a and 30a)	0.6	0.9

Table 4 – Informative values for OLT

Informative values for OLT in L0 mode

Specific technology for OLT (L0 mode) (see Note)	Informative value for equipment with more than 32 ports [W/port]	Informative value for equipment with up to32 ports [W/port]
G-PON (2.5G/1G) implementing standard Layer 2 (Ethernet) aggregation functionalities, including Multicast	11	12
G-PON (2.5G/1G) implementing also functionalities at the IP layer such as routing, MPLS and IP QoS, or more advanced Layer 2 functionality (QoS, shaping, policing)	12	13
1G-EPON (1G/1G) implementing standard Layer 2 (Ethernet) aggregation functionalities, including Multicast	7	8
1G-EPON (1G/1G) implementing also functionalities at the IP layer such as routing, MPLS and IP QoS, or more advanced Layer 2 functionality (QoS, shaping, policing)	8	9
1G-EPON (1G/1G) without Layer 2/Layer 3 aggregation functionality with 16 ports	–	13.4
10G-EPON (10G/1G) implementing standard Layer 2 (Ethernet) aggregation functionalities, including Multicast	15	16
10G-EPON (10G/1G) implementing also functionalities at the IP layer such as routing, MPLS and IP QoS, or more advanced Layer 2 functionality (QoS, shaping, policing)	16	17
10G-EPON (10G/10G) implementing standard Layer 2 (Ethernet) aggregation functionalities, including Multicast	16	17
10G-EPON (10G/10G) implementing standard Layer 2 (Ethernet) aggregation functionalities, including Multicast	17	18
PtP (1G)	2.5	4.5
PtP (10G)	18	30
NOTE – The informative values for G-PON, 1G-EPON and 10G-EPON OLT are assumed to be per port whatever the number of ONU connected to it is. The values for G-PON OLT are with Class B+ (Appendix III to [b-ITU-T G.984.2]) optical modules. Informative values reported for 10G-EPON type applies to IEEE 1904.1 Package C compliant systems.		

Equipment test methodologies for MSAN, DSLAM and OLT equipment have been defined in [ITU-T L.1310].

Informative values for wireless access technologies[27]: This clause defines the informative values with respect to the energy efficiency metrics defined for the following radio access technologies: GSM/EDGE, WCDMA/HSDPA, WiMAX and LTE.

[27] Recommendation [ITU-T L.1340] "Informative values on the energy efficiency of telecommunication equipment".

Table 5 – Informative values for GSM/EDGE/WCDMA/HSDPA/WIMAX/LTE

Informative values for GSM/EDGE network equipment

GSM/EDGE network equipment (see Note)	Informative value [W]
	0.9/1.8/1.9 GHz
GSM/EDGE radio base station (3 sectors) – full-load state	950
GSM/EDGE radio base station (3sectors) –medium-load state	750
GSM/EDGE radio base station (3sectors) – low-load state	600
NOTE – Three sectors, four carriers per sector (S444).	

Informative values for WCDMA/HSDPA network equipment

WCDMA/HSDPA network equipment (see Note)	Informative value [W]
	2.1 GHz
WCDMA/HSDPA radio base station (3 sectors) – full-load state	900
WCDMA/HSDPA radio base station (3 sectors) – medium-load state	780
WCDMA/HSDPA radio base station (3 sectors) – low-load state	690
NOTE – 3 sectors, 2.1 GHz, two carriers per sector (S222).	

Informative values for WiMAX network equipment

WiMAX network equipment (see Note)	Informative value [W]	
	2.5 GHz	3.5 GHz
WiMAX radio base station (3 sectors) – full-load state	640	610
WiMAX radio base station (3 sectors) – medium-load state	570	550
WiMAX radio base station (3 sectors) – low-load state	480	460
NOTE – 3 sectors, 2.5 GHz/3.5 GHz, 10 MHz bandwidth channel, 4 × 4 MIMO, 29:18 DL/UL sub-frame ratio.		

Informative values for WiMAX network equipment

LTE network equipment (see Note)	Informative value [W]
	2.6 GHz
LTE radio base station (3 sectors) – full-load state	1100
LTE radio base station (3 sectors) – medium-load state	950
LTE radio base station (3 sectors) – low-load state	750
NOTE – 3 sectors, 2.6 GHz, 20 MHz bandwidth channel 2 × 2 MIMO.	

The impact of ICT infrastructure could also be verified as global impact not considering only the energy consumption but also the total foot print using methodology that estimate the GHG emission of an equipment, network and service.

Recommendation [ITU-T L.1410] provides a "Methodology for the assessment of the environmental impact of information and communication technology goods, networks and services[28]". This Recommendation is part of a series of Recommendations dealing with the environmental impact assessment of ICTs.

Recommendation [ITU-T L.1400] "Overview and general principles of methodologies for assessing the environmental impact of information and communication technologies" provides a general framework and guidance and describes the full series. This Recommendation has been developed to complement ISO 14040 and ISO 14044 for the assessment of the life cycle impact of ICT goods, networks and services. It focuses on the assessment of energy consumption and greenhouse gas (GHG) emissions.

The development of ICTs has led to concerns regarding its environmental impact. Taking into consideration the on-going efforts within the United Nations Framework Convention on Climate Change [UNFCCC] to combat climate change, ITU-T decided to develop an internationally agreed methodology to help the ICT sector to assess the environmental impact of ICT goods, networks and services, focusing on energy consumption and GHG emissions.

5.5 Example of designing an open access network for smart cities

5.5.1 Background

Establishing the "Smart Cities" is one of the biggest trends around the globe in developed countries. The concept of the smart cities is to deploy advanced voice, data, video and control & management communication systems and provide high tech connectivity services to residential and business users and at the same time deploy hi-tech city management and community information portals. Some of the world's great economies like Middle Eastern countries have already started working on developing smart cities and couple of projects execution are in progress. At the same time it has become a normal practice to receive RFPs for telecom and network parts of smart cities from different governments and organizations.

In this Supplement an effort has been made to share some experience which has been learnt while designing and planning Smart City Network Solutions in Saudi Arabia. Although this is a huge topic and it is difficult to explain all the details in a few pages, efforts have been made to convey high level information which can be useful for product and solution managers.

5.5.2 Needs and challenges

The major focus here is on the communication network part of the smart cities projects. Although there are different approaches in deploying communication network for residential and business users e.g., Active Ethernet, PON networks etc. but GPON is the choice of most of the network operators around the globe. Although there are different pros and cons of the two solutions, GPON is the choice of the majority of operators due to its economy of scale and ease of deployment and management.

In smart cities, network operators generally prefer to deploy open access network and try not to be responsible for service delivery to the end subscriber. They opt to go with open access network approach which can be utilized to provide connectivity to the end users for multiple service providers. For example this will be a type of network which can be used to deliver high speed internet (HSI) service from one service provider and voice service from another service provider to a single user or the user can opt to go with all triple play services from a single service provider.

---

[28] This Recommendation provides specific guidance on energy and greenhouse gas (GHG) impacts. Recommendation [ITU-T L.1410] is organized in two parts: Part I (clause 5) – ICT life cycle assessment: framework and guidance. Part I deals with the life cycle assessment (LCA) methodology applied to ICT goods, networks and services (ICT GNS). Part II (clause 6) – Comparative analysis between ICT and a reference product system (baseline scenario); framework and guidance. Part II deals with comparative analysis based on LCA results of an ICT GNS product system and a referenced product system.

The biggest challenge in designing such networks is that the network components and equipment must be able to support the features and functionalities that can help in separating and segregating different types of services from different service providers, which are being delivered to different subscribers.

Designing an open access network is a bit different than a normal FTTx network. It is generally assumed that a network planned for triple play services using GPON technology can be utilized as an open access network. We need to understand that this is not completely true. Generally the networks deployed by telecom operators are not open access network and the reason behind is that the telecom operators are themselves responsible for the service delivery and want full control over their deployments. They do not take service from other operators and serve their users. Actually the complete end-to-end network and service delivery is managed by single network operator. Such networks do not fall under the category of open access networks. While designing the open access networks it must be kept in mind that not all OLTs, ONTs, routers and switches support open access network feature. There are limited number of devices which can be utilized for such deployments. Product selection is very critical and any mistake during this stage can be devastating at later stages.

5.5.3 About open access network

Open access provides a network business model that separates the physical bearer network from the service network. The infrastructure of an open access network, including passive infrastructure (optical fibres, equipment room premises, and cables) and active network devices, is built by an operator. Retail service providers (RSP) directly lease bandwidth on the infrastructure network to provide service packages to end subscribers.

In the conventional model, an operator builds and operates its network and delivers services to end-users. Unlike the conventional model, open access builds a layered network over which separate service providers deliver their services.

Open access brings the following benefits:

– Maximizes the freedom of choice for end users. End-users have more services to choose from and can even switch from one service provider to another without changing their home terminals (such as their ONTs).

– Lowers investment risks for retail service providers. The business model of ppen access greatly shortens the cycle of return on investment (ROI). The traditional business model of operators, who usually have monopoly over their networks, requires an ROI cycle of 8-10 years. The open access business model shortens the ROI cycle to 1-2 years. Hence open access lowers the investment entrance level and risks for RSPs, and promotes competition and innovation.

– Opens up a wider arena for RSPs. RSPs no longer need to build the infrastructure network and are able to focus on innovation and competition of services and contents.

5.5.4 Solution high level details

There are different models of deploying open access networks as shown in Figure 45, but Model-3 is the most common in the Middle East.

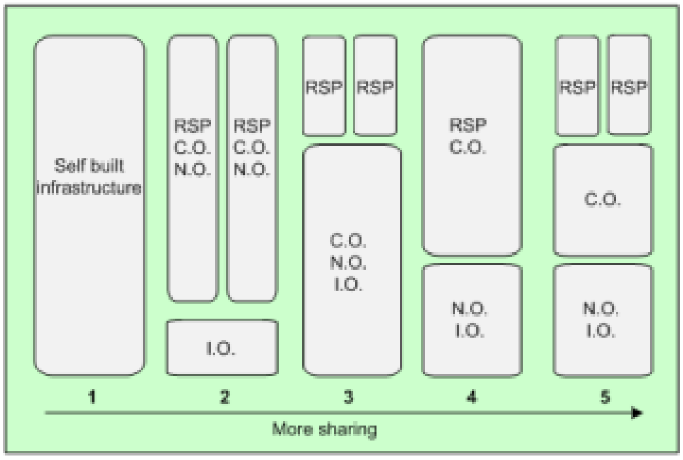


Figure 45 – Models of deploying open access networks

In this diagram:

– Infrastructure operator (IO): who operates utilities such as ducts and wire poles.

– Network operator (NO): who operators resources such as optical cables.

– Communications operator (CO): who operates active equipment, such as optical line terminals (OLTs) and optical network terminals (ONTs) on the network.

Retail service providers (RSPs): who retail services such as data, voice and video services.

In the model-3, communication operations (CO), network operations (NO) and infrastructure operations (IO) are managed by the main network owner and only services are provided by the external retail service providers.

This brief study focuses on CO part in the following sections. The most common open access network CO architecture for the smart cities is shown in Figure 46.

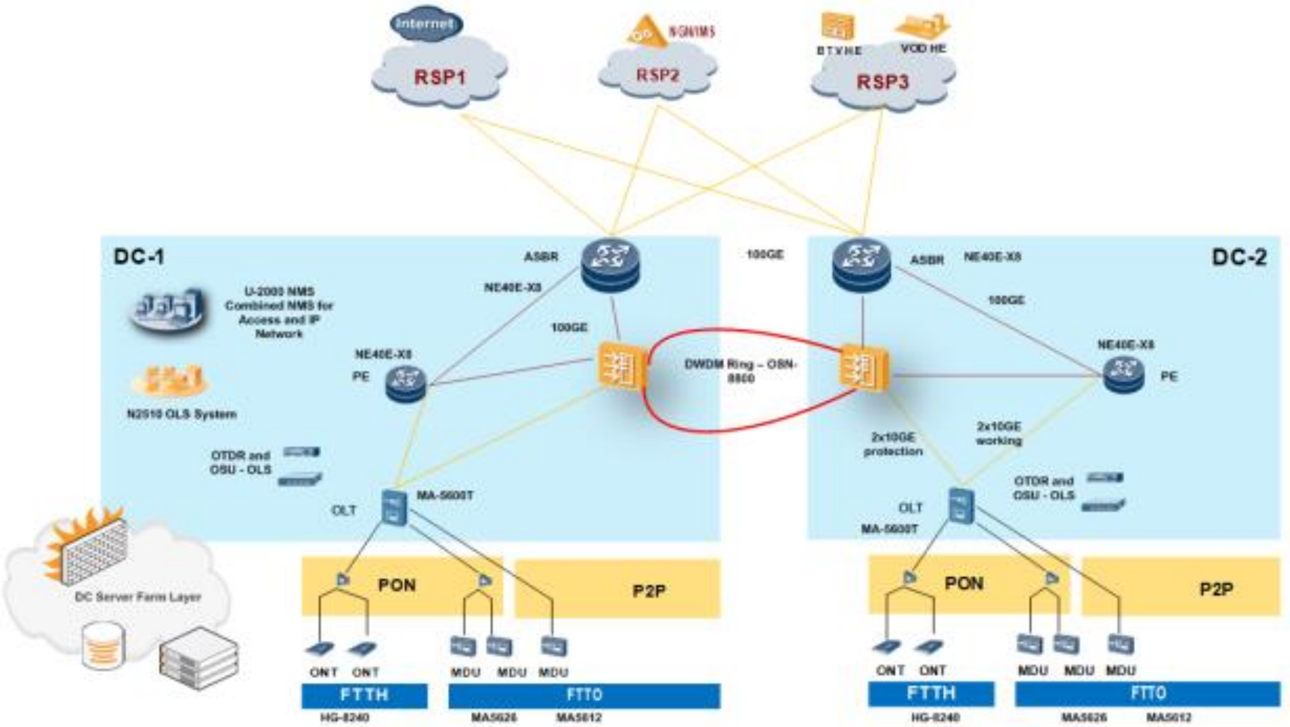


Figure 46 – The most common open access network CO architecture for smart city

The Network can be divided into the following components:

1) GPON network;
2) IP-MPLS backbone network;
3) Transmission network;
4) ODN network;
5) Network management system.

Additionally, QoS, security, VLAN, redundancy, service provisioning, network monitoring and fault management are the features which need to be considered while designing the network.

5.5.5 GPON network

GPON network in open access network is based on standard GPON Solution. GPON ports, boards (OLT dimensioning) is done based on standard procedures for GPON network design. Type-B protection is the preferred choice of the operators for GPON network. One important and major difference than the conventional GPON network is the ONT at subscriber site. There are limited ONTs which can be used for the open access model. ONT models are given below. This should be considered when deciding ONTs for your network.

Another important point is that every service provider has to provide its own home gateway or residential gateway which will be connected with ONT to provide the services which have been subscribed by the end user to that particular RSP. In standard open access network ONTs provided by network operators are demarcation points for RSPs, and network operator's network and actual services are not provided by the ONTs provided by network operators. Anyhow there are scenarios where network's operator's ONT can be used for service provisioning but there are limitations in this scenario. Generally ONTs provided by network operators are run in bridge mode and routing, NATing, WiFi, security and voice services are provided by HG/RG owned and managed by RSPs.

While planning for service provisioning and network operations, demarcation points should be clearly defined between RSPs and network operators.

Business users are generally provided GE level connectivity and P-to-P connectivity is provided by OLTs Ethernet boards. Redundant connectivity is provided using 2 ports on OLT and it is preferred to use single fibre bidirectional solution to save the fibre required for business users connectivity. To provide connectivity to business users MDUs are the preferred choice at customer end, as they provide abundant types of interfaces for voice, data and video transmission. In scenarios where end business user only requires Ethernet, specialized Ethernet switches can be utilized easily.

Table 6 contains an example of an open access network design (including GPON).

Table 6 – Contains an example of an open access network design

Classification	Example of product or hardware	Description
OLT	Infrastructure access network equipment	Large-capacity OLT
	Infrastructure access network equipment	Medium-capacity OLT
ONT	Home gateway equipment	Bridging+voice type, providing two POTS ports and four GE ports.
	Home gateway equipment	Bridging type, providing four GE ports.
Hardware dependency	Service CPU used for subsystem for control plane traffic processing (SPUA)	Use the SPUA board for upstream transmission when bandwidth control at RSP level or at RSP service level is required on the upstream ports of the OLT.

5.5.6 IP-MPLS network backbone network

This clause discusses the IP-MPLS (converged IP network) part of the network. Table 7 provides examples of products that support open access network IP-MPLS networks.

Table 7 – Products which support open access network IP-MPLS network

Network Layer	Equipment Role	Functionality	
Aggregation network	AGG-LSW	The AGG-LSW aggregates enterprise users' services from ACC-LSWs/SBUs.	
	Access LAN switch (ACC-LSW)	The ACC-LSW provides Ethernet leased-line access services for corporations. It is connected to corporation CPEs.	
	User-facing provider edge (UPE)	The UPE is on the edge of the aggregation network, directly connected to the OLT or AGG-LSW.	
	AGG	The AGG is an aggregation switching device. It is directly connected to the BRAS.	
Backbone network	Provider Edge (PE)	The PE is on the edge of the backbone network, directly connected to the MAN.	
	Provider (P)	The P is a core device of the backbone network, and is connected to the PE and RPE.	
	RSP-end Provider Edge (RPE)	The RPE is connected to the RSP network.	

The L2/L3 hybrid bearer mode is used in the open access network flexible aggregation/backbone layer scenarios. Residential HSI and VoIP services are transparently transmitted to RSP networks. Residential IPTV services are transmitted to the PE through L2VPN, and the PE forwards the services to the ASBR through L3VPN (see Figure 47).

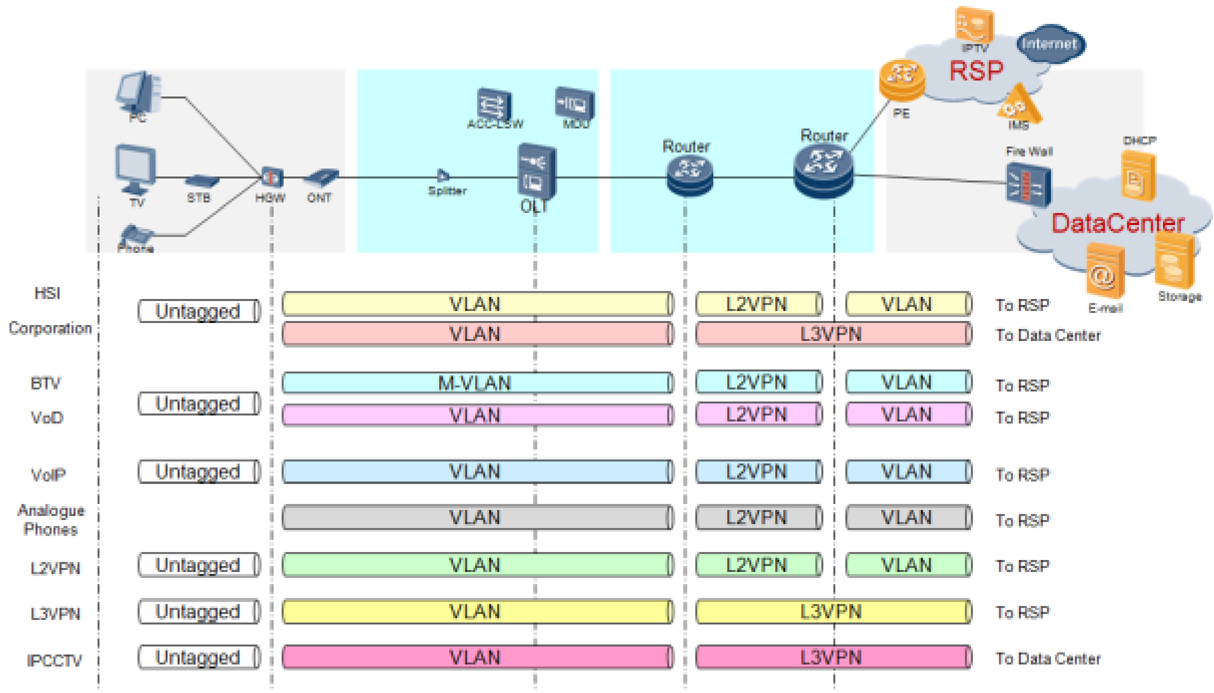


Figure 47 – Service bearer solution

Complete service types supported by the open access network are given in Table 8:

Table 8 – Complete service types supported by the open access network

User Type	Service Type	Service Name
Residential user	High-speed Internet access service wholesale	HSI wholesale
	Voice service wholesale	VoIP wholesale
	IPTV service wholesale	Broadcast TV (BTV) wholesale
		Video on Demand (VoD) wholesale
Enterprise (either corporation or small-to-medium enterprise)	Dedicated Internet access (DIA) service wholesale	Corporation DIA wholesale
	L2VPN service wholesale	Point-to-point E-LINE wholesale
		Multipoint-to-multipoint E-LAN wholesale
	L3VPN service wholesale	L3VPN wholesale
	Voice service wholesale	Corporation VoIP wholesale

5.5.7 Transmission network

The sole purpose of the transmission network in smart city network is to provide high capacity connectivity between different data centres and POPs where OLTs and other access aggregation equipment is installed. DWDM is the preferred technology with 100G, 40G and 10G Ethernet carrying wavelengths. Additionally, DWDM can be deployed in ring and mesh to provide redundancy on Layer-0.

ODN Network consists of fibre optic cables, ODFs, cabinets, splitters and related accessories. ODN network is designed to provide type-B protected connectivity to the residential subscribers towards the OLTs at aggregation and data centre sites. Splitters with 1:32 split ratio are used to provide 80Mbps connectivity to residential subscribers.

Optical line supervisor (OLS) systems are deployed to monitor the fibre optic cable. Any fibre cuts occurring in the ODN network are immediately identified by the OLS (e.g., N2510) system and field staff is informed to rectify the faults.

If customer shows interest in Huawei's ODN solution then iODN solution should be presented. Generally it has been learnt that network operator's do the design for ODN themselves or via some 3rd party consultants.

Business users are provided P-to-P connectivity to provide GE level connectivity on fibre. Redundant fibres are used to provide protected connectivity.

5.5.8 Network management system

Open access network involves interoperation across carriers and wholesale of triple-play services. These scenarios require comprehensive network management and O&M solutions to ensure network manageability and maintainability. Smooth deployment of wholesale services and rapid fault locating has become major concerns.

The network management system is located at the NE management layer and the network management layer in the telecommunication management network (TMN). It has all NE-level and network-level management functions. Figure 48 shows the positioning of the NM in the TMN.

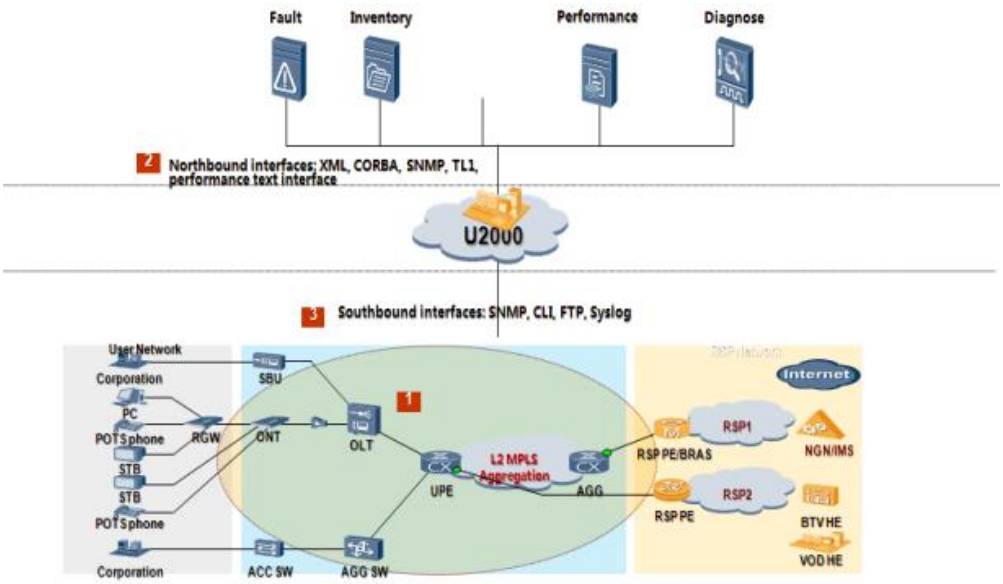


Figure 48 – Positioning of the NM in the TMN

The processes which need attention while planning NMS System include:

1) Service rollout process for RSPs
2) Service rollout process for network operators
3) Fault locating solutions
4) Alarm management and health check

5.5.9 Other design areas and considerations

While designing the open access network the following areas need special attention and agreement with customer/network operators:

1) VLAN design: Broadband service types, user locations, and RSPs to which users belong are identified by VLAN. In this manner, packets are classified and separately transmitted, and QoS is performed.
2) IGP Routing Design: Depending on IGP section, may include OSPF or ISIS routing protocol.
3) BGP routing design: In the open access network flexible aggregation/backbone layer scenario, BGP is used to transmit service routing information on the aggregation and backbone networks and between the open access network and RSP network.
4) Multicast routing: IPTV wholesale services are carried over multicast VPNs (MVPNs) on the metro aggregation and backbone networks. MVPN routes need to be deployed on the public network and VPNs.
5) MPLS design: In the flexible open access network aggregation/backbone scenario, the aggregation and backbone devices are deployed in the same MPLS domain. All wholesale services except IPTV wholesale services are carried using MPLS on the aggregation and backbone networks.
6) Voice, HSI and IPTV service bearer design.
7) Enterprise solutions: E-Line, E-LAN and Layer-3 VPN solution design.
8) End-to-End network reliability design.
9) QoS and network security design.

5.6 Adaptation to climate change effect

5.6.1 Recommendation [ITU-T L.1500] describes a framework for information and communication technologies (ICTs) and adaptation to the effects of climate change. This framework identifies and defines the basis for development of the following Recommendations:

– Recommendation [ITU-T L.1501] on best practices on how countries can utilize ICTs to adapt to the effects of climate change - It also provides a framework and a checklist for countries to integrate ICTs into their national strategies for adaptation to climate change.
– [ITU-T L.1502] on adapting the ICT sector and its infrastructure to the effects of climate change. It will provide a set of guidelines, requirements and best practices to be referred to during operation, maintenance, upgrade and improvement of existing infrastructure and when planning, designing and constructing ICT projects, goods and services to adapt to the effects of climate change.

The adverse effects of climate change pose a threat to the development and sustainability of the ICT sector and related sectors. To ensure sustainability of the ICT sector and other sectors it is important to develop adaptation strategies to address the effects of climate change. There are key areas of action to be considered in the design of ICTs and climate change adaptation strategies, including policy development and the establishment of adequate structures and processes. At the sectoral level, sector-specific strategies need to be developed to ensure sustainable development in the face of climate variability and change.

ICTs therefore have a strategic role to play in ensuring the adaptability of other sectors. Furthermore, the ICT sector itself is vulnerable to the effects of climate change and should strategically evolve to adapt infrastructure to such changes. This can be done at several levels, from the international, national, sectoral and community level, as shown in Figure 49.

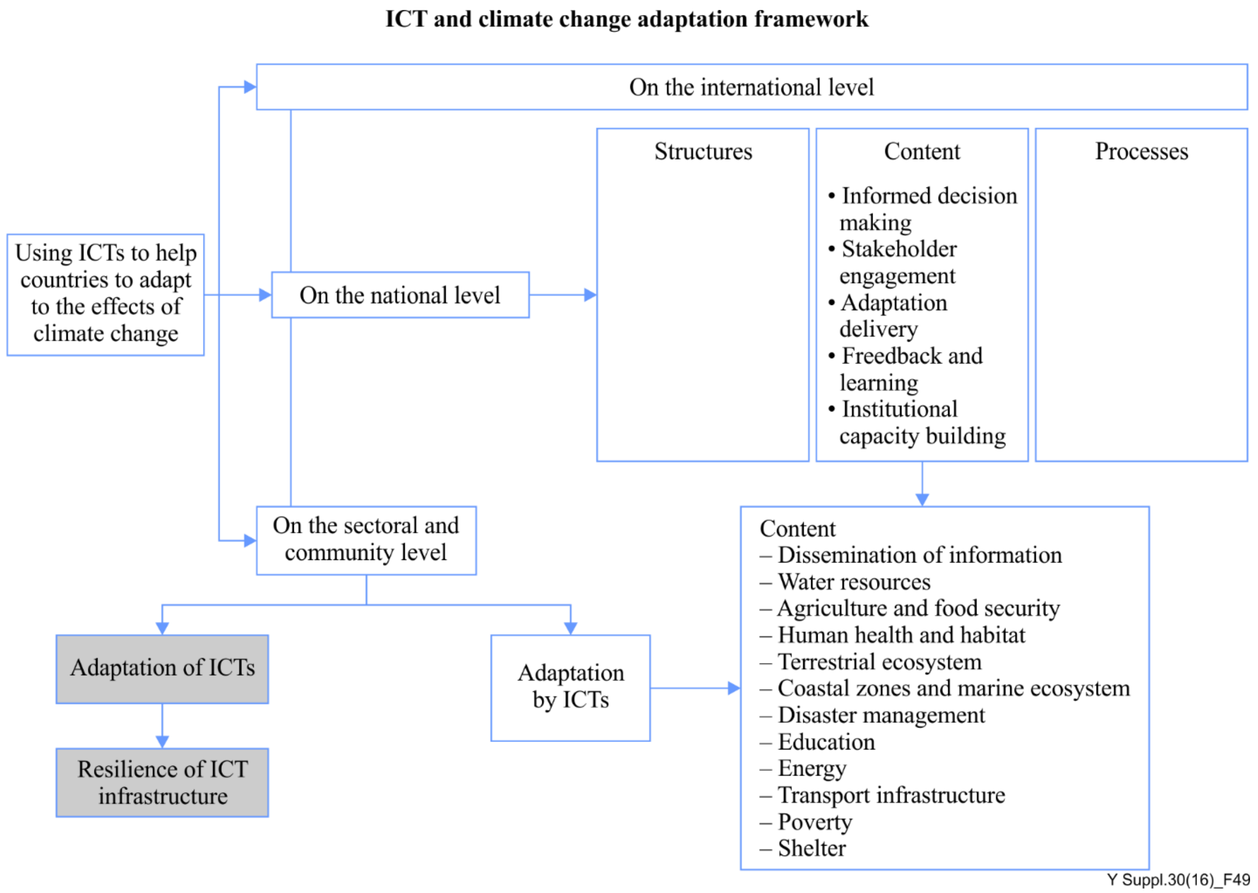


Figure 49 – ICTs and a framework for adaptation to climate change

The differences in strategic approach at various levels, and between the ICT sector and other sectors, bring out a need for several adaptation approaches specific to the ICT sector and for countries to use.

Climate change adaptation

[ITU-T L.1502] proposes the development of the work in the following areas:

– Description of ITU-T L-series Recommendations on how ICTs can help countries to adapt to the effects of climate change. This Recommendation provides an overview of how ICTs can help countries to adapt to the effects of climate change. It will also provide a framework and a checklist for countries to integrate ICTs into their national strategies for adaptation to climate change. This Recommendation will be designed to assist countries in integrating ICTs into their national climate change adaptation strategies. Recently, the effects of climate change seem to have grown quickly. In some cases it might already be too late or too costly to cope with the impact by improving the hardware, e.g., by making various social infrastructures physically strong, resilient and highly durable. It is therefore extremely important to make the best use of ICTs in saving human lives and minimizing social damages and difficulties.

– Description of ITU-T L-series Recommendations on how information and communication technologies (ICTs) can adapt to the effects of climate change. This Recommendation describes how information and communication technologies (ICTs) can adapt to the effects of climate change. It will provide a set of guidelines, requirements and best practices to be referred to during operation, maintenance, upgrade and improvement of existing infrastructure and when planning, designing and constructing ICT projects, goods and services to adapt to the effects of climate change.

5.6.2 Recommendation [ITU-T L.1501]: This Recommendation deals with how countries can utilize ICTs to adapt to the effects of climate change. It provides a framework for countries to integrate ICTs into their national strategies for adaptation to climate change.

The Recommendation also provides a checklist as an instrument for policy makers to ensure that they have the necessary pre-requisites to adapt the suggested framework in their national legislations, enabling them to assess the adoption and implementation of the framework.

Framework for ICTs and climate change adaptation

The Recommendation provides the multi-level framework for ICTs integration in climate change adaptation for countries to integrate ICTs into their national climate change adaptation strategies.

Figure 50 shows the relation between ICTs and climate change adaptation.

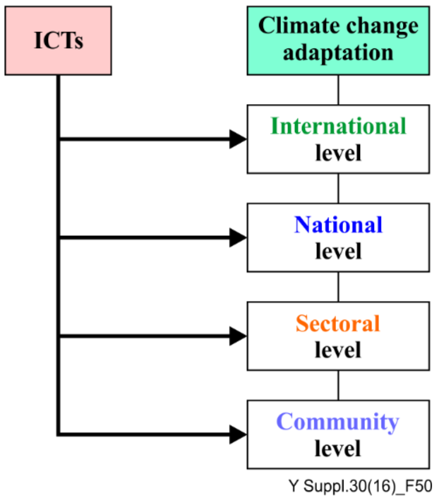


Figure 50 – Framework for ICTs and climate change adaptation

6 Physical infrastructure and its intelligent upgrading

ICT infrastructure allows to improve appreciably and intelligently, the rest of major infrastructure of a city. This infrastructure also serves to deploy ICT networks and systems and it is organized in groups located in Layer 2 (non ICT-based hard infrastructure) and Layer 3 (ICT-based hard infrastructure) of SSC ICT eta-architecture (Figure 2).

The infrastructure concerns the following aspects:

– Water supply utilities, enhanced by smart water infrastructure.
– Energy supply utilities, upgraded with smart grids.
– Transportation networks, supported by intelligent transportation systems (ITS).
– Facilities for Health and care, supported by smart health systems.
– Safety and emergency infrastructure, accompanied by ICT for emergency management.
– Education and tourism facilities (i.e., schools and hotels), enhanced by corresponding ICT solutions.
– Buildings and smart buildings systems.
– Government infrastructure, upgraded by e-government solutions.
– Business facilities, streamlined and enhanced by e-business systems.

In fact, in addition to the traditional telecommunications networks deployed in cities, road infrastructure (rail and road), electrical lines, pipelines for hydrocarbons, gas distribution networks and water ducts can serve as support for greater deployment of such telecom networks.

Road networks often favour long distance telecom network deployments, as they facilitate the laying of fibre optic cables. There is greater diversity of deployments in urban areas, because operators use roads, as well as poles, sanitation ducts, etc. They usually use the streets as a guide to the communication networks.

6.1 Energy and water

6.1.1 Smart energy

Smart grids are one of the main smart energy concepts that are developed to ensure: i) reliability, ii) self-healing, iii) interactivity, iv) compatibility, v) energy saving, vi) optimal use of energy from renewable sources, vii) safety, and viii) minimum carbon footprint.

Concerns about legacy ICT infrastructure for energy management

The operation of an electrical grid is a complex task driven by different needs: balancing the production and consumption of energy, maintaining the stability of frequency and voltage, protecting the electrical equipment against overcurrent and short circuits, assuring system reliability, restoring from disturbances (shunt faults, equipment failure with subsequent isolation, switching surges and lightning strikes, mechanical damages), etc.

Current electrical grids show quite a hierarchical structure. The energy is mainly flowing from the (few) generation sites, through the electrical transport and distribution infrastructure, to the users. Legacy communication architectures for electricity grids are thus hierarchical architectures that reflect the classical structure of the power grid: measurements and data flow up from bottom (equipment and metering infrastructures) to higher levels (management centres), while control information is transmitted in the opposite direction. However, communication infrastructures have mainly been deployed in the higher segment of electrical networks, typically involving generation plants, HV transport and HV/MV substations. Such segments have often been served through the use of ad hoc networks (mainly radio relays and in some cases fibre optic systems).

– Electric network supervision and alarms management (mainly in MV/LV substations):
  - Mono-directional (alarms + information) or bi-directional (alarms + information + activation);
  - Information transmitted;
  - Communications type – wireline, wireless or power line communications;
  - Bit rate, latency, others.
– Remote metering:
  - Power line communication, wireless.

Smart grids

Future grids are expected to integrate a virtually unlimited number of sensors and meters in the distribution segments, distribution energy resources (DER) sites and homes to support demand/ response, distributed generation and energy-aware applications. This will produce a huge amount of critical information for grid operation to be collected, exchanged and managed in a trustworthy way, requiring bidirectional flows among different layers. The first initiatives in such directions are the deployment of automated meter reading systems at the customers' sites, under the boost of lowering management costs and the push from government institutions. The meter provides a bidirectional communication channel:

– Control network;
– Metering network.

The Standardization Sector of the ITU (ITU-T) Study Group 15 has developed home networking specifications under the title of ITU-T G.hnem for smart electrical grid products. G.hnem is the new project titled "Home Networking Aspects of Energy Management". The main objective of this project is to define home network devices with low complexity for home automation, home control, electric vehicles and smart electrical grid applications. Among the applications of smart electrical grid that will benefit from the G.hnem are:

– Programs on demand response based on utilities through Internet broadband communications or through advanced metering infrastructure (AMI) systems;

– Remote repair to minimize costs;

– Support for systems on demand response in real time to compensate users according to their use;

– Flexible control of devices to reduce power consumption during peak periods of consumption.

The Focus Group on Smart Grid[29] collected and documented information and concepts that can be helpful to prepare recommendations on the smart electrical grid from the perspective of telecommunications. Upon completion of its mandate, the Focus Group had produced five documents. The Joint Coordination Activity on smart grid and residential network (SG & JCA- HN), successor of the Focus Group, forwarded these documents to all Study Groups and Thematic Groups and urged them to use these in preparing advice. Study Group 15 of ITU-T (Transport and Access) developed a number of Recommendations on electrical transmission lines to support the smart grid. Study Group 5 of the ITU-T (Environment and Climate Change) is also introducing a new question on the smart grid.

There are initiatives[30] that target to group energetic networks as electricity and gas networks.

In the area of business management, the development of technologies for creating new environments of Network Operation (including simulation tools and estimation states), the Active Demand Management and the Planning and Optimization of Operations, are included.

In the area of Platform Integration and Communication, the Focus Group on Smart Grid worked on the proceedings of acquiring and processing information in real time (with the difficulties of the huge volumes of information that will be generated and the criticality of their availability), the necessary infrastructure to management and recharging of electric vehicles and requirements of supervision and control of micro-grids. These are smart networks of distribution self-managed locally, so they can function both connected to the distribution network as isolated from it.

The Network Intelligent Devices will include new techniques of signals acquisition, the development of smart devices of energetic register and automation of network equipment.

The European Commission has done intensive work on the subject; there is a working group on this issue. The Smart Grids Task Force (SGTF) was set up by the European Commission (EC) at the end of 2009. The SGTF reached a consensus over the last two years on policy and regulatory directions for the deployment of Smart Grids. The SGTF has also issued key recommendations for standardization, consumer data privacy and security.

Based on these results, during 2011 the EC has adopted the "Communication on Smart Grids" initiative, which issued a mandate for smart grids standards to the European Standardization

[29] The Focus Group on Smart Grid was created in February 2010 and concluded its work in December 2011.

[30] As the Spanish Energos Project (led by the distribution of gas and electricity Union Fenosa) is a research project for the development of knowledge and technologies to advance the deployment of smart grid power distribution (Smart-Grid). It is within the National Strategic Consortia for Technical Research (CENIT) to boost innovation and technological development in key areas of society. The Centre for Industrial Technological Development (CDTI) subsidizes half the budget, amounting to 24.3 million euros.

Organization and created an Inventory of Smart Grid projects and lessons learned in the European Union[31].

In order to summarize the functionalities of smart grids, this document presents an extraction from "Definition, Expected Services, Functionalities and Benefits of Smart Grids" document:

A Enabling the network to integrate users with new requirements

1) Facilitate connections at all voltages/locations for all existing and future devices with smart grid solutions through the availability of technical data and additional grid information to:
   - simplify and reduce the cost of the connection process subject to maintain network integrity/safety;
   - facilitate an 'open platform' approach – close to 'plug & play';
   - make connection options transparent;
   - facilitate connection of new load types, particularly electrical vehicle EV;
   - ensure that the most efficient DER connection strategies can be pursued from a total system perspective.
2) Better use of the grid for users at all voltages/locations, including in renewable generators.
3) Registers of the technical capabilities[32] of connected users/devices with an improved network control system, to be used for network purposes (ancillary services) to increase a better control of energy production and utilization.
4) Updated performance data on continuity of supply and voltage quality to inform connected users and prospective users.

B Enhancing efficiency in day-to-day grid operation

1) Improved automated fault identification and optimal grid reconfiguration after faults reducing outage times:
   - Using dynamic protection and automation schemes with additional information where distributed generation is present;
   - Strengthening Distribution Management Systems of distribution grids.
2) Enhanced monitoring and control of power flows and voltages.
3) Enhanced monitoring and observability of network components down to low voltage levels, potentially using the smart metering infrastructure.
4) Improved monitoring of network assets to enhance efficiency in day-to-day network operation and maintenance (proactive, condition based, operation history based maintenance).
5) Identification of technical and non-technical losses through power flow analysis, network balances calculation and smart metering information.
6) Frequent information on actual active/reactive injections/withdrawals by generation and flexible consumption to system operator.

---

[31] http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm.

[32] Network users/devices, to actively participate/be managed in network's operations and energy management must be characterized by adequate technical capabilities. Considering the active control and demand-response of Distributed Energy Resources (i.e., generators, controllable loads and storage) some of the most relevant technical capabilities that have to be taken into account are: (i) Active – reactive power capabilities (ii) Dynamic response, (iii) Electric storage capacity in terms of energy and power. For example, referring to the renewable generators participation in the network voltage regulation or power flows control, the generator reactive power capability curve and the other capabilities aforementioned, are technical constraints that have to be managed.

C Ensuring network security, system control and quality of supply

1) Solutions to allow grid users and aggregators to participate in an ancillary services market to enhance network operation.

2) Improved operation schemes for voltage/current control taking into account ancillary services.

3) Solutions to allow intermittent generation sources to contribute to system security through automation and control.

4) System security assessment and management of remedies, including actions against terrorist attacks, cyber threats, actions during emergencies, exceptional weather events and force majeure events.

5) Improved monitoring of safety particularly in public areas during network operations[33].

6) Solutions for demand response for system security purposes in required response times.

D Better planning of future network investment

1) Better models of DG, storage, flexible loads (including EV), and the ancillary services provided by them for an improvement of infrastructure planning.

2) Improved asset management and replacement strategies by information on actual/forecasted network utilization.

3) Additional information on supply quality and consumption made available by smart metering infrastructure to support network investment planning.

E Improving market functioning and customer service

1) Solutions for participation of all connected generators in the electricity market.

2) Solutions for participation of VPPs in the electricity market, including access to the register of technical capabilities of connected users/devices.

3) Solutions for consumer participation in the electricity market, allowing market participants to offer:

- Time based energy pricing, dynamic energy pricing and critical peak pricing;
- Demand response/load control programs.

4) Grid solutions for EV recharging:

- Open platform grid infrastructure for EV recharge purposes accessible to all market players and customers;
- Smart control of the recharging process through load management functionalities of EV.

5) Improved industry systems for settlement, system balance, scheduling and forecasting and customer switching.

6) Grid support to intelligent home/facilities automation and smart devices by consumers.

7) Individual advance notice to grids users for planned interruptions.

8) Customer level reporting in event of interruptions (during, and after event).

6.1.2 Smart water management

Smart water management (SWM) promotes the sustainable consumption of water resources through coordinated water management, by the integration of ICTs products, solution and systems, to maximize the socioeconomic welfare of a society without compromising the environment. As it was

[33] Control of access to the equipment, detection of fault on overhead networks, protection of the contents of the buildings.

indicated before, SMW has applicability in many different sectors (for example industries, agriculture etc.).

From a general point of view, SMW has two main functions:

– Sensing: This involves the use of Internet of things (IoT) technology for sensing and intelligent monitoring to achieve business related data and centralized management such as water quality monitoring, ship scheduling in rivers, etc.;
– Intelligent scheduling: Water resource could be sensed by the IoT integrated system to make decisions on flood control and drought prevention; intelligent management of water environment; and intelligent management of water distributions.

Steps have been made to improve the capabilities of the information technology needed for flood and drought decision, water environment treatment, and water resources management.

In particular, smart metering technologies will play an important role in the real-time measurement of water consumption, identifying leaks at the consumer level and raising more awareness to consumers on water consumption. With the development of sensors of active outlet, the web of semantic sensors, the geoweb, the geographic modelling in 3D, and mobile communications, this field has great potential for water authorities.

Smart water management in cities[34]

Today's integrated global economy and innovations in telecommunications, have created a massive opportunity in utilities to assist in addressing water management challenges within cities and urban areas.

The recognition of the challenges in the water sector have created intelligent tools which use ICTs to alleviate global water issues. These technologies create tremendous opportunities to improve the productivity and efficiency within the water sector with an aim to generate sustainability of the resource. ICTs permit the continuous monitoring of water resources, providing real time monitoring and measuring, making improvements in modelling and by extension problems diagnosis, enabling proper maintenance and optimization of all aspects of the water network.

An opportunity for more intelligent means to manage and protect the planet's water resources has led to the development of smart water management.

Smart water management increases the efficiency of the water sector while ensuring its economic sustainability since municipalities and water utilities are better able to recover costs from non-revenue water and are better able to detect illegal connections.

Smart water management tools fall into the main areas listed below. However it should be noted that the examples provided are not confined only to the areas represented but may overlap several areas as seen in Figure51.

1) Data acquisition & integration (e.g., sensor networks, smart pipes, smart meters etc.);
2) Data dissemination (e.g., radio transmitters, Wi-Fi, Internet etc.);
3) Modelling and analytics (e.g., GIS, MikeURBAN, Aquacycle, AISUWRS, and UGROW etc.);
4) Data processing and storage (e.g., SaaS, cloud computing, etc.);
5) Management and control (e.g., SCADA, optimization tools, etc.);
6) Visualization and decision support (e.g., web-based communication and information systems tools etc.).

[34] Extracted from the "Technical Report on Smart Water Management for Smart Sustainable Cities" [ITU-T TR SWM].

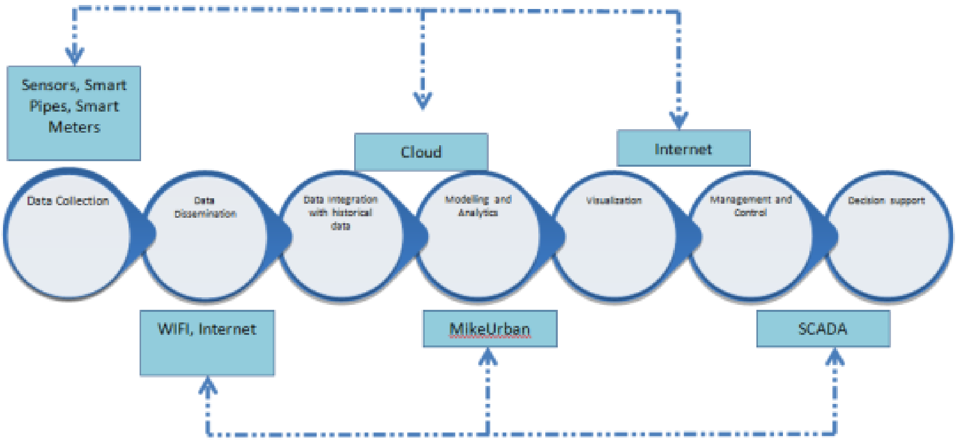


Figure 51 – Schematic representation of smart water management technologies and tools

Source: McIntosh 2014.

Smart water management technologies

Smart water management technologies are already currently applied to many different areas of water management (Figure 52). These technologies when applied to cities, help acquire reliable data and enhancement to operations and safeguard proper decision making. In this context, many of these innovative ICT tools have been developed to shape next-generation urban water infrastructure systems to improve performance, increase efficiency, reduce costs, decrease redundancy, as well as ensure negligible environmental impacts.

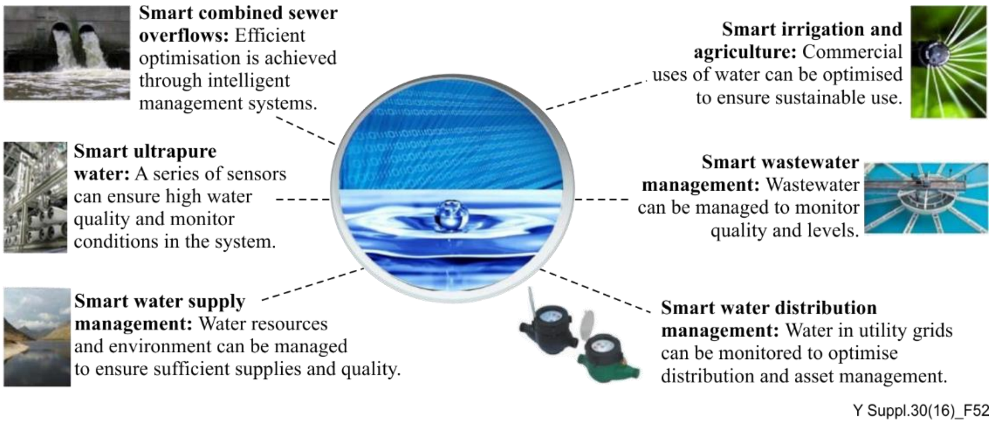


Figure 52 – Current implementation of smart water management technologies and tools

Source: Hauser 2012.

Smart pipes and sensor networks[35]

Smart pipes incorporates multi-functional sensors that can sense strain, temperature and pressure anomalies, as well as measure water flow and quality during service, to provide operators with continuous monitoring and inspection features assuring safer water supply distribution. Connecting smart pipes with a wireless processor and antenna enables data to be transferred directly to a command centre, equipping water managers with the tools to detect and locate potential leaks in real time.

---

[35] For more information: http://www.isws.illinois.edu/gws/sensor/smartpipe/.

Sensors can also be incorporated to optimize the water used in irrigation to measure parameters such as: air temperature, air humidity, soil temperature, soil moisture, leaf wetness, atmospheric pressure, solar radiation, trunk/stem/fruit diameter, wind speed/direction, and rainfall. The range of application within cities can be from park irrigation or commercial irrigation, allowing for better management and more accurate allocation of water resources between sectors.

Wireless sensor networks provide the technology for cities to more accurately monitor their water supply systems intricately using different parameters. Sensors are multifunctional for instance they have the ability to monitor soil moisture and can therefore detect leaks since if the ground is absorbing water there may be a pipe leak. Many ICT companies are developing a wide range of sensors specifically for water networks.

The major tasks for smart sensor networks in water quality monitoring are to:

– Identify and characterize changes existing or emerging trends in surface water quality over time.
– Gather information to design or assess specific pollution prevention or remediation programs or to provide information in a timely manner to allow quick respond to emergencies, such as spills and sewage leakages.
– Determine whether program goals – such as compliance with pollution regulations or implementation of effective pollution control actions – are being met.

Integrating smart pipes and sensors within the urban system, leads to many possibilities such as the detection of flow rate, pipe pressure, stagnant points, slow-flow sections, pipe leakage, backflow, and water quality; necessary data lacking in current networks.

Smart metering

Smart meters are electronic devices which have advanced metering infrastructure (AMI) that would support the real time measuring of electric, heat, gas, and water consumption. These devices are rapidly evolving in response to market forces and governmental regulations. In the case of water consumption, these smart meters typically consist of an embedded controller which interfaces with a metering sensor, a wireless transmitter as well as display and communications extension (see Figure 53). The meters are connected to a data logger which allows for the continuous monitoring of water consumption of a building, a business or a home. The innovation of smart meters, permit two-way communication between the meter and a central system by transmitting data which can be done through different channels (power line, Internet, or telephone).

Smart meters typically collect consumption data, transmitting this data to a Gateway which interfaces with the local area network (LAN), home area network (HAN) and a wide area network (WAN). The LAN consists of the metrology or measurement function of the meter, while the HAN is connected to the customers' network. Moreover, the display functions of the HAN easily allows accessibility to consumption data through a user friendly interface with possibilities for customers to compare and track their water consumption. The WAN is managed by the utilities and allows them to track, monitor and bill consumption.

The deployment of smart meters within an urban infrastructure enables remote accessibility of consumption data which improves meter reading and billing, detection of leaks, illegal connections and tamper alerts, as well as enhances the determination of peak demand. Customer and provider relationships are improved through increased communication and consumers are also equipped to options to change payment methods (e.g., prepaid or post-paid).

Moreover smart metering allows the water utilities to provide clear, water consumption information which can help customers to track and control their water usage and thereby see immediate savings on their bills enabling better distribution network and consumption planning due to the real-time monitoring capabilities.

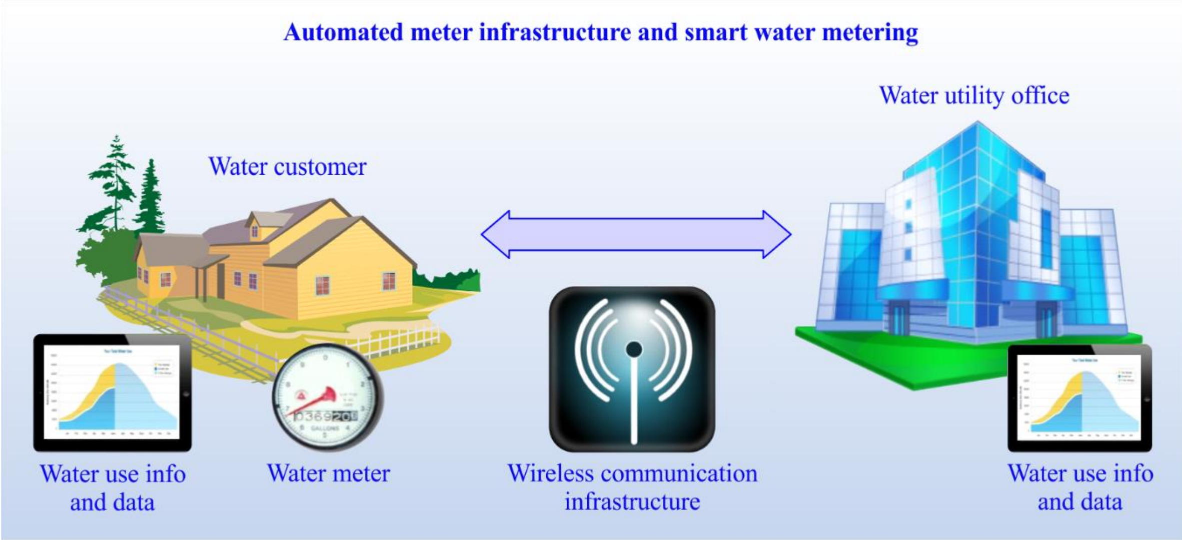


Figure 53 – Smart meter technologies

Source: http://www.allianceforwaterefficiency.org/smart-meter-introduction.aspx.

GIS integration can improve data management especially of large volume projects. GIS provides high quality result display especially in hydraulic simulation modelling and provides additional analysis useful for decision support. GIS allows visualization and analysis of data about water resources/issues and human activity by linking geographic information with descriptive information. This is highly valuable to the urban water management in assessing water quality and day to day operations on a local and regional scale. However, its benefits are not limited to urban issues such flooding that can also be mitigated by the use of GIS by providing information on critical areas which are at a risk of flooding. This is necessary in developing hazard maps as well as development of emergency response planning. GIS utilization offers more robust analysis, increased efficiency and reduced costs.

By integrating information from resource satellites, GIS can cover large river basins which some cities occupy. Combined with local rainfall patterns, meteorological and hydrological data, as well as drainage systems, GIS improve urban storm water management by strengthening drainage management and enhance rainwater reuse. This helps to reduce the prevalence of urban flooding which is increasing in cities since the development of infrastructure in cities has created large expanses of impermeable earth.

Supervisory control and data management (SCADA) systems when incorporated in water management systems are computer-controlled systems which contain large communication systems that permit the monitoring and control of water treatment and distribution as well as wastewater collection and treatment. The system allows for supervision through data acquisition and management with the ability to process and send commands within the system. The communication system may involve radio, direct wired connections or telemetry. Its dynamic network can allow for weather forecast model inputs as well as hydraulic model system optimization (see Figure 54).

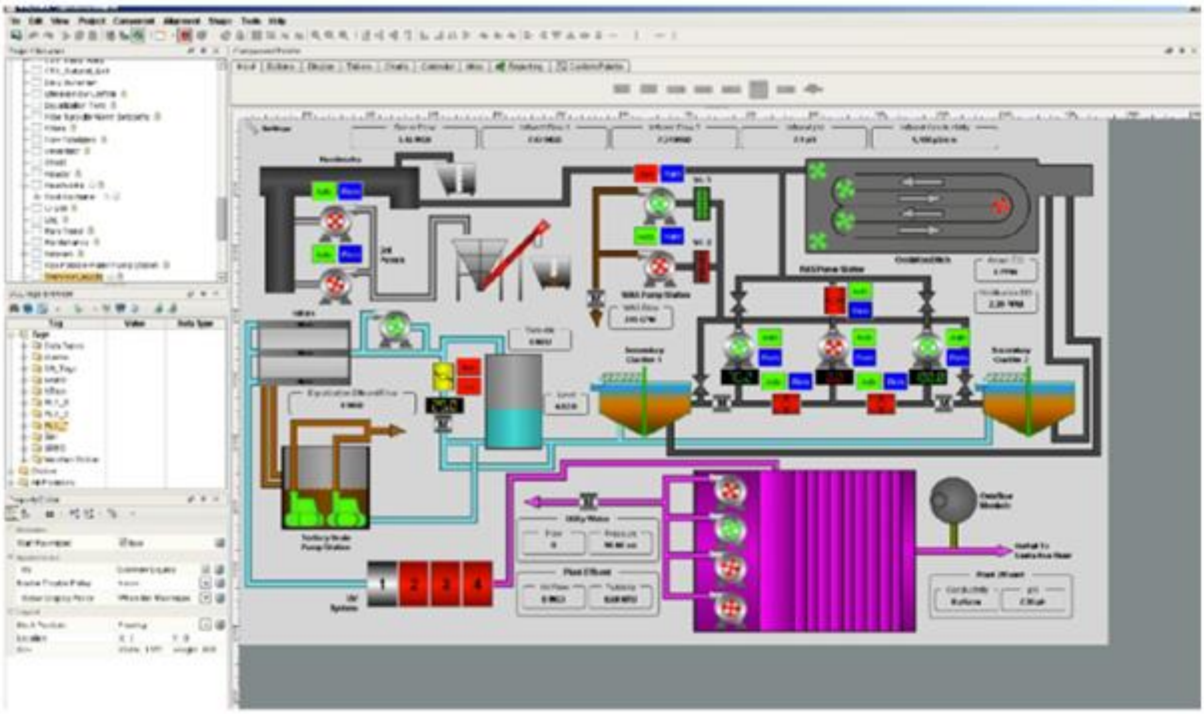


Figure 54 – SCADA software the Western Municipal Water District (WMWD), California

Source: http://www.automationworld.com/sites/default/files/styles/lightbox/public/field/image/120723scada_web.png?itok=IlXV7wPd.

Utilities have been using SCADA systems for higher-level applications; such as determining times of peak water use, identifying potential system leaks, setting billing rates etc. SCADA systems have even reduced the operating costs of utilities and have improved the delivery of water distribution to residential areas, businesses and industry. The monitoring aspect of SCADA systems also helps utilities to protect their infrastructure and prevent severe degradation. In 2013, implementation of SCADA has seen 30% savings on energy used to manage water systems, 20% reduction on water loss and 20% reduction in disruption. Applying SCADA in an urban system can also see the enhancement of disaster preparedness through storm water management or support the remote operation and monitoring of major dams and weirs.

Models, optimization tools and decision support

Model based water management has evolved over the years to improve the quality and quantity of global water supply through comprehensive modelling applications. These modelling software incorporate to some extent processes observed in the real world (through equations, algorithms and scenarios) and contain various data reporting and visualization tools useful for interpreting results from water distribution piping systems, water quality monitoring data, wastewater management systems, decision support etc. Urban water managers have used many models such as MikeURBAN, Aquacycle, AISUWRS, and UGROW among others.

Optimization tools aim at finding the technical, environmental and financial best solution from models, therefore "optimization tools and principles have made it possible to develop prescriptive models for optimal management of large scale water resources systems, incorporating ubiquitous uncertainties in the prediction of natural processes and the economic impacts" (Datta and Harikrishna). By incorporating optimization tools, decision making in the planning, design and operation water resource systems can be achieved in an efficient and effective manner.

Models, optimization tools and decision support for network management urban water and wastewater are able to calculate and forecast consumption, reduce costs through the optimization of operations, plan and evaluate strategies and conduct vulnerability studies.

Web-based communication and information system tools

Information and knowledge management are increasingly recognized as important features in effective and efficient work in the water sector (Dondeynaz et al. 2009). The main problem is that more data within the water sector are large, complex, unstructured and fragmented. However web-based interfaces and online platforms provides a solution for proper management, display, and retrieval of the relevant information necessary for water managers/operators, urban planners, governments and the public alike.

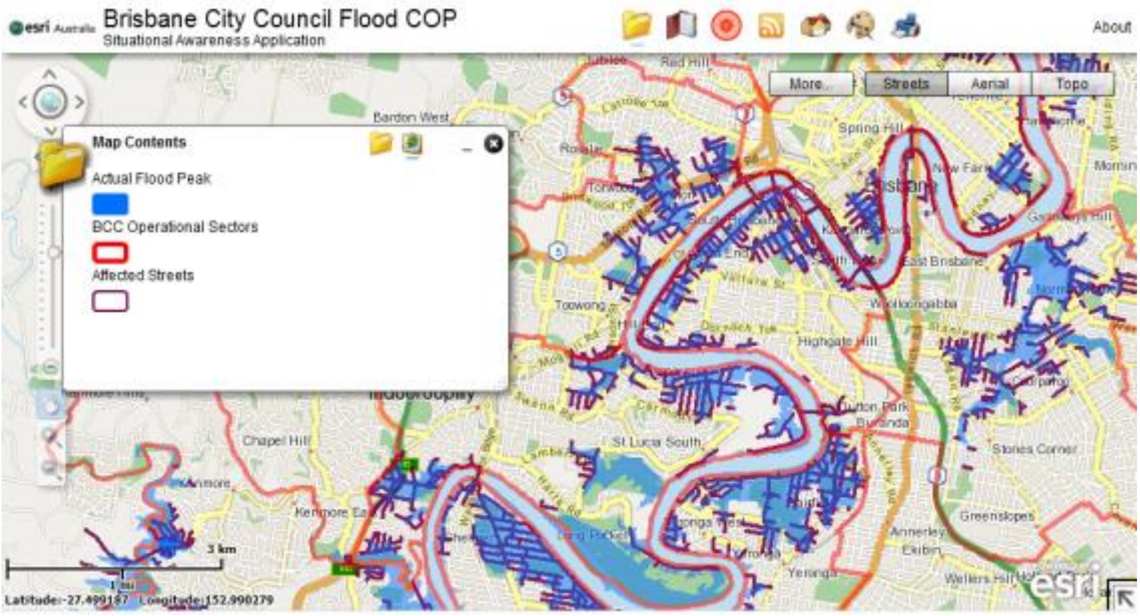


Figure 55 – The Brisbane City web based flood map

Source: http://www.sweetmaps.com/blog/wp-content/uploads/2011/01/BCC_esri_flood_map.jpg.

Web-based servers offer access to integrated information from heterogeneous data sources, as well as the innovative tools for analysis and assessment of a broad area such as climate change, water scarcity, human health, sanitation and urbanization necessary for proper urban water management. Integration of such web based communication tools using open communication standards allow a range of stakeholders to connect to the system, to use or add to its resources.

Information and communication systems which are composed of two parts can enable both the general public and administrators to access relevant information; allowing for transparency and visibility of current water related activities by the specialized users (such as water managers, municipalities, governments), building trust and better public/stakeholder involvement. An intuitive and user friendly interface, means that there can be ease of data acquisition and dissemination especially for the public.

Web-based information and communication system tools for information acquisition have been successfully utilized by governments and municipalities to deliver high quality water information to the public as well as provide flood warnings (see example of web-based flood map in Figure 55). Such systems can allow urban water managers access to relevant information such as rainfall, storage, distribution while providing necessary information to the public.

6.2 Transportation

Intelligent transport systems (ITS) may be defined as systems utilizing a combination of computers, communications, positioning and automation technologies to use available data to improve the safety, management and efficiency of terrestrial transport, and to reduce environmental impact[36].

ITS incorporate four essential components, as illustrated in Figure 56:

– Vehicles, which can be located, identified, assessed and controlled using ITS.

– Road users, who employ ITS, for instance, for navigation, travel information and their monitoring capabilities.

– Infrastructure, for which ITS can provide monitoring, detection, response, control, road management and administration functions.

– Communications networks, to enable wireless transactions amongst vehicles and transport users.

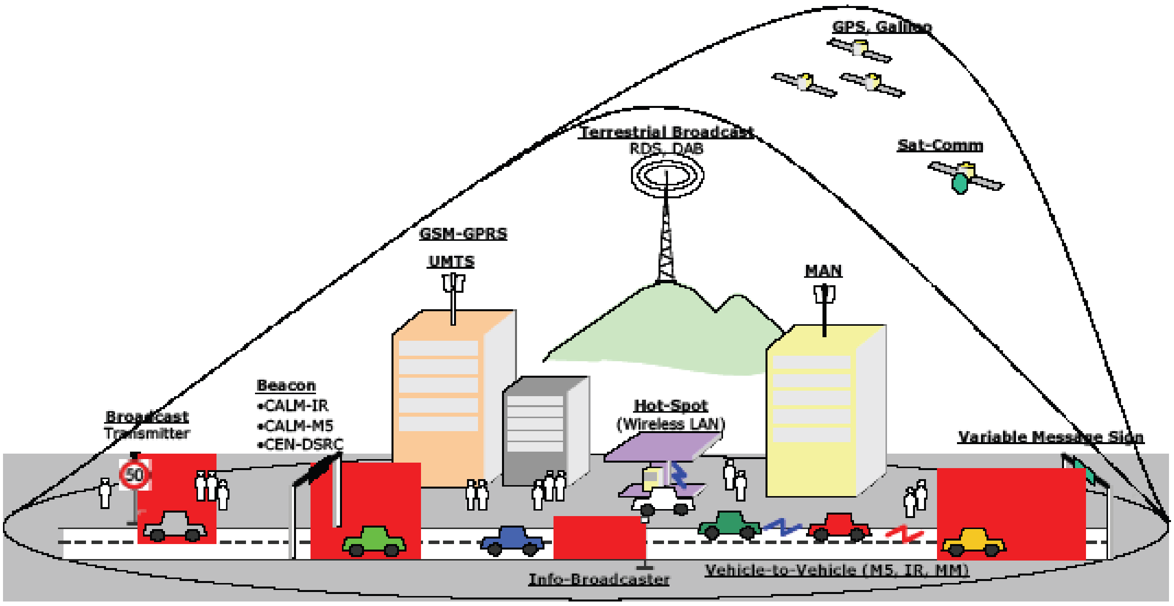


Figure 56 – Intelligent transport systems (ITS)

Source: The CALM Forum/ISO TC 204, reprinted in ITU-R Land Mobile Handbook, Vol 4: Intelligent Transport Systems (2006), available at: www.itu.int/pub/R-HDB-49-2006/en.

Intelligent transport systems include telematics and all types of communications in vehicles, between vehicles (e.g., car-to-car), and between vehicles and fixed locations (e.g., car-to-infrastructure). However, ITS are not restricted to road transport - they also include the use of ICT for rail, water and air transport, including navigation systems[37].

There are currently the following projects related to automotive ITS:

A) Continuous air interface long and medium range (CALM) provides continuous communications between a vehicle and the roadside using a variety of communication media, including cellular, 5 GHz, 63 GHz and infra-red links. CALM will provide a range of applications, including vehicle safety and information, as well as entertainment for driver and passengers.

---

36 "Intelligent Transport Systems and CALM" ITU-T Technology Watch Report 1 October 2007. https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000010003PDFE.pdf.

37 European Telecommunications Standards Institute http://www.etsi.org/technologies-clusters/technologies/intelligent-transport.

The aim of CALM is to provide wide area communications to support ITS applications that work equally well on a variety of different network platforms, including second generation (2G) mobile (e.g., GSM/GPRS), 3G (IMT-2000 e.g., W-CDMA/CDMA 1x EV-DO) 4G (IMT-Advanced), as well as satellite, microwave, millimetre wave, infrared, WiMAX and short-range technologies like WiFi.

The main characteristics of CALM are:

– It allows for continuous (or quasi-continuous) communications, in three main modes of operation: vehicle-infrastructure; vehicle-vehicle; and infrastructure-infrastructure.

– Inter-operability and seamless handover between networks and applications.

– In its initial specification, CALM used Internet protocol version 6 (IPv6) exclusively. However, in order to meet the requirement for very fast short communications in time and in critical situations, such as C2C applications (e.g., collision avoidance), a non-IP solution with lower processing overhead and lower latency may be more suitable, and this is incorporated in the new specification (CALM Fast).

– It is the single global architecture which is compatible with existing ITS standards (e.g., DSRC) and wireless standards (e.g., GSM/GPRS) and which is expected to conform to future ones too.

– It provides platform-independent support for multiple radio communication network platforms. For instance, the basic CALM system architecture (ISO 27217) foresees support for 10 main categories of network, and 22 different sub-categories each of which would need a different service access protocol (SAP).

Figure 57 shows the new (2007) merged CALM architecture. The likely future direction seems to be a flexible CALM architecture and a division of labour among different organizations.

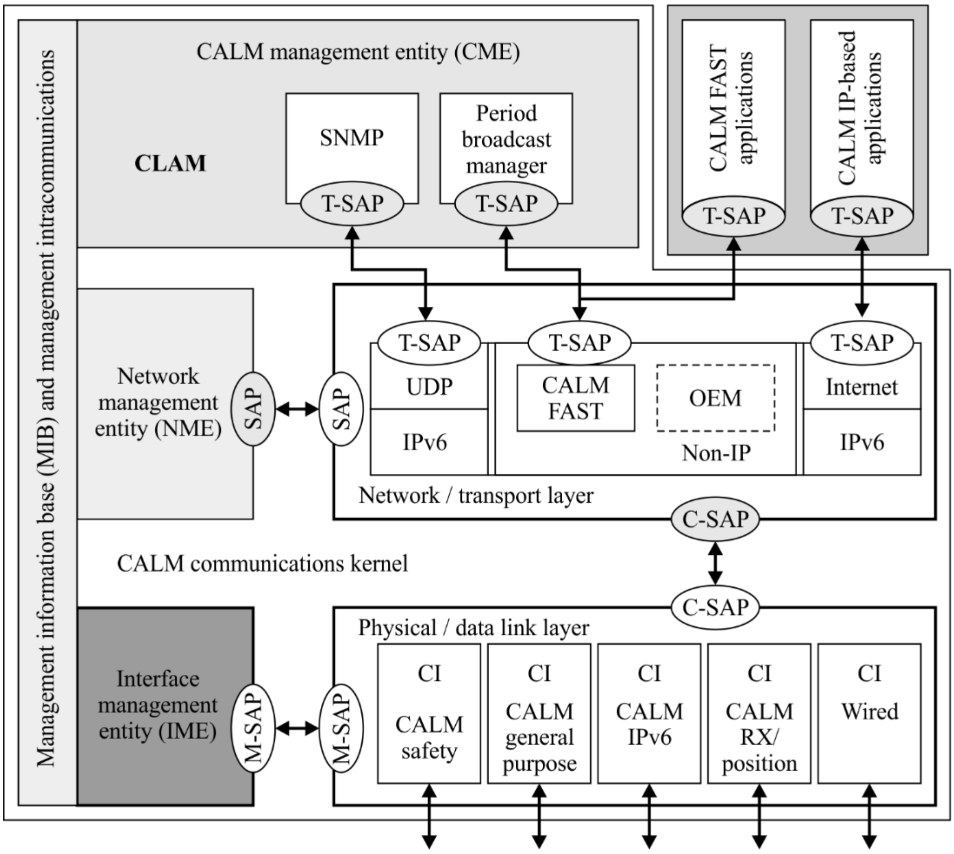


Figure 57 – CALM architecture

Source: ISO TC 204 – See http://www.itu.int/dms_pub/itu-t/oth/06/05/T06050000130001PDFE.pdf.

CALM is intended to provide a standardized set of air interface protocols for ITS applications, using multiple network platforms. These include:

– 2G mobile systems, including GSM/GPRS, which are the most widely deployed mobile network worldwide.
– 3G (IMT-2000) mobile systems, including W-CDMA and CDMA 1x EVDO.
– Infrared.
– Wireless LAN systems, including the IEEE 802.11 series.
– Millimetre wave systems, including radar.
– DSRC, including national and regional implementations
– Wireless MAN systems, including WiMAX.
– Broadcast signals, including GPS and digital audio broadcasting (DAB).
– Personal area networks (PAN) including UWB and Bluetooth.
– Fixed-line networks (for infrastructure to infrastructure communications), including Fibre and Ethernet.

Figure 58 shows some scenarios of application for vehicle safety and information.

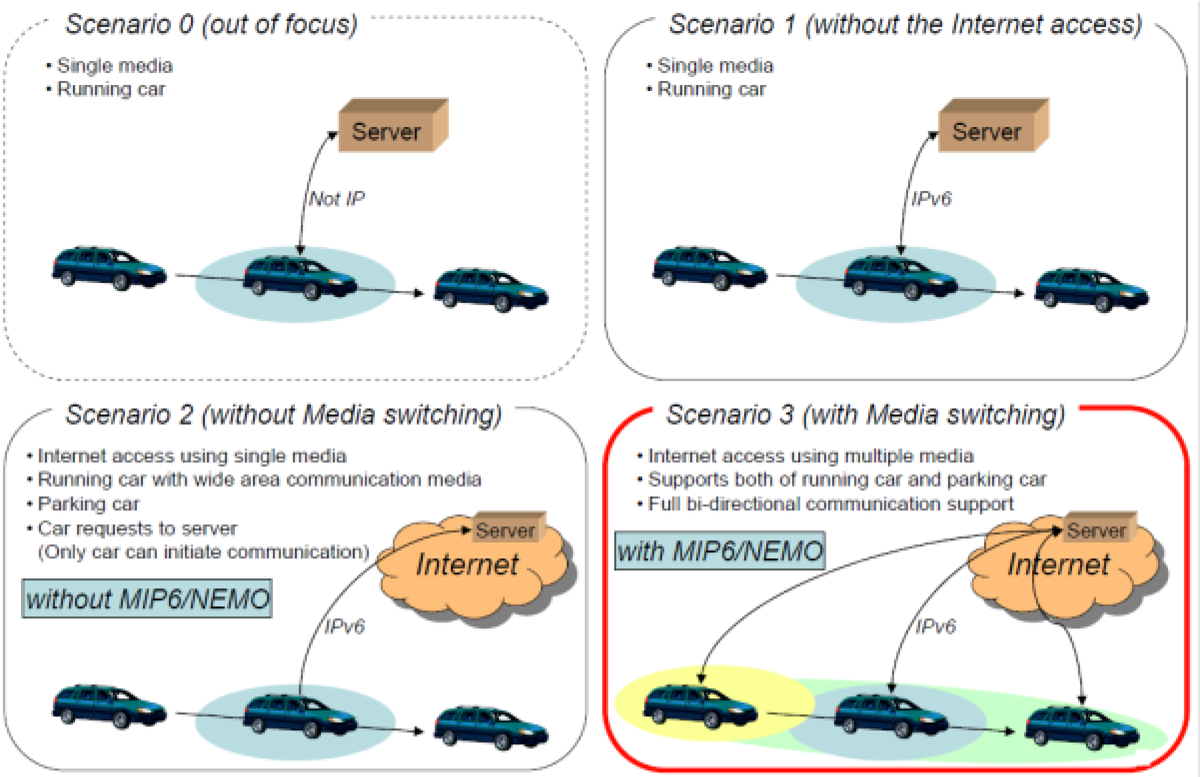


Figure 58 – CALM scenarios of application for vehicle safety and information

Figure 59 shows the three physical configurations for scenario 3: Internet access using multiple media with full bi-directional communication support.

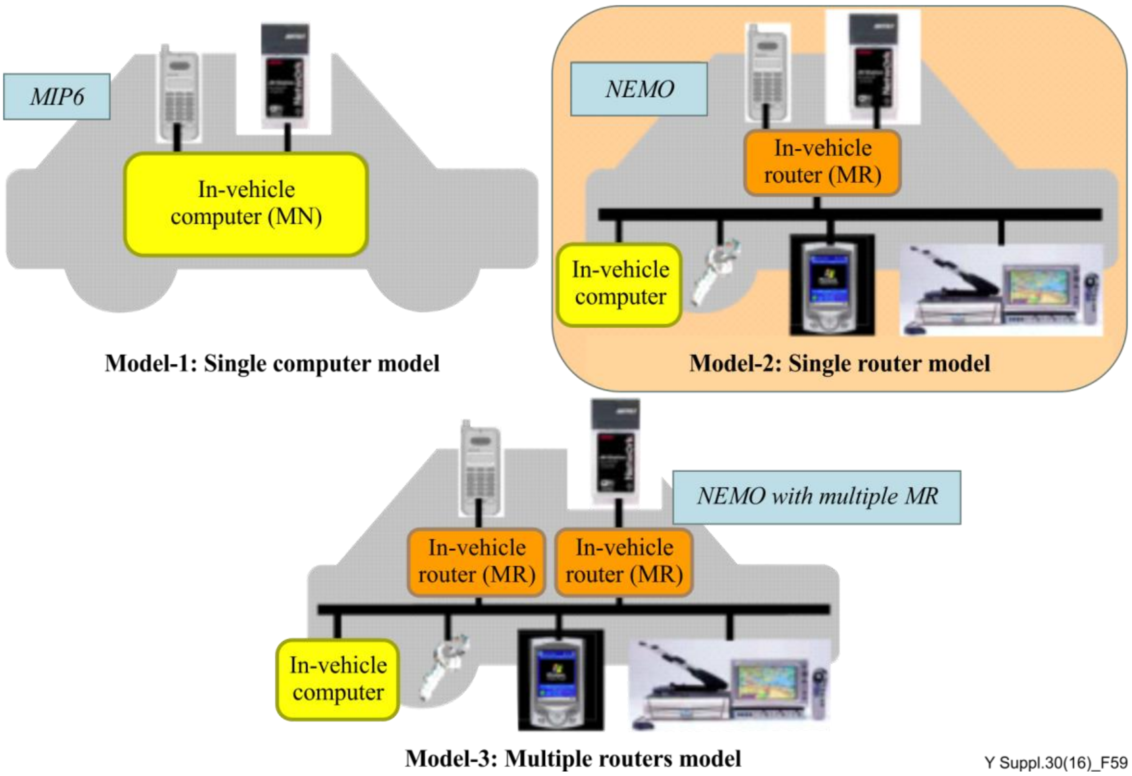


Figure 59 – Three physical configurations for scenario 3

Figure 60 shows the summary description of the entities defined in the CALM architecture and service access protocol (SAP).

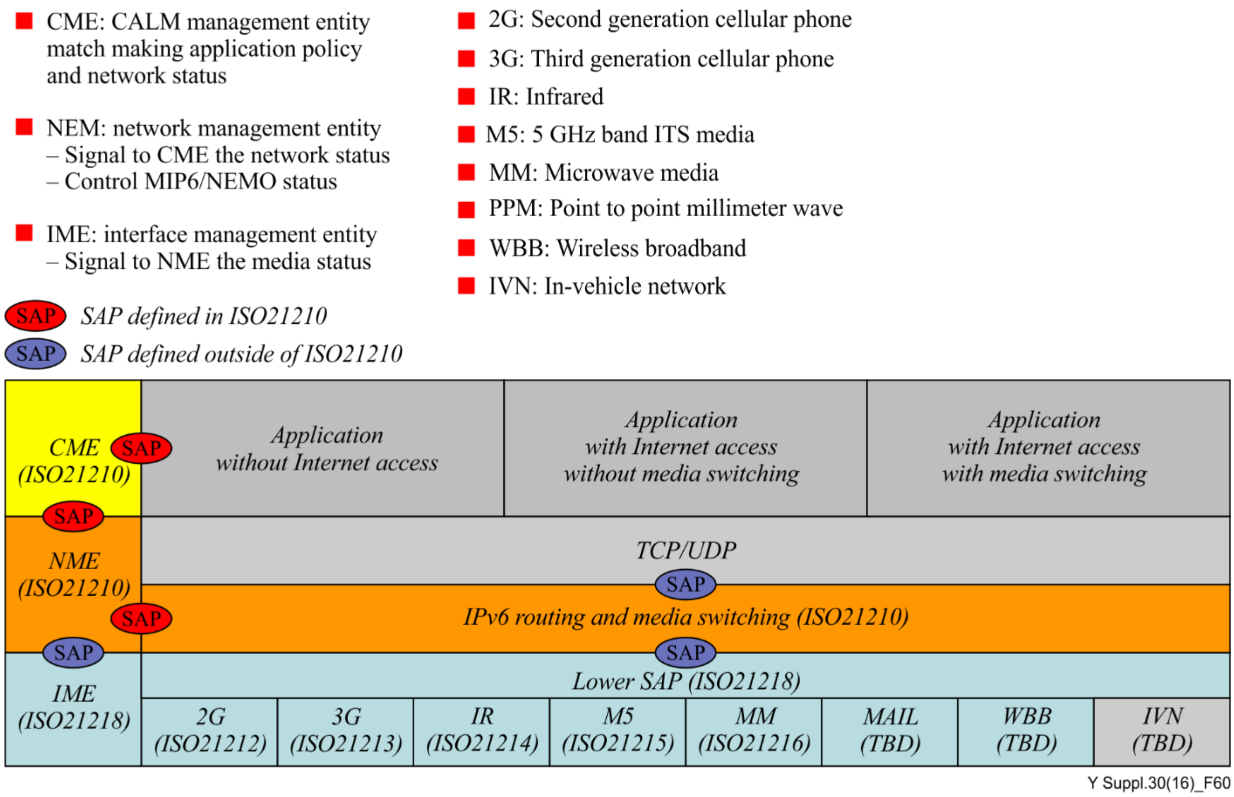


Figure 60 – CALM architecture and SAPs of networks part

B) Dedicated short-range communications (DSRC) provides communications between the vehicle and the roadside in specific locations (for example toll plazas). Applications such as electronic fee collection (EFC) will operate over DSRC. Figure 61 shows the interaction of DSRC and CALM.

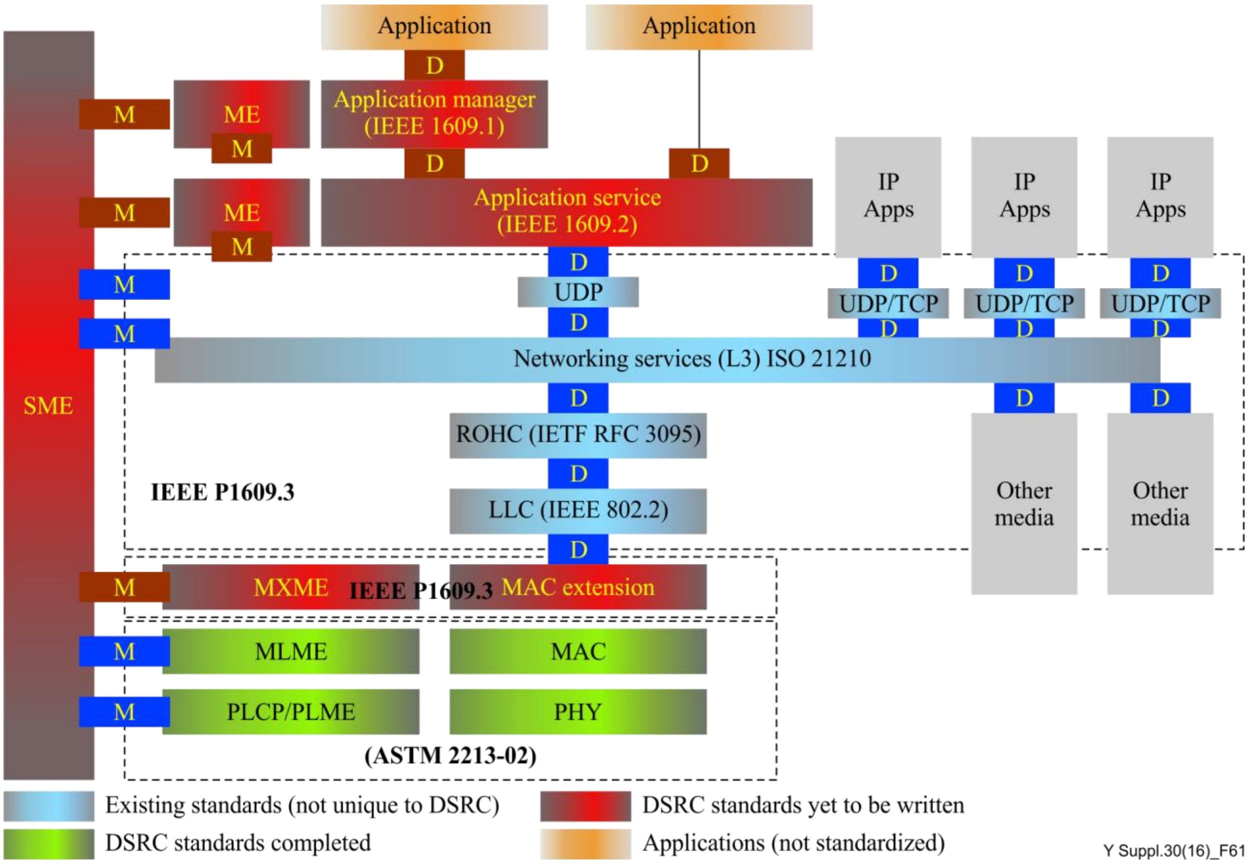


Figure 61 – ISO TC204 WG16 CALM M5 architecture

C) Wireless multiservice payment system for vehicles

Toll payment collection on highways, as shown in Figure 62, is one of the applications of intelligent transport system (ITS) technology. At the beginning of the 1990s, the electronic fee collection (EFC) tele-toll systems were introduced in Europe by various highway operators. These systems are currently generalized all over Europe. The advantage of electronic payment is the fact that the vehicle does not need to stop, thus avoiding traffic jams, besides the fact that it is not necessary to carry money. In this way, it is possible to provide greater customer satisfaction and a reduction of human resource costs to the operator, among other advantages.

Typically, a tele-toll system is based on short range microwave technology designed for the purpose, known as dedicated short range communications. However, for the majority of European highway concession holders the systems are incompatible with each other, given that the initial standard only served as a recommendation for the system. Hence each operator installs it in accordance with the application sought. The majority of these systems are based on the low data rate (LDR) sub-standard, given that this was the first standard created. The incompatibility raises some difficulties for car drivers, who (sometimes inside the same area), have to affix several identifiers in their vehicle if they wish to use various systems. With the increase in traffic on European roads, the problem of interoperability between country systems/operators takes on greater importance. With a view to resolving this problem, the medium data rate (MDR) sub-standard was devised, aiming at providing interoperability between countries and systems. Nowadays, DSRC technology is not used exclusively for the electronic payment of tolls, for it is starting to have other applications, such as payment at parking lots and fuel stations, or even simply for controlling the access of vehicles. This system implies the need for toll barriers (access points), where the vehicle makes the transactions.

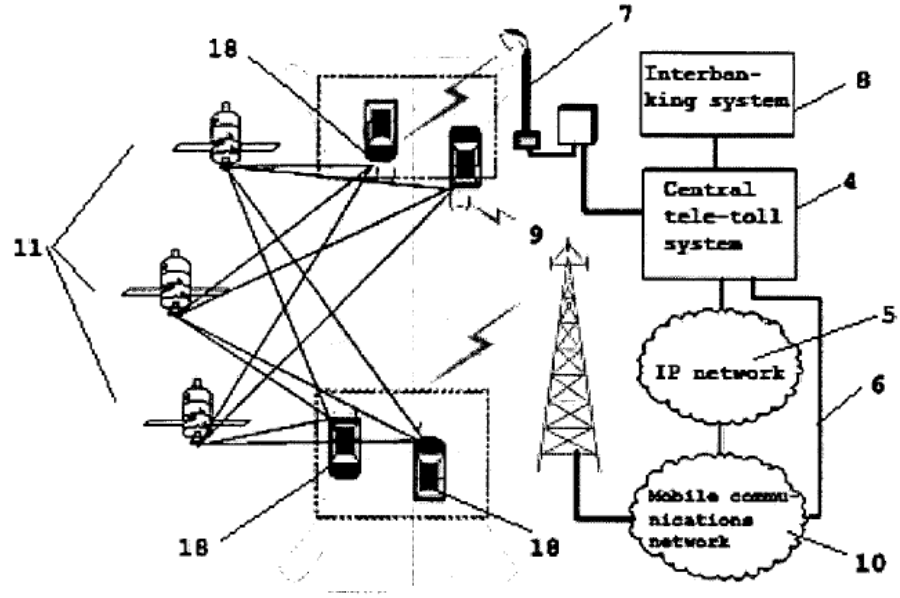


Figure 62 – Diagram of the operation of the toll payment systems on highways

Source: European Patent Application EP 1944736 A1.

Communication through short range radio based on microwaves (9) is regulated by the DSRC standard, which is currently used in tele-toll systems (4). There are three sub-standards in the DSRC, which are LDR, MDR and high data rate (HDR). LDR merely contains recommendations, having no obligatory character. On the other hand, MDR, was developed in order to guarantee greater interoperability between systems. HDR was devised to permit communication between vehicles. The MDR sub-standard is the one adopted in this invention, consisting of three layers which have a message/protocol stack specific for carrying out transactions.

The DSRC system mainly consists, in terms of radio, of two units: the road side unit (RSU) and the on board unit (OBU). The RSU is placed at the tollgate, being responsible for starting and ending the communication with the OBU, in order to carry out the transaction. Of the two units, it can be said that the RSU is fully active, since it is always connected and is the only one which transmits a carrier, so as to provide communication. This carrier is also used by the OBU so as to enable it to communicate, by reflection, with the RSU. The OBU is the equipment placed inside the vehicle in order to permit its identification. This module only has to generate a sub-carrier, which modulates the carrier received from the RSU, reflecting it back to the RSU. The OBU is passive, given that it does not generate a carrier to communicate with the RSU. Furthermore, the OBU is only active when it detects the RSU carrier, its consumption thus being minimised.

The use of the MDR standard makes it possible for the communication between the OBU and the RSU to be established through microwaves or infrareds. Figure 63 shows a schematic representation of the module installed on board the motor vehicle and its links to the various technologies available for operating the system.

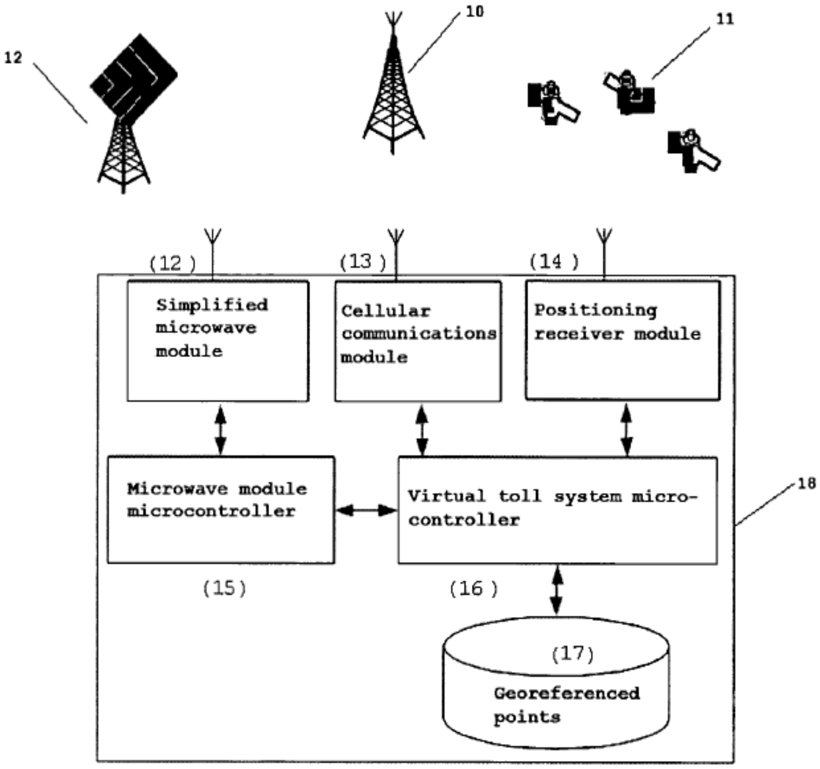


FIG. 2

Figure 63 – OBU and different technologies

Source: European Patent Application EP 1944736 A1.

These technological projects form a part of wider initiatives on matters such as road safety (for example the European Commission's eSafety initiative) and road tolling.

The goal of intelligent transportation systems) is to improve the effectiveness, efficiency, and safety of the transportation system. Effective deployment of ITS technologies depends in part on the knowledge of which technologies will most effectively address the issues of congestion and safety. Thus, it is important to understand the benefits of both existing and emerging technologies. Based on documented experience locally and throughout the country, ITS deployments in urban areas have the potential to offer the following benefits[38]:

- Arterial management systems can potentially reduce delays between 5% and 40% with the implementation of advanced control systems and traveler information dissemination.
- Freeway management systems can reduce the occurrence of crashes by up to 40%, increase capacity, and decrease overall travel times by up to 60%.
- Freight management systems reduce costs to motor carriers by 35% with the implementation of the commercial vehicle information systems and networks.
- Transit management systems may reduce travel times by up to 50% and increased reliability by 35% with automatic vehicle location and transit signal priority implementation.
- Incident management systems potentially reduce incident duration by 40% and offer numerous other benefits, such as increased public support for DOT activities and goodwill.

[38] "Benefits of Intelligent Transportation Systems Technologies in Urban Areas: A Literature Review" Portland State University http://www.its.pdx.edu/upload_docs/1248894206QpPC5zVqkd.pdf.

Besides ITU and European Telecommunications Standards Institute (ETSI), there are works from other institutions, thus IEEE has an organization named "IEEE Intelligent Transportation Systems Society". In the same way a helpful resource was the National ITS Benefits Database available at www.benefitcost.its.dot.gov.

6.3 Healthcare

Healthcare delivery can benefit from a connected approach, with electronic patient records (EPR) available to all medical services. This will enable public health professionals and clinicians to collaboratively access information in a secure way, at any time, from anywhere and from any device.

In many cases, telemedicine solutions, connected through broadband, wireless or satellite, can prove vital in situations where the infrastructure or specific contingencies do not allow for the physical presence of a specialist – such as natural disasters or remote geographical locations.

An ageing population needs traditional care, but also assisted living and health monitoring services to enable independence at home. This can be achieved through the utilization of sensors and devices connected to health operators through broadband, wireless and data analytics, and crucially, the deployment of privacy, identification and security systems.

The new telemedicine services, such as online medical consultations, improved emergency care and portable devices that allow monitoring the health status of people with chronic diseases and disabilities, can provide a freedom of movement which was previously unknown.

6.3.1 M2M use cases: e-health[39]

Figure 64 shows an overview of e-health M2M use cases written in this deliverable. There are various kinds of sensors near patients and their sensors send data to M2M Platform. In e-health use cases, caregiver provides care services supported by medical institutions using vital data and related information on M2M platform.

[39] Focus Group on Machine-To-Machine Service Layer M2M-I-196.

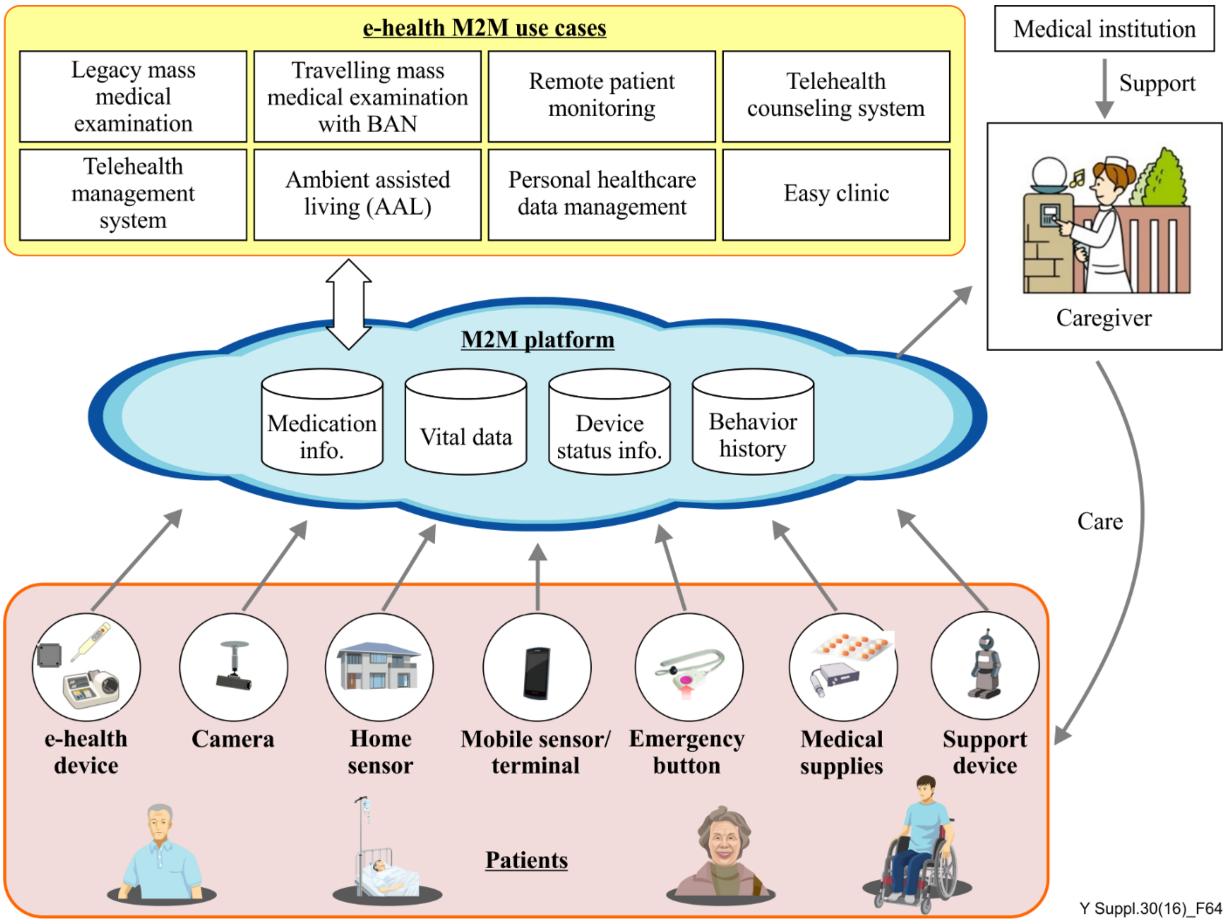


Figure 64 – Overview of e-health M2M use cases

6.4 Public safety and emergency

The power provided by the ICT infrastructure to public safety is beyond doubt. However a city highly dependent on all aspects of technology, has risks of sabotage that can disable much of their public services and good performance in general, so public safety must also ensure the continuity of the technological features using a good protection to the ICT infrastructure.

Public Safety is one of the key issues of a city. ICT facilities should include:

– City safety system combined with environmental monitoring, road monitoring, perimeter security, product safety and access control, and other functions.

– Cloud-based large-scale data storage, retrieval, intelligent video analysis, biometric technology, integrated platform for data intelligent analysis, etc.

– Increased bandwidth to support a wide range of applications of security. The smart city safety system builds a network of security, helping security officers avoid misjudgements, while providing a scientific and reliable method for security.

Two important systems for public safety: Geo-location systems of cell phones and the system of national alert using cell broadcast are shown in Figure 65. Both systems are interconnected and managed by the centralized emergency centre.

It's important to note that these types of solutions, requires not only ICT infrastructure, smart network and sensors (e.g., surveillance cameras) but also the participation of public/private organizations involved in emergency tasks, such as firemen, police, health professionals, etc. with established procedures to attend emergencies.

Centralized emergency centre

Quickly reaching the right place where an accident, fire or a crime has occurred or is occurring, is vital to save lives and minimize damage. Therefore the emergency centres need to quickly obtain the exact location where the event is occurring and other key information in order to facilitate swift responses.

One of the main objectives of an emergency centre is to reduce the response time to a minimum, as a minute lost to reach the exact location of the emergency can cost lives.

A caller location system needs an emergency centre that receives and centralizes all calls. This brings the following benefits:

a) Increases personal safety of citizens and reduces crime.

b) Allows better coordination of emergency response tasks.

c) Brings speed and efficiency to the work of police, fire and ambulance.

d) Significantly reduces the incidence of false calls.

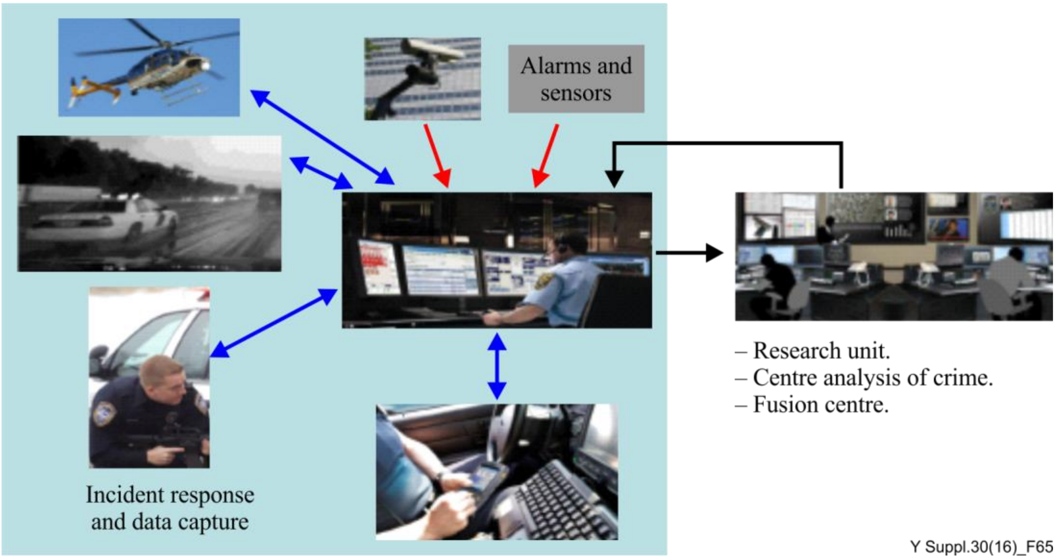


Figure 65 – Flow information of public safety

Components that will be installed in the emergency care centres (Figure 66) are as follows:

– Core switching with technology "Voice over IP" (VoIP) with automatic call distribution.

– Computer aided dispatch.

– GIS server.

– Call recording equipment

– Data base for location of fixed phones.

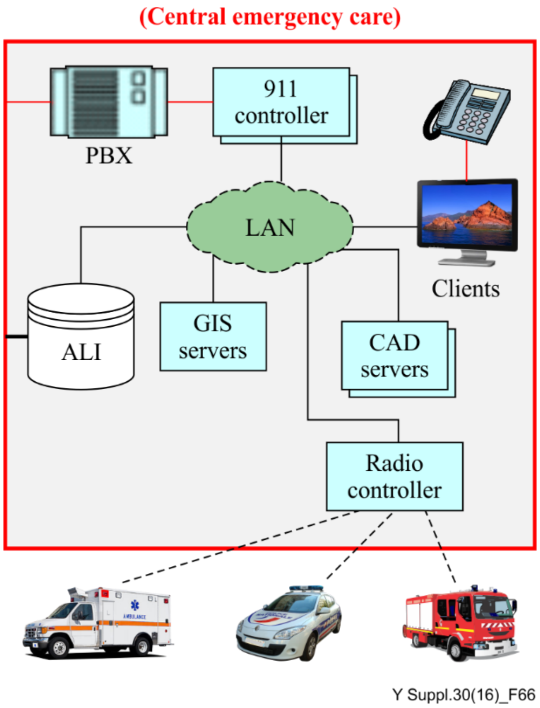


Figure 66 – Emergency network

Location of emergency calls

The solution needs a location platform, as is shown in Figure 67:

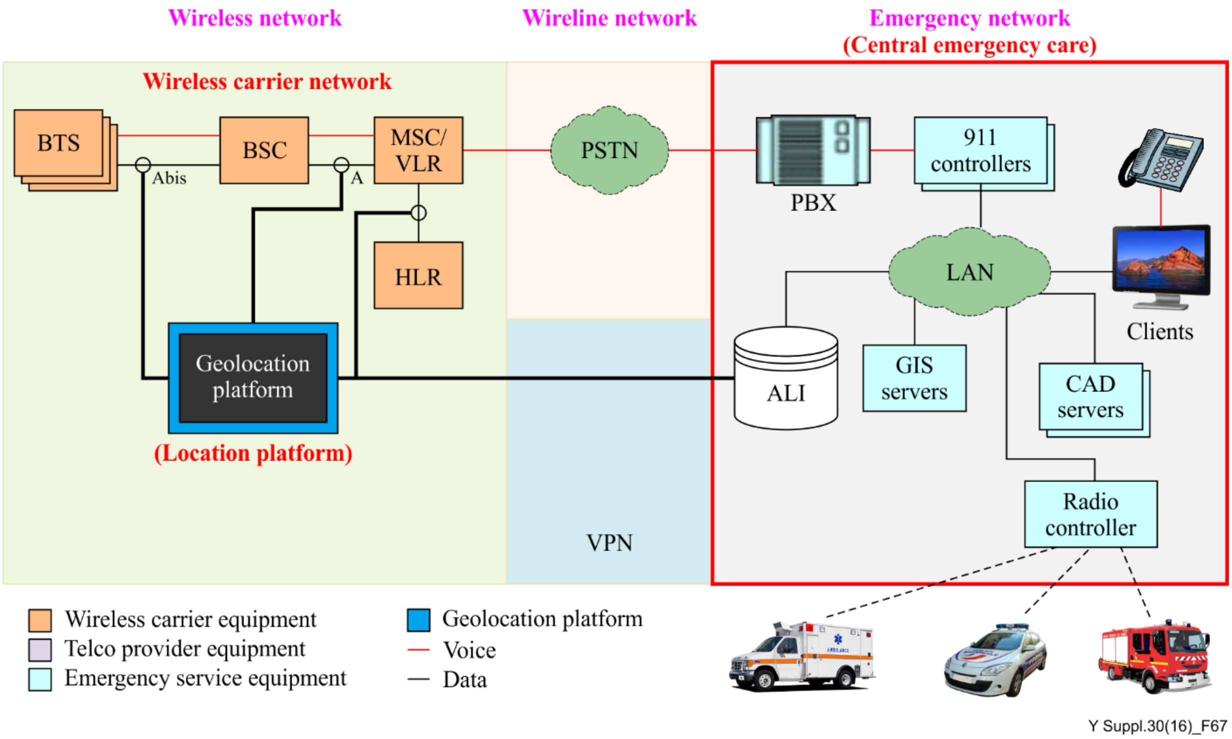


Figure 67 – Location of emergency calls

The solution needs hardware and software, database, operators and dispatchers for the centre for emergency calls, as well as location systems for calls made from fixed and wireless networks.

This solution locates emergency calls of fixed and wireless network automatically, and route them to qualified personnel with the latest technology equipment, showing the location information.

Considering that it's simple to obtain the localization of calls originating in fixed networks (just checking users address database), location technologies have been developed mainly for mobile environments, and must meet four essential characteristics:

1) High precision.
2) Establish a system that never fails.
3) Locate any mobile phone.
4) Operate in all environments (indoor, inside vehicles, in urban and rural areas).

One of the technologies used for location of mobile phones and devices is the technology "Uplink-Time Difference of Arrival" (U-TDOA), which provides highly accurate information, high performance, and low response time. See Figure 68 for an image of the location process using U-TODA.

The operating mode of the U-TDOA technology is as follows:

– A radio signal emitted by the mobile device spreads in radial form at a constant speed (the speed of light).
– U-TDOA compares the time of arrival of the same signal between two base stations equipped with measurement units for location (location measurement units-LMUs).
– As the distance between the mobile device and base stations are different, the time of arrival is also different.
– When the measurements of three or more base stations are combined, it is possible to estimate the point where the probability is higher of finding the mobile device.

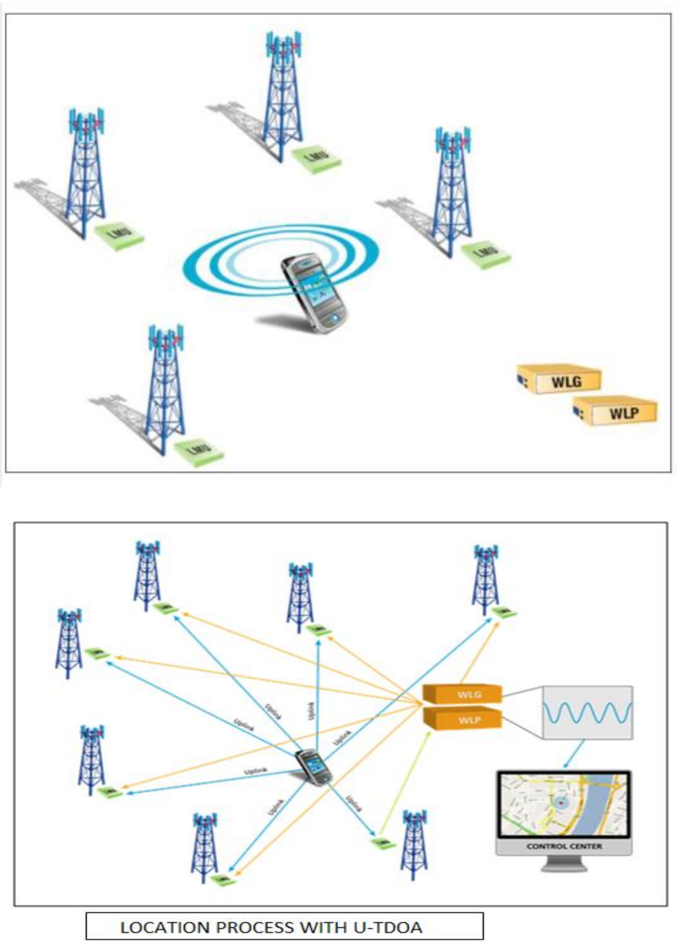


Figure 68 – Location process with U-TDOA

The location technology uses the difference in times of arrival or U-TDOA to determine the location of a mobile phone by comparing the times at which the signal of a mobile device arrives at special receivers installed in multiple cellular base stations.

Receptors are highly sensitive instruments; called Location Measurement Units (LMU). They contain accurate and synchronized clocks that record the time a Radiofrequency signal arrives up to location. The results of different LMU are compared to determine the most likely location of the phone.

Under optimal conditions, where there is more density of base stations, U-TDOA technology locates mobile phones within a radius of 50 meters. The accuracy decreases in areas where there are less radio bases and therefore less LMU.

The U-TDOA method has several advantages such as : accuracy, consistency and reliability. It is also the method of locating cell phones that has focused more precisely on security. Also the U-TDOA location technology is typically able to locate a mobile phone in less than 5 seconds.

Figure 69 shows the location procedure of a mobile terminal:

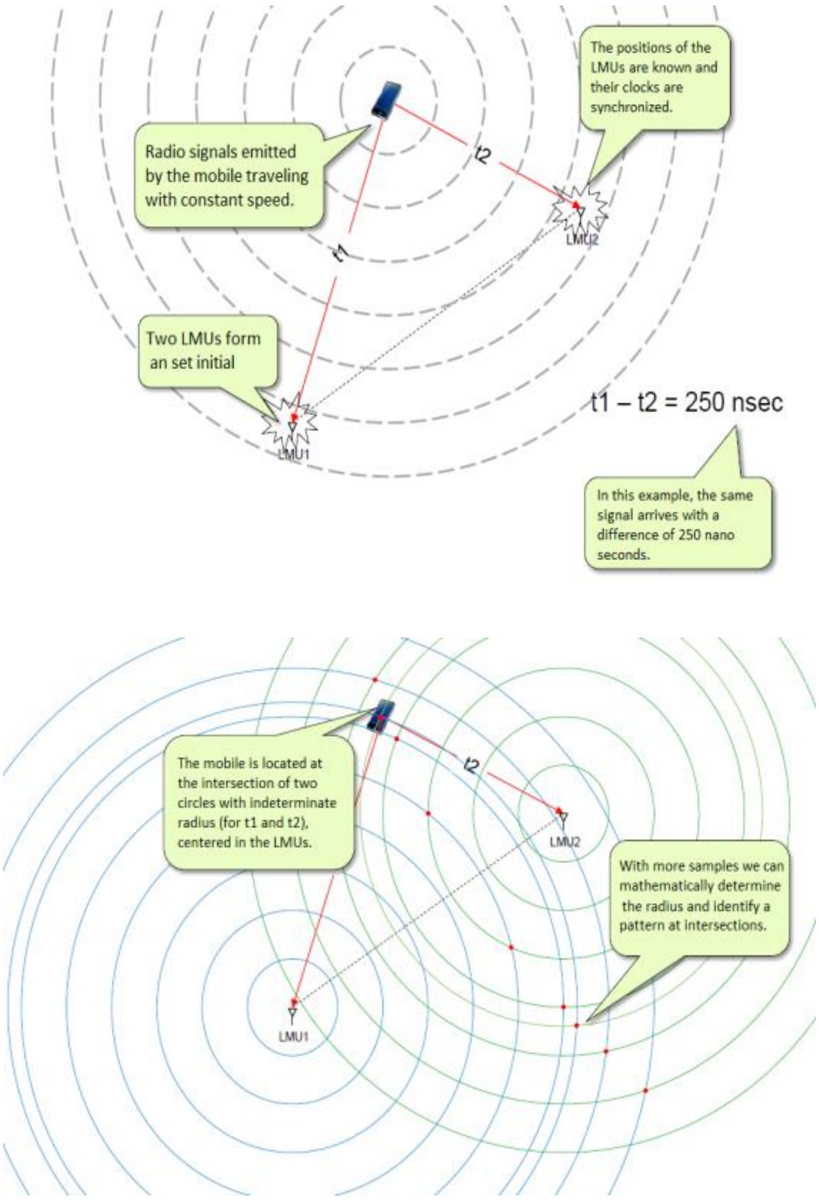


Figure 69-a– Location procedure of a mobile terminal

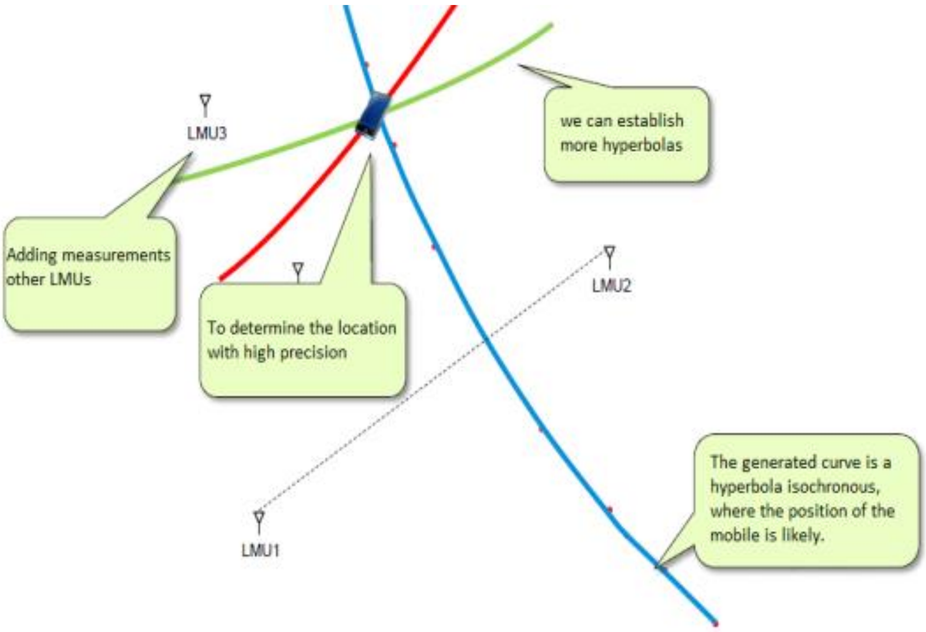


Figure 69-b – Location procedure of a mobile terminal

National alert system using cell broadcast

Especially designed for local and national authorities to deliver urgent messages to large populations, the national alert system can be used to inform the public about hazardous situations such as terrorist attacks, pollution outbreaks, storms, fires, traffic jams and accidents as well as minor events that are not immediately endangering the public safety and security such as water break, power break, construction work, etc.). There are different types of solutions that are designed to effectively send messages to large numbers of mobile telephone users almost instantaneously while receiving input from the subscribers. The national alert system using cell broadcast as shown in Figure 70 is an example of such solution.

This solution not only enables swift responses from authorities but gives them the capabilities to provide a controlled and managed constant flow of information and instructions to the public using different channels depending on the nature and status of the events.

Figure 70 – National alert system using cell broadcast

Moreover, it gives the authorities real-time segmented information based on their relevant departments (i.e., the police department, the fire department, etc.) using both cell broadcast technology as well as "Push IP".

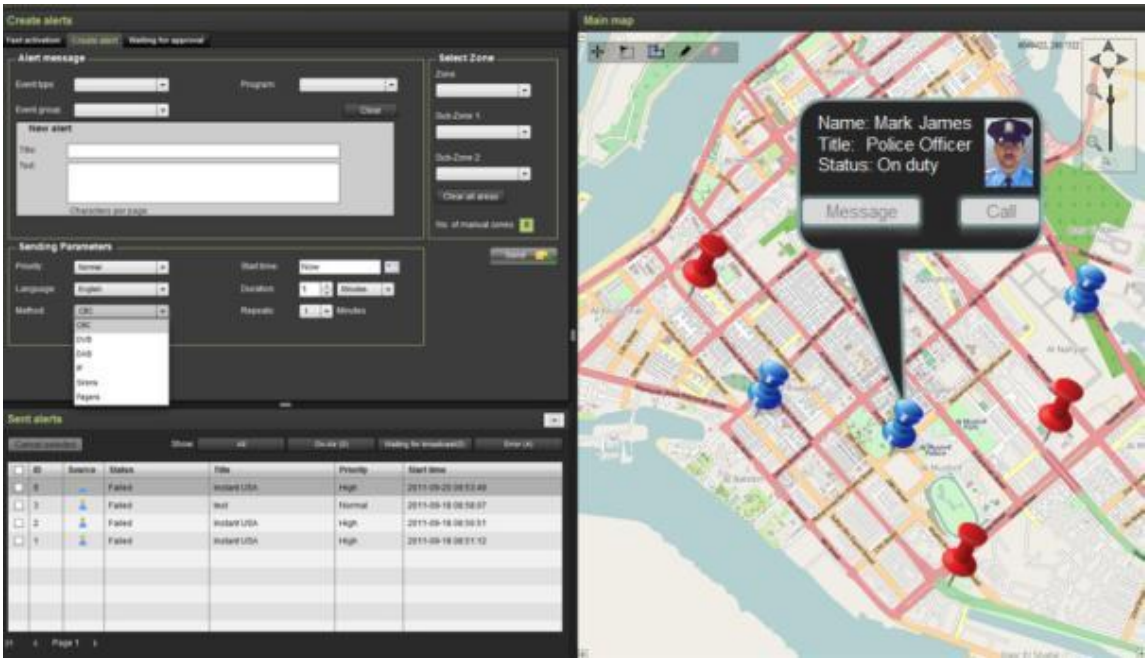


Figure 71 – Using integrated GIS engines

The use of integrated GIS engines (see Figure 71) enables the authorities to deliver the messages geo-targeted and to make them available only to the people who need to get this information. Cell broadcast technology can deliver messages geo-targeted to the cellular antennas at the event's location. Furthermore, it is possible to deliver the information to fix IP addresses of billboards as well as to digital televisions.

Figure 72 shows cell broadcast management software with a GIS engine that allows human operators to select specific geographic areas, to send the messages.

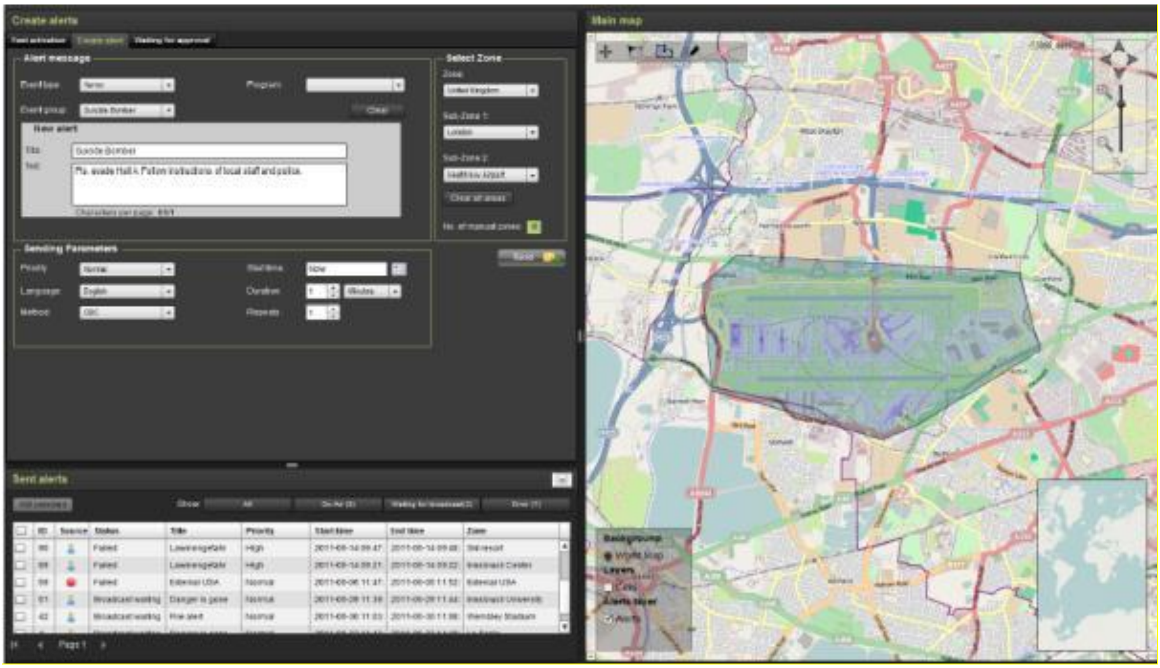


Figure 72 – Cell broadcast management software

The proposed system architecture includes the use of a cell broadcast centre (CBC) directly driven by a SMART system. The architecture of the system can be summarized as outlined in Figure 73.

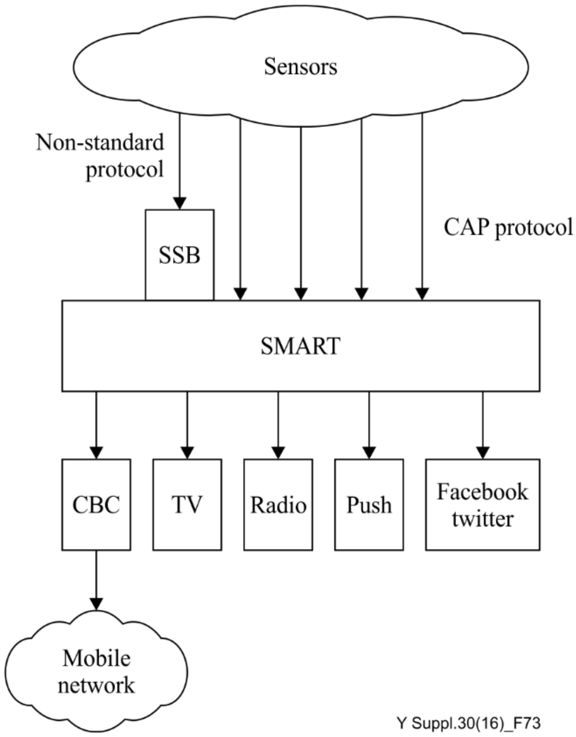


Figure 73 – Architecture cell broadcast centre

The various inputs, which could be either sensors or human operators, communicate with the system through standard interfaces that operate in common alerting protocol (CAP) which is based on XML and is used for the transmission of public warnings and emergencies.

In case of having non-standard interfaces, conversion is performed on the Sensor Service Bus (SSB) entity which facilitates communication to the SMART system from other systems that do not have support of CAP.

The SMART system also allows the creation of polygons that are targeted toward specific geographic areas of interest within which one wants to disseminate alerts. This definition is made from geo-referenced graphical interface. To this end, SMART has an updated database of the location of cell phone stations BSC/RNC and BTS/NodeB that automatically updates through the CBC (that becomes the interface from the network mobile phone.

It is important to note that the system can be deployed under different topologies hence two alternative solutions. First, it is to have a centralized CBC such as in the case of Israel. Second, it is to have one CBC distributed such as in the case of Chile.

Architecture with centralized CBC

This solution requires an updated network information from all the cells, which is crucial to ensure that the cells are correct in their respective polygon.

Citing the case of Israel, all mobile operators are required to update at least once per day by using the FTP protocol. After creating the polygons by using alert handler, the SMART system will define the BSC/RNC and BTS/NodeB that are relevant in its coverage area. The SMART system will then order the CBC to send the message directly to the relevant cells (BTS/NodeB). The key advantage of this strategy is that the administrator (for example, government agencies) has to centralize control of system interfaces and the overall system.

A centralized CBC (see Figure 74) handled by SMART system allows full control over the evolution of the system, allowing the inclusion of new communication standards in the CBC (LTE, femtocells, etc.), where and when available. Thus, the administrator (for example, government agencies) need not wait for mobile operators to update the CBC because this factor will be under his own control.

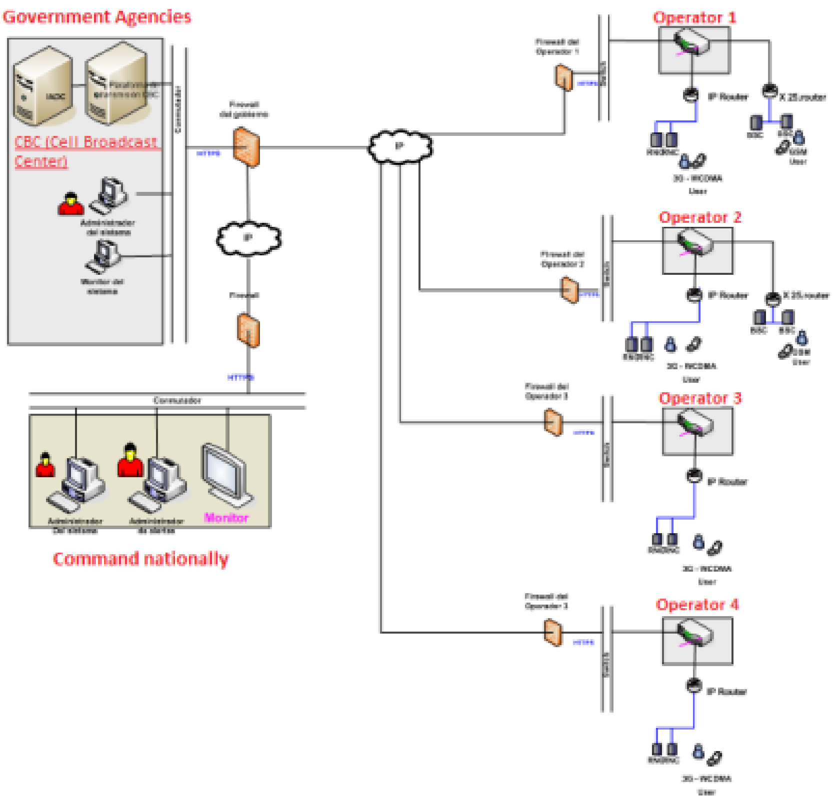


Figure 74 – Arch diagram of solution with central CBC

Architecture with distributed CBC

A distributed system would imply that although the SMART system is installed outside the network of the mobile operator, the CBC is deployed within it. As a result of this, the SMART system should have an interface for each CBC installed on each of the mobile operators (see diagram in Figure 75). The advantages of such solutions focuses on the fact that mobile operators are not required to disclose information about the position and coverage of their cells. Because of this, it is necessary to develop mechanisms of cell load information to inform external system about the change of information in a cell.

This also implies strong consequences for the translation of the respective polygon geographic (longitude/latitude) to specific cells located within the respective area covered by the polygon. Dynamic changes in the radial structures (especially on 3G networks) need not be reported to the SMART system because sending messages CBC to BSC and RNC of operators will be managed within their own facilities. Additionally, mobile operators can also use the CBC for other commercial services. This also allows the operators to decide the vendor of CBC equipment.

However, as the intermediary will only transmit information respective of polygon to CBC (longitude/latitude) and not the ID information of the cell, an additional intermediate component between the intermediary and the CBC would be needed in the equipment room of the mobile operator. The component is called portal (gateway) CMSP. This component is responsible for translating the polygon information (latitude/longitude) to the ID of the respective cells of the relevant mobile operator. Each component in the portal (GW) CMSP will be customized according to the CBC interface to which ones connect.

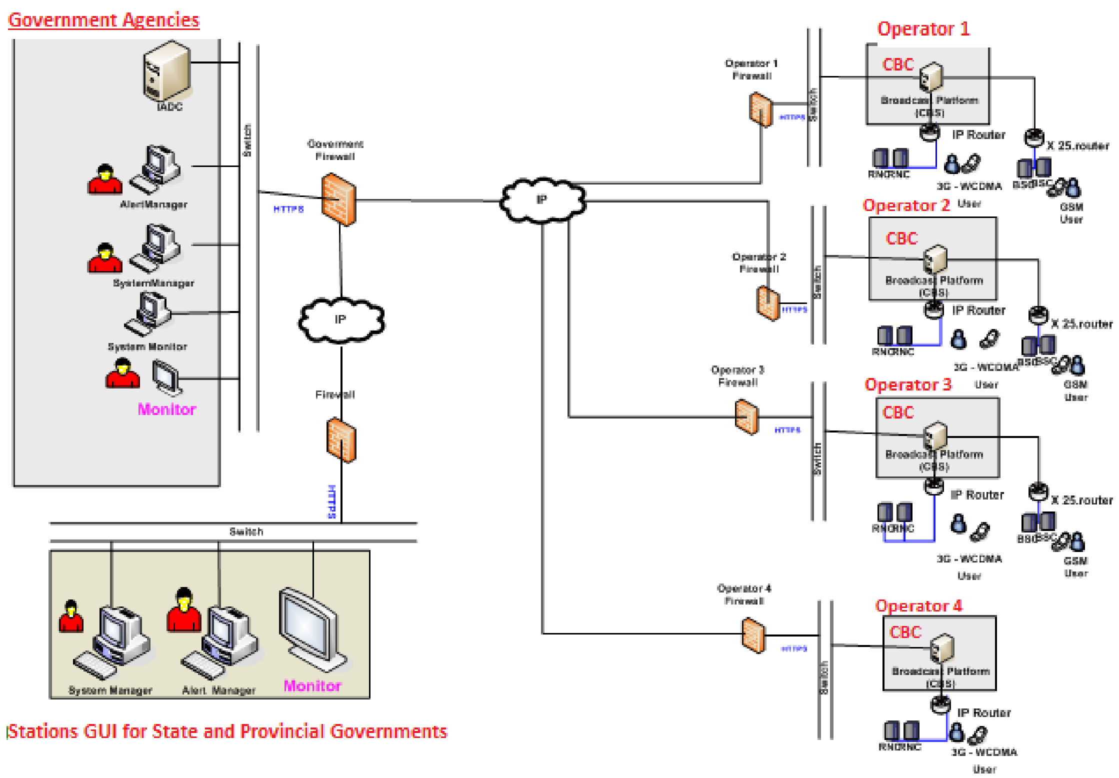


Figure 75 – Diagram of solution with distributed Cell Broadcast Centre (CBC)

In this scheme operators can use a different brand of CBC for each of them, as one2many, Huawei, Alcatel-Lucent and others.

6.5 Education and tourism

The ICT infrastructure should also serve to improve aspects such as education and tourism; that is in general to ensure tangible economic growth such as higher standards of living and employment opportunities for its citizens.

Besides the known contribution of ICT to education, both classroom-based and distance-learning, the influence of the SCC will mean that the citizen will be placed in the centre of the educational scenario. The perimeter of the physical space in which educational experiences develop is becoming increasingly more indefinite and liquid, by hosting more informal practices characterized by high density of social interactions.

The SCC itself has the potential to serve as a teacher; for example, cities that already have a strong historical or artistic component must be an open book for the citizens and visitors supported by ICT. The visions are cities increasingly more open to participation in a smart and spatially widespread temporal education: online learning systems, training by computer, support forums and collaboration with experts, information about job opportunities and meetings that promote retraining etc. Other functionality may also include the use of new information and communication technologies to develop virtual museums, digital public libraries, augmented reality, digital art, co-creation and other leisure activities and assisted real-time translation and cultural mediation.

Data analysis, mobility and ICT are part of the industry trends in travel and tourism. New computing tools and large volumes of data are being used to retain customers, improve operations and meet the service experience of travellers in hotels. For example, the Electronic Guides that are found included in mobile applications, allow the visualization and identification of points of interest for the tourist (municipalities, commerce, museums, churches and hotels) through the Geo positioning systems. Reality augmented services (concept later extended) have also emerged as new applications for mobile phones that provide information to tourists based on their experiences, geographic locations, and interests. The smart sustainable city concept could positively affect tourist arrivals with environmental or technological concerns. On the other hand, it may offer to tourists, as well as everyone involved in this business, updated and accessible information (location and hours of entertainment events, etc.).

6.6 Environment and waste management

The ICT infrastructure can establish an environmentally responsible and sustainable future which "meets the needs of today without sacrificing the needs of future generations". Aspects such as improvement of transport courtesy of the ICT infrastructure and its applications, and an improvement in energy efficiency, can reduce pollution for example.

The environmental sustainability of an ideal SSC could be achieved by upgrading the following infrastructure:

– Use the IoT technology to form a closed-loop management for the monitoring, early warning and control of pollution sources.
– Use distributed sensors to enhance the air quality and urban noise monitoring, to communicate with the public, and using mobile communication systems to strengthen the linkage between the supervision and inspection departments.
– Strengthen the real-time water quality testing network system constructed for reservoir, river, and residential building secondary water supply in order to guarantee true real-time monitoring.
– Strengthen the sensing system construction for green belt of forests, wetlands and other natural resources, and timely access green resources situation combined with geospatial databases.

– Use sensor technology, communications technology and other means to improve the monitoring, control and management on the thermal energy and building temperature systems.

Through the improvement of an overall smart system, water, electricity, natural gas, coal, oil and other resources could be reasonably allocated and utilized. Sensors installed in strategic locations, territories and cities are improving the monitoring of environmental variables and disposing higher information for decision-making.

It is necessary to incorporate clean and responsible management of waste, thus the amount of waste produced by citizens is one of the future challenges within the concept of clean and sustainable cities.

For example, in the Dutch city of Groningen, a personal card is required before depositing wastes in a container. This personal card would record every time the user opens the lid and therefore assemble behavioural data of the user with the hope of encouraging responsible waste management[40].

Another of these smart elements is the fill control, whereby when the container is full it emits a signal that alerts the garbage collection service. In this way, routes and schedules are optimized, the time spent on garbage collection is improved. This process also saves energy and reduces CO_2 emissions by better organizing the transport and avoid the unwanted waste in the street by overfilling containers. These advantages are made possible by the incorporation of chips in containers, which generate appropriate signals by microwaves, providing all necessary information, such as temperature. If the container temperature passes from some determined degrees, the chip shall deliver signals to firefighters to avoid fire. This not only minimizes the risk, but also extends its useful live, with consequent cost savings.

6.7 Smart building, digital home

The city life does not end in public spaces like streets, squares, parks, etc. It also includes the life of the population in their own homes and in public and private buildings; that is what one calls a digital/smart home/building.

A smart building is the integration of building, technology, and energy systems. These systems may include building automation, life safety, telecommunications, user systems and facility management systems. Smart buildings recognize and reflect the technological advancements and convergence of building systems, the common elements of the systems and the additional functionality that integrated systems provide. Smart buildings provide actionable information about a building or space within a building to allow the building owner or occupant to manage the building or space[41].

---

40 An example of this use is the Dutch city of Groningen.

41 http://econtrol.me/Smart%20Building.html.

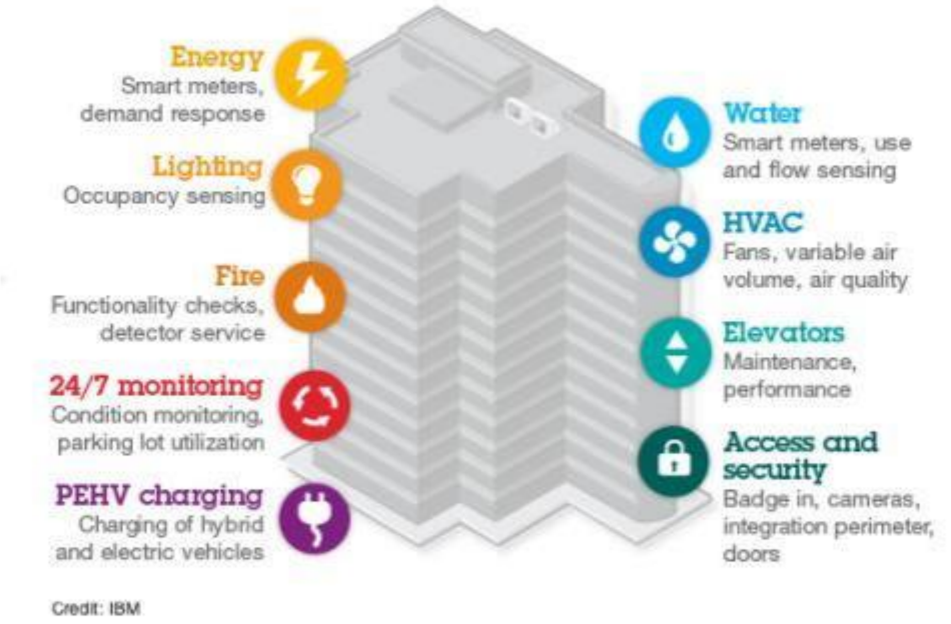


Figure 76 – Intelligent buildings

The future and the development of intelligent buildings (model shown in Figure 76) are based on the following pillars: "Smart" objects with electronic chips embedded capable of receiving and transmitting information (e.g., Sensors), devices using remote control, communications favoring the transmission of information between devices and interactive and accessible interface to the users that allow the network used in homes to become easy to use (user-friendly), Intelligent building management systems (IBMS), smart energy control systems for buildings and economic efficiency and impact on energy savings[42].

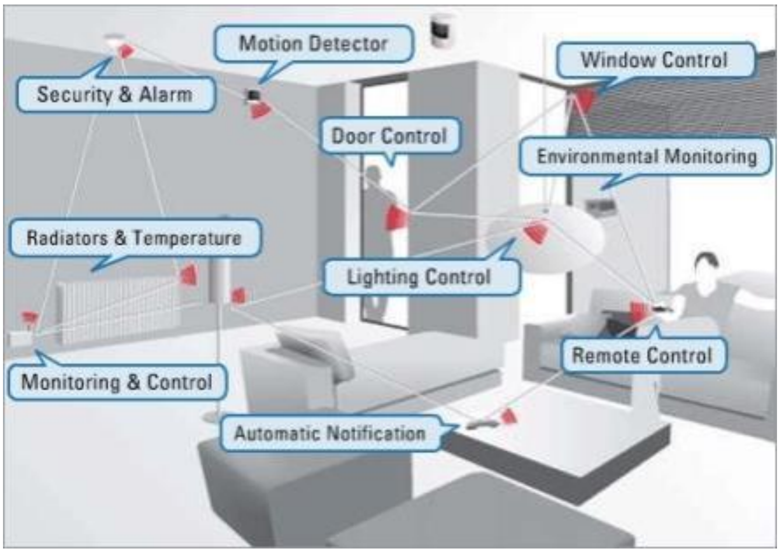


Figure 77 – Smart energy control systems for buildings

[42] Technology Map "Smart Cities"; Ministry of Industry, Trade and Tourism of Spain.

6.7.1 Home energy management

Visualization service of consumed energy

The smart energy control system (Figure 77) is required to measure the consumed electric energy of each distributer, breakers the generated energy by solar cells, and allow to calculate the fee of energy and to inform the cable customer of the result. The current sensor is required to transmit measured data (consumed or generated electric power) to the radio terminal device by ZigBee or wireless fidelity (Wi-Fi) radio chip. The residential gateway (RGW) is required to store the data temporarily (e.g., for one day) and to upload the data to the collection server of sensor information.

The system is also required to present the cable customer with a regional power saving period, a power saving announcement, and information on power balance from a municipal office or power company. In other words, the system should not only display consumed/generated power. The system can provide, optionally, recommend services for power and cost saving, in line with the customer's power consumption pattern.

Furthermore, the system can optionally provide any additional support including regional ranking information of power saving or additional incentive services. The system is required to be operated on RGW (see Figure 78) at home and on a smart phone or tablet terminal, and in an outdoor environment through the cable portal function. The system is required to send the information by e-mail to the assigned address.

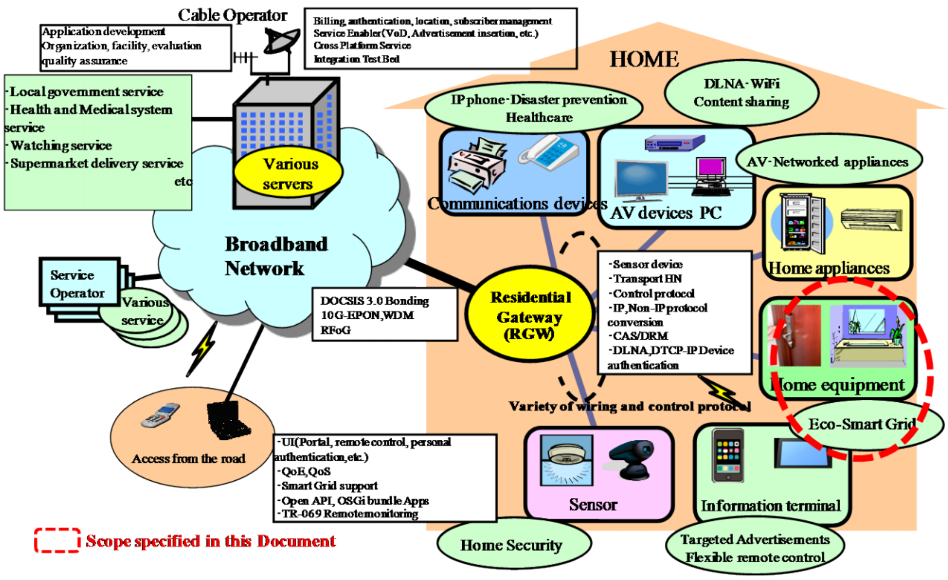


Figure 78 – RGW and related entities for home ICT services

Source: Technical Report of the Focus Group on Smart Cable Television.

Solar power cell maintenance service

This is an information service to the cable customer on the maintenance of the solar power cell. The system is required to report to the cable customer the necessity of surface cleaning, the existence of malfunction through the monitoring of past power generation record and comparison with regional standard generation value.

In general, the detection of the failure of the solar panel module is difficult; hence, it is normally left without maintenance even during the guarantee period. It is also useful for the customer to be informed that the trouble is caused by climate change or a stain/malfunction of the solar panel. The system has to report the result to the cable customer. In case of a home battery, the system has to provide the appropriate exchange date of the defective battery or advise on the economical usage of the battery based on a past operation record. The system must send the information by e-mail to the assigned address.

Presentation items

The presentation items are shown below to realize the aforementioned services:

1) Electric power consumption (real time, every hour, past record, regional ranking);
2) Electric power generation (real time, every hour, past record, regional ranking);
3) Electric power fee (time zone, monthly, comparison with previous year);
4) Battery status (real time, charge/discharge record) and exchange date;
5) Usage report by the power company (regional power balance);
6) Malfunction of the solar power panel and/or necessity of cleaning;
7) Setting threshold of power consumption and control. Technical Report of the Focus Group on Smart Cable Television ITU-T FG Smart Cable Technical Report 5;
8) Alert indication over threshold, usage recommendation, sending e-mail;
9) Power saving schedule in region;
10) Economical usage information;
11) Contract detail with the power company;
12) Setting of presentation.

High-level system architecture

Figure 79 shows the high-level system architecture for home energy management services.

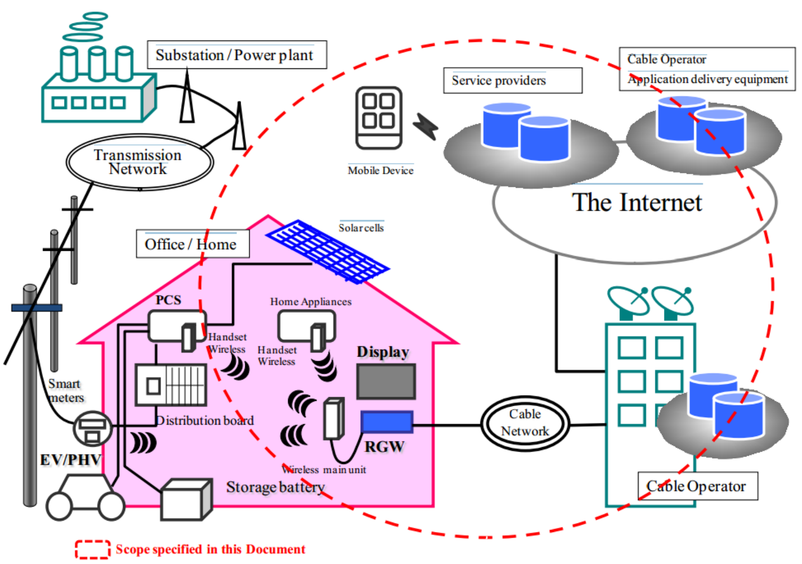


Figure 79 – High-level system architecture for home energy management services

Pre-conditions

– The residential gateway and measurement devices for power consumption should be provided in the customer premises.

– The interface conditions and transmission protocols (device discovery, capability check, data acquisition, etc.) between the measurement devices and the gateway, and between the gateway and the cloud should be standardized.

– The application for the visualization service of consumed power should be provided.
– The application download function should be provided in the application distribution system and the terminal devices.
– Data processing in the cloud should be available in real time by the application.

The terminal devices (RGW and mobile devices) should have a browser function to present data processing results.

Main steps

1) The customer is able to download the application for the visualization service of consumed power in the terminal devices.
2) The customer selects the service (visualization service of consumed power) on TV or on a mobile device screen and logs using their ID and password.
3) At the selection of the service by the customer, the functions for the discovery of measurement devices and communication to the gateway are activated.
4) The measurement device reports the obtained data to the gateway function periodically or at the time of customer access.
5) The gateway function transfers the measured data to the cloud by the application, the cloud processes the data, and the results are conveyed to display terminals (TV or mobile devices) through the gateway function.
6) The terminals present the processed data on their screens.

7 Planning the national deployment of ICT infrastructure for SSC

Until today, the planning of a SSC is in the hands of the Government, although the private sector has been engaged in developing and implementing corresponding frameworks. It should focus on generating cross-cutting, inclusive and comprehensive strategies, using ICTs, to optimize the meeting of the diverse needs of the citizens.

The use of ICT in the planning of a smart sustainable city must be aimed at interrelating the complex systems that form an urban area (utilities, communications, production, information, infrastructure, vulnerability, etc.), as well as, proposing smart and inclusive solutions oriented to use efficiently and sustainably the resources required by the citizens, particularly the non-renewable ones (Figure 2).

In this sense, the challenge of planning raises the need to:

– Design efficient management schemes for electricity consumption;
– Monitor and rationalize the use of water;
– Create control systems to reduce vehicular air pollution;
– Design more interactive communication tools to meet the need of information, avoid physical movement of people, among other solutions.

These solutions can be developed individually, but they must be transversal. It will allow to identify synergies and opportunities for improvement, reduce costs, seek the well-being of the population, and thus, achieve a smart sustainable city.

There are two aspects to consider during the strategic planning of the deployment of ICT infrastructure: first, the deployment of new ICT infrastructure itself; and second, the improvement of current ICT infrastructure using new technologies. In the first case, the strategies can be addressed both from the point of view of the previously mentioned stakeholders and also from the point of view of the ICT infrastructure itself as an object to be upgraded. The last point of view needs to include convergence strategies.

It is recommended that the formulation and implementation of policies and strategies are followed by a multi-stakeholder (i.e., public and private, local and supra- and commercial and non-commercial) approach. However, conflicting interests from different stakeholders may arise. For instance, there are differences of views between local governments and operators about the consideration of providing free basic connectivity, since it can be seen as a form of unfair competition by the operators, rather than a complement and a new civil right.

Regarding the point of view of infrastructure as an object to be upgraded, there is a natural predisposition to match the classical networks (roads, energy, sanitation, etc.) with digital technologies of communication and information. It is appropriate to note that the communication networks have an impact on the physiognomy of cities, as demonstrated Figure 80 showing images of New York in the late nineteenth century where the web of high telegraph and telephone cables brand the image of a networked city.

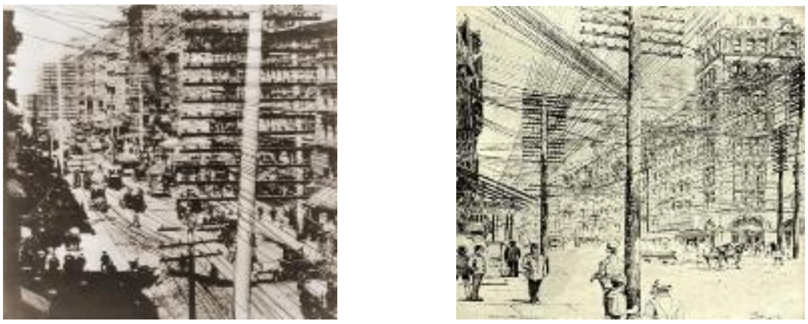


Figure 80 – New York (United States) at the end of the XIX century

The images in Figure 81 show the communication networks' impact on the physiognomy of some cities in the developing world in the XXI century.

Figure 81 – Manila (Filipinas) and Vijayawada (India) at the beginning of XXI century

As demonstrated in Figure 81, many of the existing urban environments are overran by thousands of cables with little regards to safety and efficiency. Therefore, it is imperative that communication infrastructures must exit in an affordable and accessible way. Successful strategies could then be replicated based on the given specific measurements such as in the case of laying cable in the suburban zones.

Currently, infrastructures in cities should overcome the following shortcomings such as; the lack of exploit of synergies among public services and the communication restrictions; the uneven bandwidth capacity among different providers and so on.

To remedy these defects, one should aim to create a strategic model from a holistic approach, with particular actions that would improve the adaptation ability of the existing, infrastructure, which would in turns supports and builds the SSC.

The existence of these limitations can be conceptualized with the idea of "Liquid network" (see Figure 82), which is an approach to describe the citizen's communications traffic and their daily trends. There is a behavioural pattern of the online communications traffic in a fluid form that generates "waves" of data traffic. These waves accompany with the movement of connections (for example from the outskirts of the cities to work centres) or a movement related to the time (concentration of masses, i.e., in stadiums for sporting events).

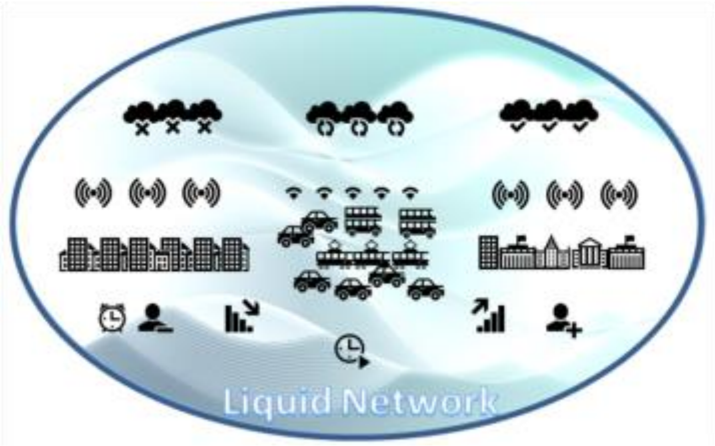


Figure 82 – Liquid networks

Clearly, it is a challenge to have infrastructure adaptable to large daily changes according to the traffic needs as described. Strategies are needed to handle a "Liquid Network" urban character, in order to meet individual bandwidth requirements and to have the functionality of mobile usage, as well as, strong processing capacity in different areas of the city, according to each time of day.

Nowadays, issues such as smart radio, mobile mesh networking, mobile ad-hoc network (MANET), mesh radio and others are nicknames used to designate different technological aspects of a future scenario, where the user terminal devices have sufficient capacity to constitute networks of varying topology and also perform the functions of both the structural nodes of network (such as routers and servers) and customers.

The possibilities for the deployment of services in such scenario are immense and could correct many of the defects mentioned before. For example, each device in a MANET has the freedom to move independently in any direction. It enables dynamical changing over new conditions of link between the devices. Each device is uncoupled from traffic and therefore, performs missions of a router.

One of the main challenges in the build time of a MANET is to equip each device to continuously maintain the information required for routing. Such networks result from the combination in each of the terminals or nodes of the layers identified ICT infrastructure, i.e., the data communication and the detection layers, and they can operate independently or be connected to the Internet.

Other infrastructure to be considered is the High-altitude platform station (HAPS). Its ability to vary the beam communication is highly adaptable in an urban environment, directing more bandwidth to where it is most needed in the daily evolution of zonal needed for data traffic. Although, its commercial use is now limited and focused on remote areas (such as Alaska), ITU-R has already defined the total area coverage of a HAPS aircraft in the bands 47/48 GHz and have divided it into three areas: urban, suburban and rural (they are needed to ensure consistent broadband users throughout the visibility zone on the floor of the HAPS). The urban area coverage extends between 36 and 43 km from a point directly under the platform. Users of these areas can be portable modems. The suburban urban area coverage is up to 76.5/90.5 km, depending on the altitude of operation of the HAPS. Users from suburban area coverage should use high gain directional antennas and transmit power.

Besides, there are also business technology initiatives that take advantage of the height, both for energy production and for the establishment of communication nodes (and meteorological studies). One example is the bouyant airborne turbine (BAT) that uses high winds to produce power and to transmit it to land routes subject to the anchors (see Figure 83). Clean energy + point communication are a typical combination of infrastructure for future SSC.

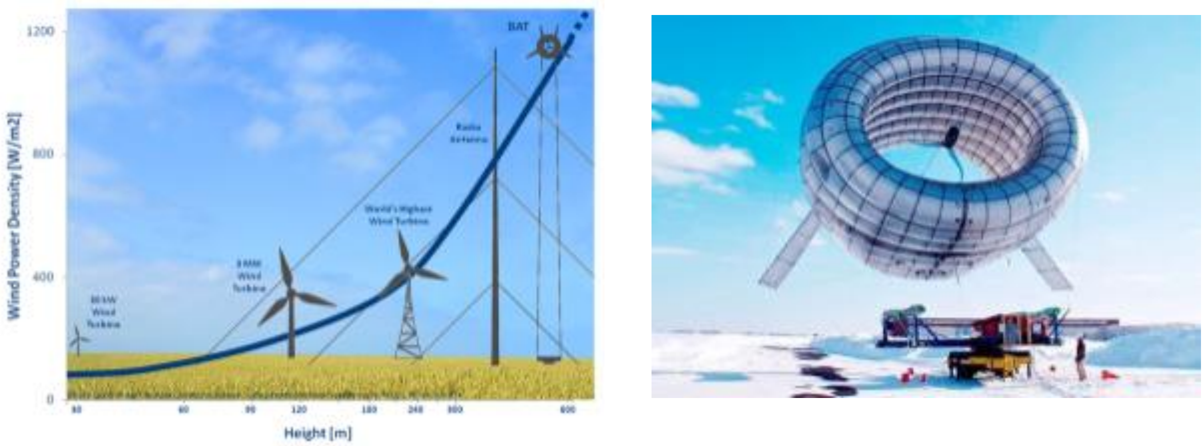


Figure 83 – Example is the bouyant airborne turbine (BAT)

Image of BAT near to the ground and explanation of the height gain.

7.1 Urban growth in the knowledge era and the digital divide

There is a common census on how important knowledge, technology, and innovation are in contributing to the success of a city. However, differences can be drawn from debating what are the key factors that would influence knowledge and innovation[43].

Therefore, any strategy of planning for the ICT infrastructure deployment should take into account aspects such as combating the digital divide within cities.

[43] This document focus on the "hard" part associated with the influence of business; however there are explanations due to the influence of persons (talented and creative people changing the structural design of cities).

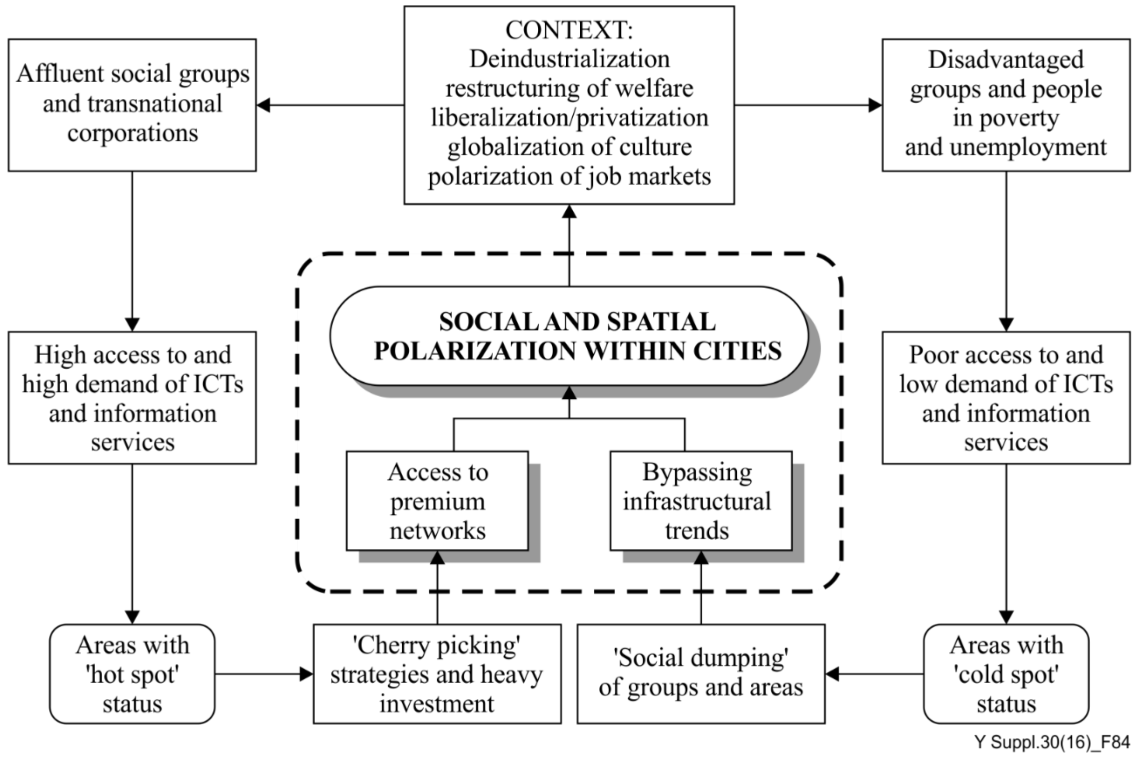


Figure 84 – Social and spatial polarization within cities

Figure 84 shows a scheme of how trends in telecommunications are underpinning the shift to more socially polarized cities.

The authorities should be aware of the polarization problem caused by the lack of infrastructure and the differences in economic and social conditions within cities. Therefore, it is recommended that communication infrastructure projects should be given a priority status in the political agenda and receive an adequate amount of public resource for these projects to reach maturation.

7.2 Strategies for the deployment of digital/ICT infrastructure

An approach to establish deployment strategies is to study the interactions between the supply and demand components. An adequate offer of connectivity boosts the demand, while more demand increases and improves the supply (a desirable virtuous circle). Taking that into consideration, the content of this section should not focus only on supply strategies, but also on demand strategies. Moreover, appropriate strategies in the regulatory and financial aspects should also be included.

7.2.1 Strategies to stimulate the supply

Governments may own existing infrastructure and share it with private operators in order to develop new projects:

– Telecommunication networks: Governments may own existing wireless accesses and share their network capacity. Projects are usually focused on facilitating the administrative tasks of local government and providing connectivity to educational institutions.
– Poles, lampposts, buildings and other high places: High points are necessary to place antennas and other infrastructures.
– Ducts such as sewers, gas pipes and others: They are especially important for transport networks. For example, sewers are used for fibre optic laying. There may be versatile ducts for all networks (electricity, gas, telecommunications, air conditioning and water).
– Public roads: Road networks facilitate the laying of telecommunication transmission lines.

– Traffic light's networks: Traffic lights can be used for wireless connectivity. In fact, there are initiatives that use preinstalled infrastructure for traffic control network. This type of network has centralized intelligence that demands telecommunications for the vehicles control system.

7.2.2 Strategies to boost the demand

ICT are demanded for its utility. The services and valuable content are what provide meaning and utility to its infrastructure. Without infrastructure, the content and services do not exist. The mutual dependence of both infrastructure and content is what configures its development.

When governments intervene on infrastructure that supports ICT, they are concerned about two aspects: (i) management of services and (ii) establishment of good relationships with the citizens:

– Give content to the demand: Currently, the biggest boost to the demand for ICT comes from the possible exploitation of the broadband services such as VoIP, IPTV, monitoring camera applications, video streaming, augmented reality, video conferencing, etc. In this sense, the government can stimulate the demand by using those tools and providing content over the network.

– Train users in the use of ICT: The intervention may be oriented to improve both disposition of consumers to use technology (since what is not known is not appreciated) and increase their capabilities.

– Provide connectivity: Hardware, software, appropriate contents as well as knowledge and skills to micro, small and medium enterprises (SME) should also be provided.

– Give direct subsidy: First, government can subsidy the user final system (directed to the terminal such as the PC or to the modem). This kind of subsidy is usually used on educational institutions. Second, government can subsidy the access itself.

– Provide public free access at municipal level (it means a full connection subsidy). This is increasingly widespread and funds will usually come from supranational contributions canalized by regional and local governments.

7.2.3 Regulation and financing

No infrastructure deployment strategy can overlook the regulation and financing aspects. In markets involving utility networks such as telecommunications, regulation is essential.

The regulatory institutions are different according to the national law. They are affected by the type of state (unitary, federal or confederal), and also by the integration of a country. Strong integration will lead to supranational regulations to be applicable in the whole country.

The regulatory role of local governments can vary depending on the countries, and it can be extremely relevant in countries that are highly decentralized. Local government's capacities to involve in regulation and financing of city infrastructures may vary depending on their correlated legal-institutional frameworks and jurisdictions. An example would be the United States, where each state has been given extensive jurisdictions over the telecommunication infrastructures.

The regulatory control of natural monopolies involves the encouragement of competition, the efficient use of scarce resources, ensures the quality of services and the defence of the users' rights. Although this issue is a matter of sectorial management (for instance, a Ministry), local governments come to venture into these issues.

Thus, besides the sectorial normativity, there are other regulations which can be affected. For example, there are countries in which their interest access is governed by community centres. While formally in other countries these centres are not regulated by the telecommunication authority. Instead, there may be local regulations (i.e., civil defence and protection of children) that affect the sector for instance by establishing a minimum number of posts, the distance between posts or by filtering some Internet content. Then, at the municipal level, in virtually all cases and countries, there are regulations exclusive to cities in building permits, use of rights of way, visual impact (antennas), urban impact, environmental impact, operating licenses, zoning and other issues related with the internal structure of the city itself. In other cases the city government promotes infrastructure deployment, by allowing (with or without cost) the use of public structures such as poles, street lights, tunnels, ducts or roads, etc.).

Thereby, local governments can play a very important role, since rigid normativity on certain facilities (air, antennas, ducts) inhibits the deployment of networks. In the same way, high costs of the right of way increase the cost of infrastructure and the corporate management.

In cases when governments deploy infrastructure projects, financing strategies are very heterogeneous. Even though, all of them are public initiatives, not all financial models will use taxation. The main funding mechanisms that can be used are:

– From taxes: It is one of the most important source of public funding. It is criticized by opponents of the government intervention, especially when governments intervene in areas where there is already telecommunication access.

– Redeemed for taxes (tax or rates): It happens when government taxing rights (i.e., rights of way) are exchanged for infrastructure development or services. Another form of redemption is tax relief to stimulate the infrastructure deployment of some operators. An alternative form of this type of funding mechanism is "tax works" where operators develop infrastructure in exchange of not paying some taxes (equivalent to the cost of the infrastructure).

– Loans + free cash flow: It is a mechanism comparable to the financing of any private project, where the initial capital comes from the financial leverage from partners. In this case, the government can appear as the first guarantor of loans, either directly or appearing as the main customer. Subsequently the project can try to sustain itself by the received revenue as a compensation for their services.

– Government as a major customer: Deployment projects can be funded by the income provided by governments, such as the city government.

– Advertising: It refers to the funding mechanism from Internet contents: paid access and advertisement financing. Part of the revenues from the two concepts may end in the government coffers.

– Utility allowance: It refers to using funds collected from other public service (mainly from electricity distribution service) to maintain telecommunications infrastructure projects. However, some regulations prevent these cross-subsidies.

– Corporate donations: As a form of social responsibility, there may be private donations from businesses.

– Agreements with companies: Sometimes, private companies offer a portion of its capacity to the public free of charge.

– National or multinational Subsidies: It is not rare to see municipal or supra-regional projects funded with capital from Central Government or multinational organizations.

– Cooperative projects: Cooperative wireless broadband networks are a common phenomenon. However, it does not always have municipal support or intervention. In fact, sometimes the local government ends up with a project that was originally created as a cooperative and community project. In Latin America, there are cooperative models related to municipal action; in some countries cooperative telecommunications companies have their origin in a local government intervention.

7.3 Evolution to become a smart sustainable city

Evolution occurs from different starting points (depending on the current development of each urban area). It is better to study how the more advanced cities evolved, in order to replicate this evolution in less developed cities. For instance, as it can be seen earlier in this chapter, in 1887 telegraph and telephone cables in New York City were tangled over the outline of urban roads. Nearly 130 years later, an identical phenomenon occurs in the developing world. That is why learning from the past results is necessary. In the same way, many other lessons can be learnt from the cities that are open to the idea of SSC.

It is not necessary to go through each stage in the evolution to become a SSC. In this regard, it will be useful not only to pose an ideal model for SCC, but also to identify specific cities that are moving toward that goal. Even if these cities haven´t reached the model completely (must be noted that the SCC, as all human work, can be improved on, and therefore, it will be a moving target, under constant improvement). In that way, other cities can replicate their strategies, correct errors, ignore delay factors and accelerate the followed steps.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016