Electric Mobility

"ecoCity eMotion"

24-25th September 2014, Erlangen, Germany

Standardization in Smart Grids – An IoE Perspective

Peter Caldera
Lantiq, Austria

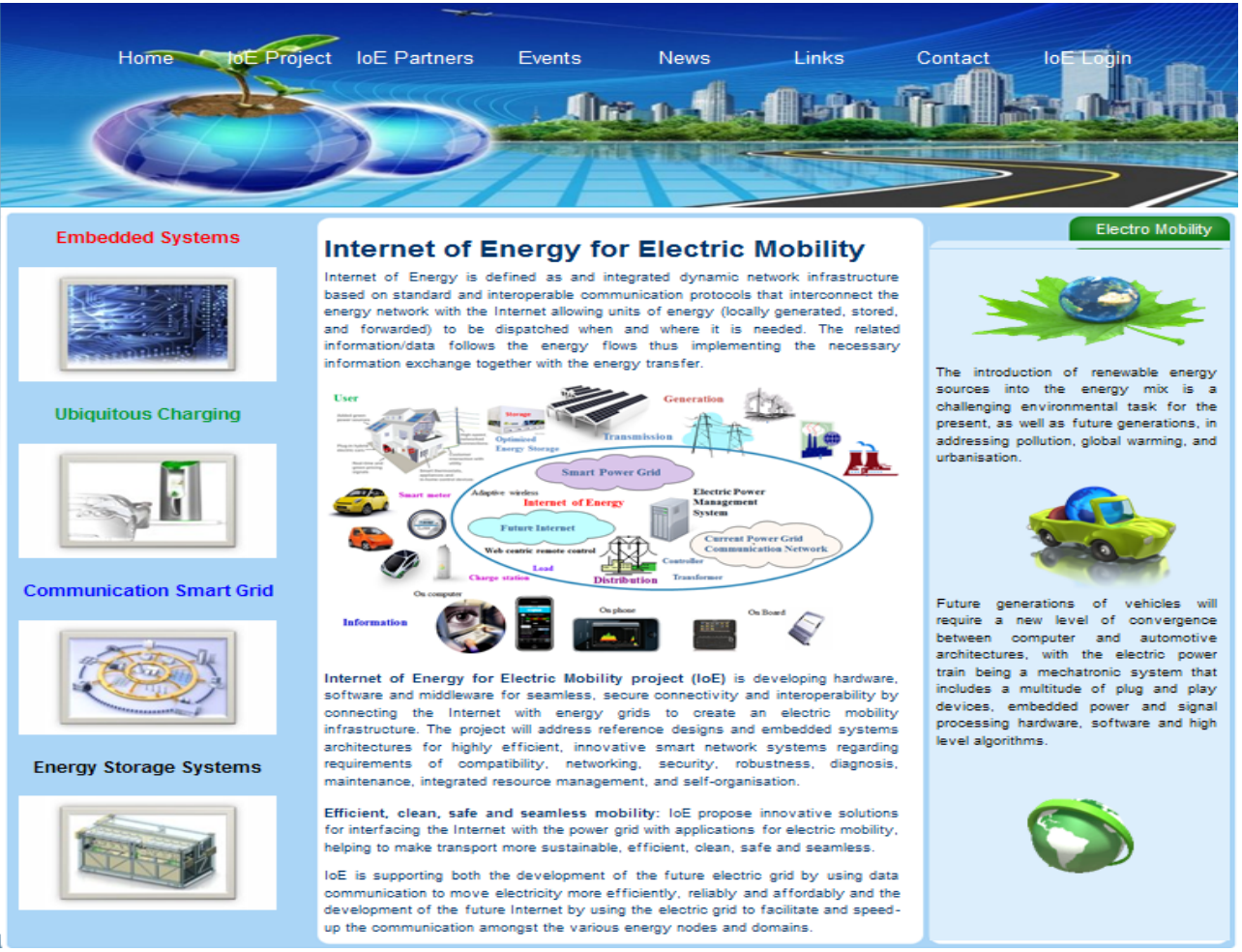
ECSEL JU

Presentation Outline

- Introduction
- State of the Art and Beyond, Requirements
- Existing Solution and Problems
- Overview on Standardization Activities
- Summary

ECSEL JU

Internet of Energy - Standards



The EU/ARTEMIS project "Internet of Energy for Electric Mobility" (May 2011 until Sept 2014) investigates the **integration of**

- electric vehicle infrastructure,

- renewable energy resources

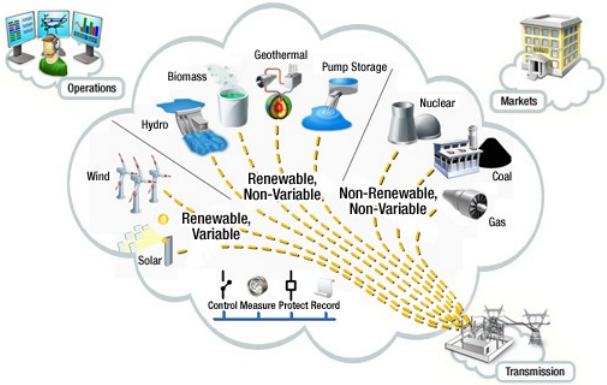
- stationary electrical energy storage systems

via buildings into the smart grid.

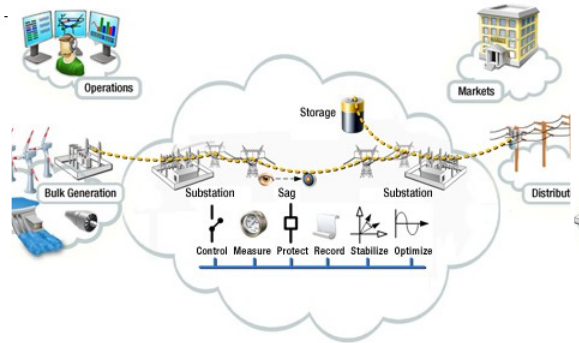
At present, this integration is rather difficult because of a lack of standards, especially for the communication protocols.

ECSEL JU

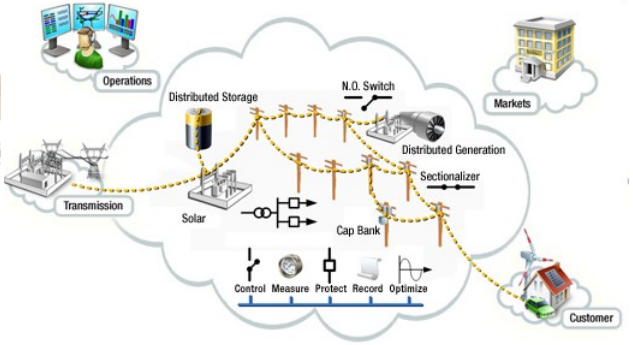
Introduction



generation

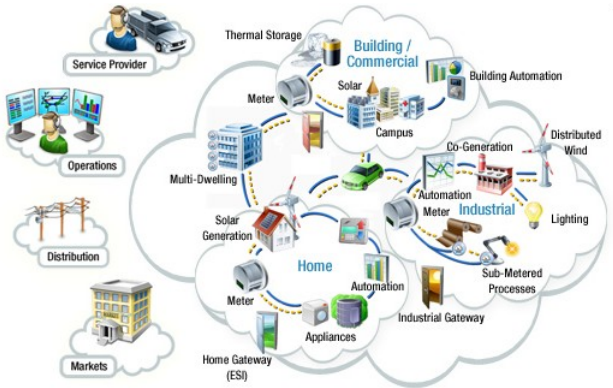


transmission



distribution

- Smart Grid is composed by several domains
- Intelligent and dynamic grid with distributed generation and storage options
- Active participation by customers
- The Smart Grid elements of each domain are interconnected through two-way communication



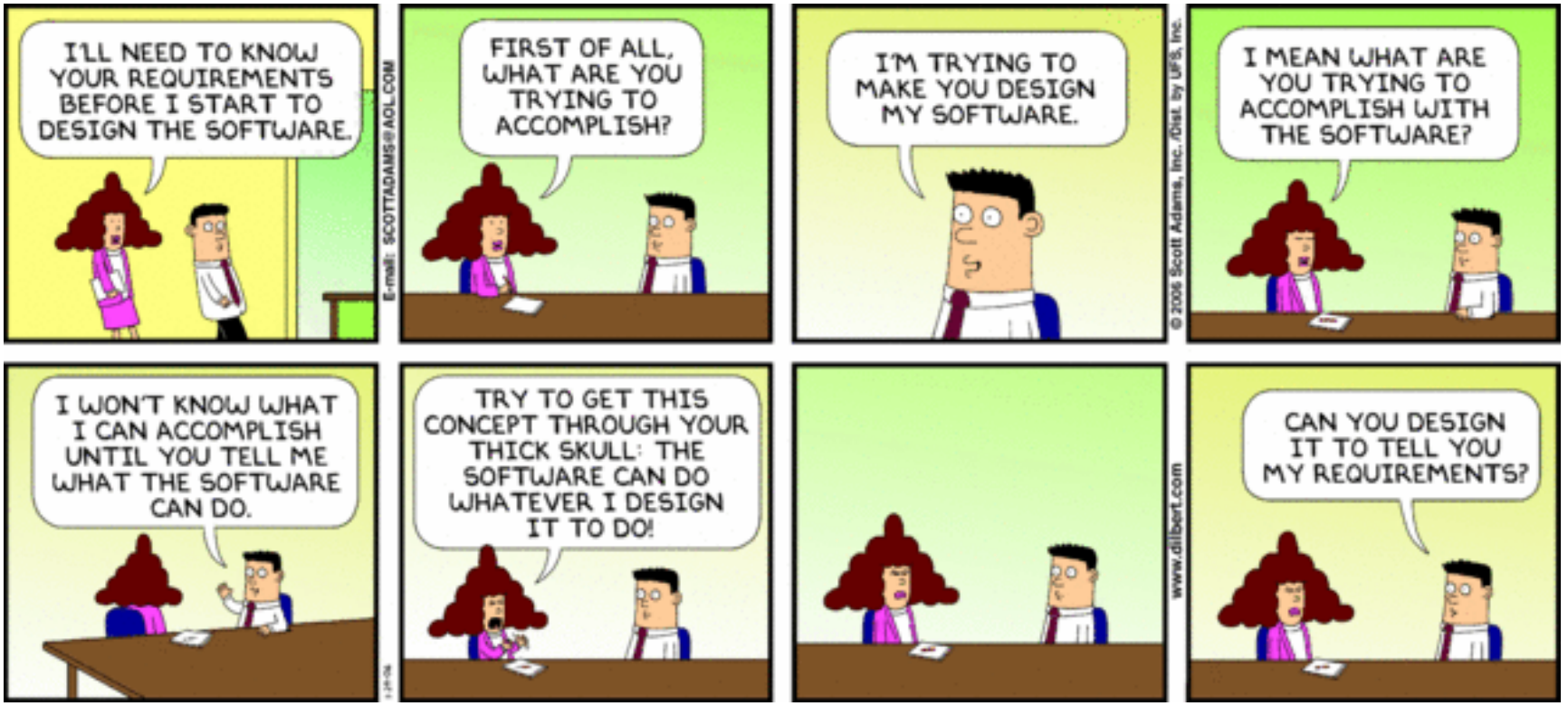
customer

Convergence of TLC and Electrical Networks

NIST: Smart Grid Domains

ECSEL JU

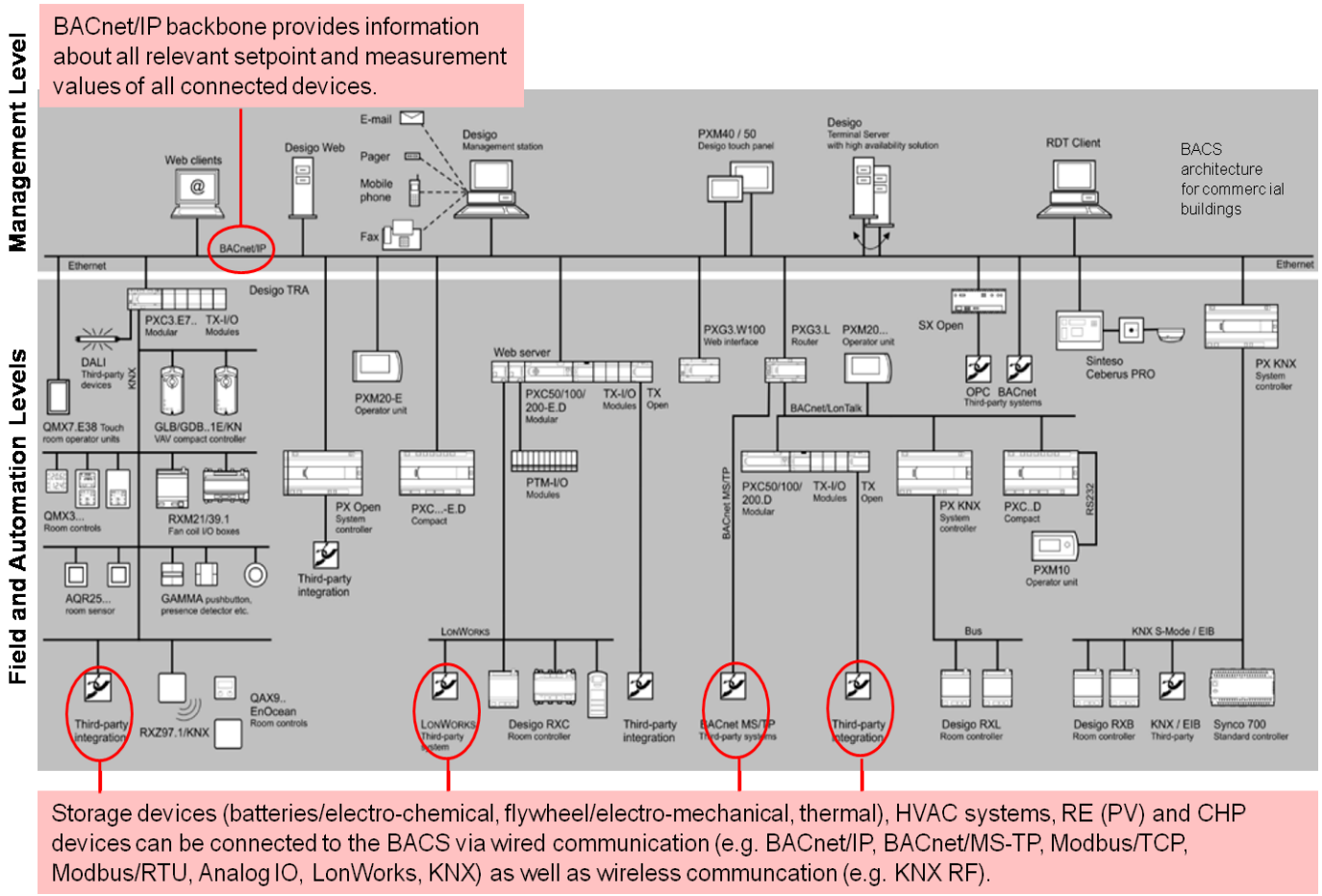
Requirements



ECSEL JU

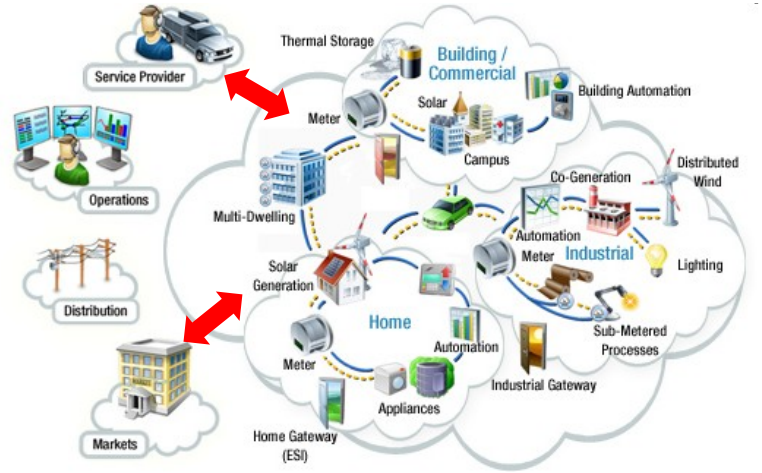
Requirements - State of the Art

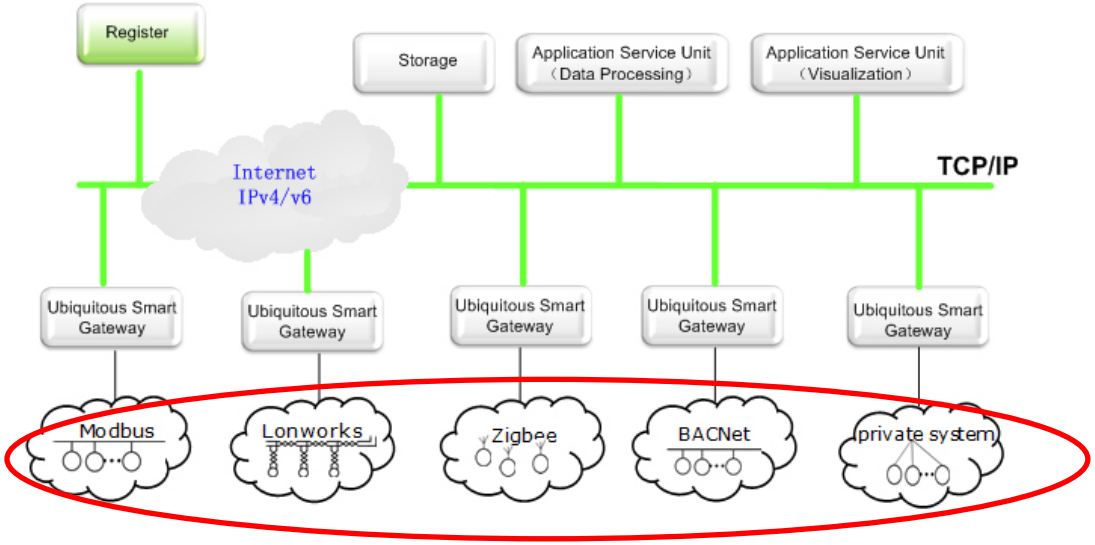
Existing architectures of building automation systems



Storage devices (batteries/electro-chemical, flywheel/electro-mechanical, thermal), HVAC systems, RE (PV) and CHP devices can be connected to the BACS via wired communication (e.g. BACnet/IP, BACnet/MS-TP, Modbus/TCP, Modbus/RTU, Analog IO, LonWorks, KNX) as well as wireless communcation (e.g. KNX RF).

Requirements – beyond S.o.A.



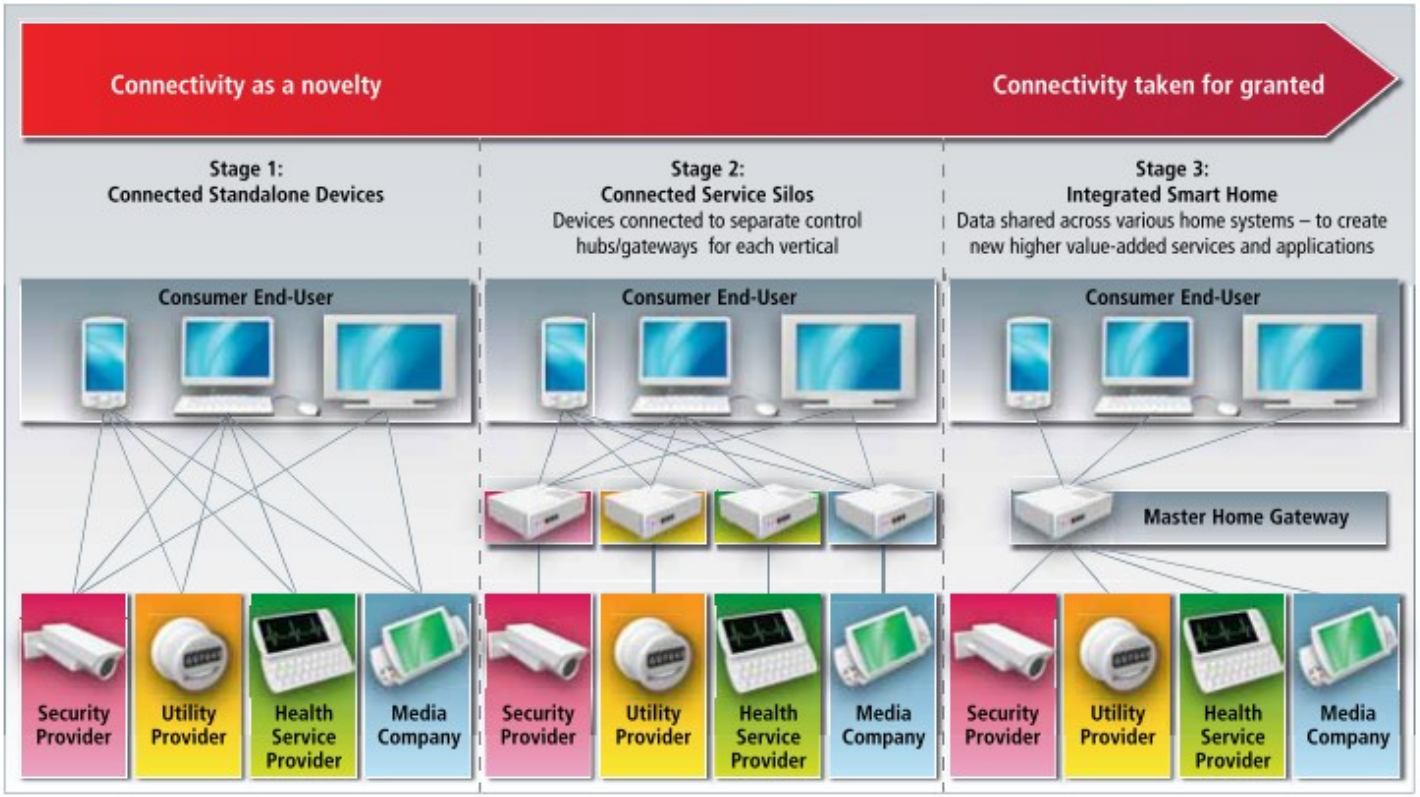


- We are faced with a
  - Heterogeneous System
  - Inter-domain Communication

IEEE 1888:
An Open and Smart Energy Management Architecture based on IoT

Requirements – beyond S.o.A.

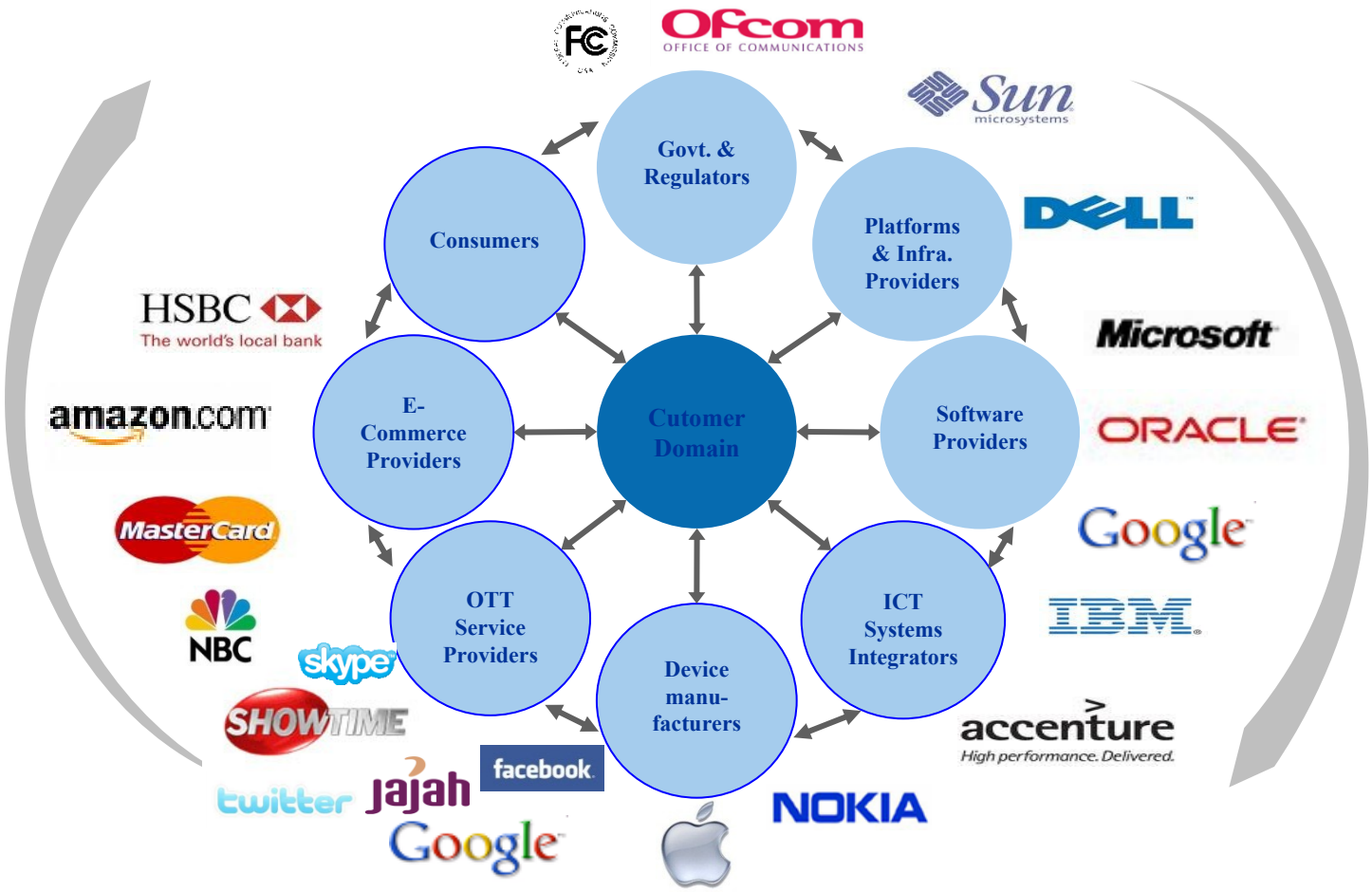
- Security and Privacy
- User Authentication
- On-demand Services
- Scalable QoS
  - Latency
  - Bandwidth
  - Energy



Source: GESMA "Vision of Smart Home"

Requirements

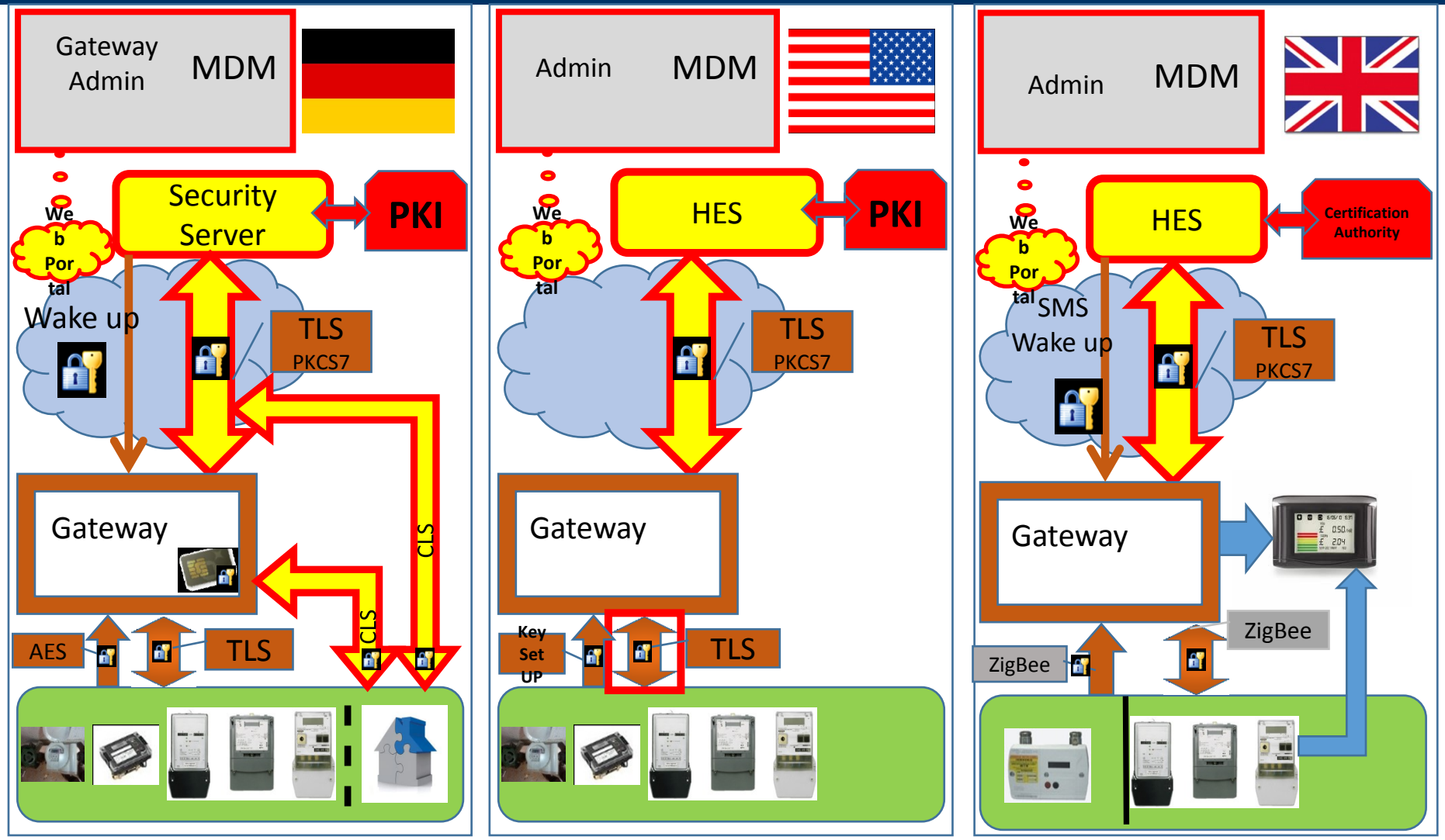
Communications Ecosystem



ECSEL JU

Source: Booz & Company analysis

Solutions - Example Architectures



HES: Headend System
TLS: Transport Layer Security
MDM : Meter Data Management
CLS: Controllable Local System
PKI: Public Key Infrastruktur

ECSEL JU

Solutions - German Protection Profile

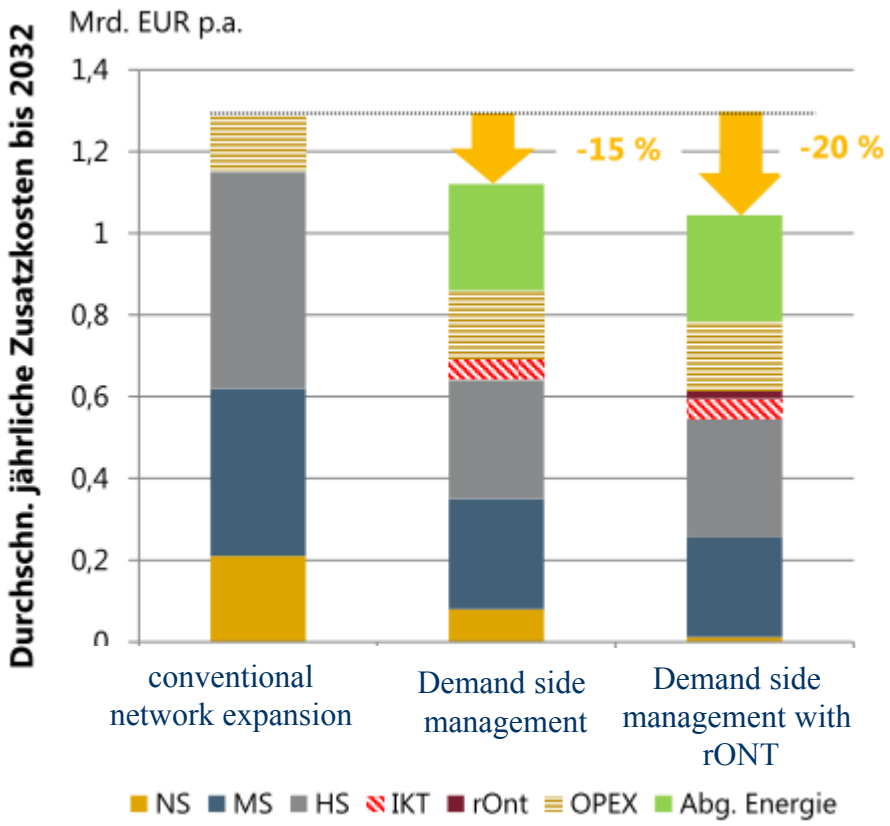
- The MUS with Smart Meter Gateway Protection Profile was intended to be standardized by Common Criteria

- Discussion that new and innovative concepts are cheaper
- VDE DKE
  - Open concept

Moderne Verteilernetze für Deutschland
„Verteilernetzstudie“

rONT: Ortsnetztransformatoren,
transformers for the local distribution system

Verteilnetz: distribution network



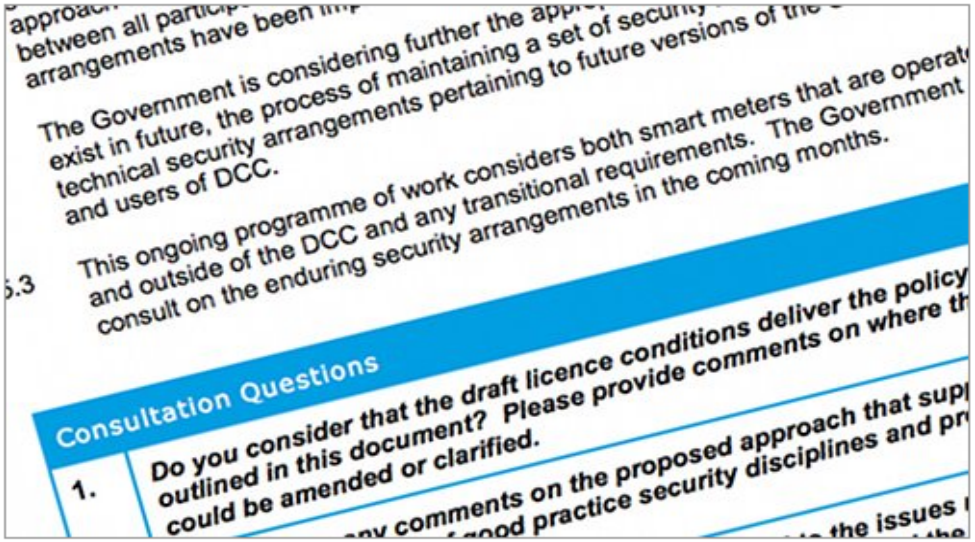
ECSEL JU

Problems

25 June 2012

Smart Meter Security, Risk Assessments and Audits

In another consultation, the UK's Department for Energy and Climate Change (DECC) is asking for views on the draft licence conditions relating to security risk assessments and audits for the UK's smart meter implementation programme.


between all partic
arrangements have been
The Government is considering further the
exist in future, the process of maintaining a set of
technical security arrangements pertaining to future versions of
and users of DCC.
This ongoing programme of work considers both smart meters that are
and outside of the DCC and any transitional requirements. The Government
consult on the enduring security arrangements in the coming months.
5.3
Consultation Questions
1.
Do you consider that the draft licence conditions deliver the policy
outlined in this document? Please provide comments on where
could be amended or clarified.
comments on the proposed approach that
good practice security disciplines and
the issues

The licence conditions will run through to when the planned Data and Communications Company (DCC) becomes responsible for the provision of services. 55 million smart meters will be rolled out to consumers from 2014 through to 2019. The consultation is important in that it sets the precedent for the security of "end-to-end smart metering systems" in the UK. This includes equipment located at consumers' premises, the communications network between the consumers' premises and the energy suppliers, and the the energy suppliers' head end system — and all business procedures associated with the installation, operation and support of the system. The scope is all-encompassing. Additionally the government wants to ensure security is embedded into the design of the systems and that they continue to be for for purpose as risks, technologies and requirements evolve.

The consultation document includes the draft energy supplier licence conditions (in Annex A), and the consultation asks three questions:

- "Do you consider that the draft licence conditions deliver the policy intention outlined in this document? Please provide comments on where the drafting could be amended or clarified.
- Do you have any comments on the proposed approach that suppliers should carry out a number of good practice security disciplines and procedures as is set out in this document?

Problems

1. Information Request

1.1. Introduction

1.1.1. Purpose

This Information Request (IR) has been issued by the Department of Energy and C
Metering Implementation Programme (SMIP) to assess the availability of technolog
Network (HAN) connectivity to electricity and gas metering equipment, communica
in cases where a 2.4GHz ZigBee wireless HAN will not work effectively. *Appendix:*
describes the HAN topology based on 2.4GHz ZigBee wireless technology without

Following evaluation of the IR responses, DECC will determine if the selection of s
further informed through a technology field trial.

In the event that DECC determines that a specific technology trial is required in orc
technology options then such a trial will be run as a separate exercise, participation
future notification and selection process.

DECC may use the responses to this IR, together with the results from any technol
performed, in its analysis of potential HAN technologies and the ultimate selection
technologies. Respondents should note that the process referred to above relates
and is not intended in any way to determine the preferred provider(s) for any such

Responses may include a mix of wired and wireless technologies. Consideration sh
technical solutions that would minimise the requirements to install communications
infrastructure, except at the meter locations and within the consumer's property.

1.1.2. Instructions to respondents

Deadline for submission of responses

Responses should be submitted by 15 April 2013.

1.1.3. Outline of the Problem

HAN Topology

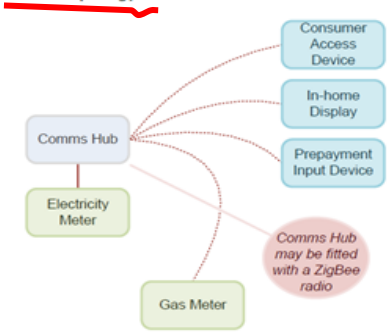


Figure 1: HAN Topology

Information Request

Smart Metering Implementation Programme:
Availability of technologies for provisioning Home Area Network (HAN) connectivity to electricity and gas metering equipment, communications hub and in-home devices in cases where a 2.4GHz ZigBee wireless HAN will not work effectively.

Department of Energy & Climate Change

Smart Metering Implementation Programme

Government response to a consultation on a licence condition for security risk assessments and audits in the period before the DCC provides services to smart meters

ECSEL JU

Problems

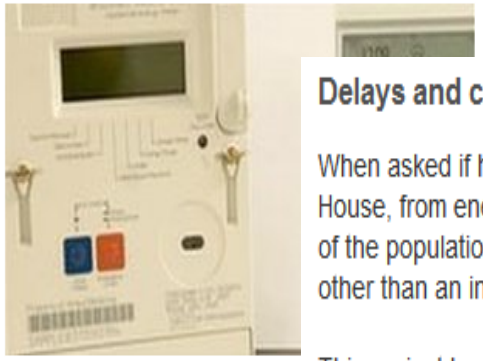
10 May 2013 Last updated at 12:33 GMT

Smart meter project is delayed

The introduction of energy smart meters in 30 million UK homes will be delayed for more than a year, the government has announced.

The £11.7bn project will start in the autumn of 2015, rather than the summer of next year, the Department of Energy and Climate Change (DECC) said.

It said that the industry needed more time to design, build and test the communications system required.



Smart meters show customers h
electricity is being used

Delays and cost over-runs

When asked if he thought the in-home units were good value Tony House, from energy company SSE, said that "for an increasing segment of the population... the benefits are better delivered through something other than an in-home display".

This project has run in to delays, and the main roll-out is now **not expected to begin until 2015**.

Rela

Dr Martyn Thomas, from the Institution of Engineering and Technology, said the new time-frame was "better than the old one", and that the time the project takes should be judged by engineers, not by "politicians or by senior civil servants for political reasons".

He criticised the government for beginning the large-scale trial of the project before a final specification for the smart meters had been agreed, and said that this could cause serious problems when the project went nationwide.

He added that "a typical IT project of this complexity over-runs its declared timescale and cost by 100%".

ECSEL JU

Problems

Smart electricity meters in Puerto Rico made to look foolish

According to a report by US journalist Brian Krebs, the near ubiquity of smart meters in Puerto Rico is matched only by the frequency with which they are hacked. Krebs cites a 2010 FBI report, according to which spot checks by an unnamed electricity supplier found that around one in ten smart meters had been modified. The company estimates the resulting losses at up to $400 million (around €300 million) per year.

According to the FBI, power thieves on the Caribbean island nation, an unincorporated territory of the USA, used optical probes to hack the meters via the infrared maintenance port. Suitable probes are available online for around $400 and are connected to a laptop which runs software to modify the meter's settings. The software needed to carry out the hack is freely available online. The hack does not damage the smart meter hardware or require its removal.

It is also possible to get free electricity from the meters by placing a powerful magnet on the devices, the FBI says. Some customers use this method to disable the meters at night when running power-hungry air-conditioning units, ensuring a cool night-time environment. The magnets are then removed during the day when the customer is out at work. This can reduce the electricity metered by up to 75 per cent. Because the meters continue to send readings to the supplier at regular intervals, the fraud is not easily detected.

According to the FBI report, criminals are charging domestic users $300 to $1000 to have their meters hacked, rising to around $3000 for commercial customers. The FBI believes that former employees of the smart meter supplier and of the electricity company are cashing in by hacking the meters and by selling their knowledge to others.

The FBI report does not give the name of the electricity supplier involved, but according to Krebs it can only be Puerto Rico's largest power company, the state-owned Puerto Rico Electric Power Authority (PREPA). The company reports that it has been installing remotely readable smart meters since 1992.

Problems

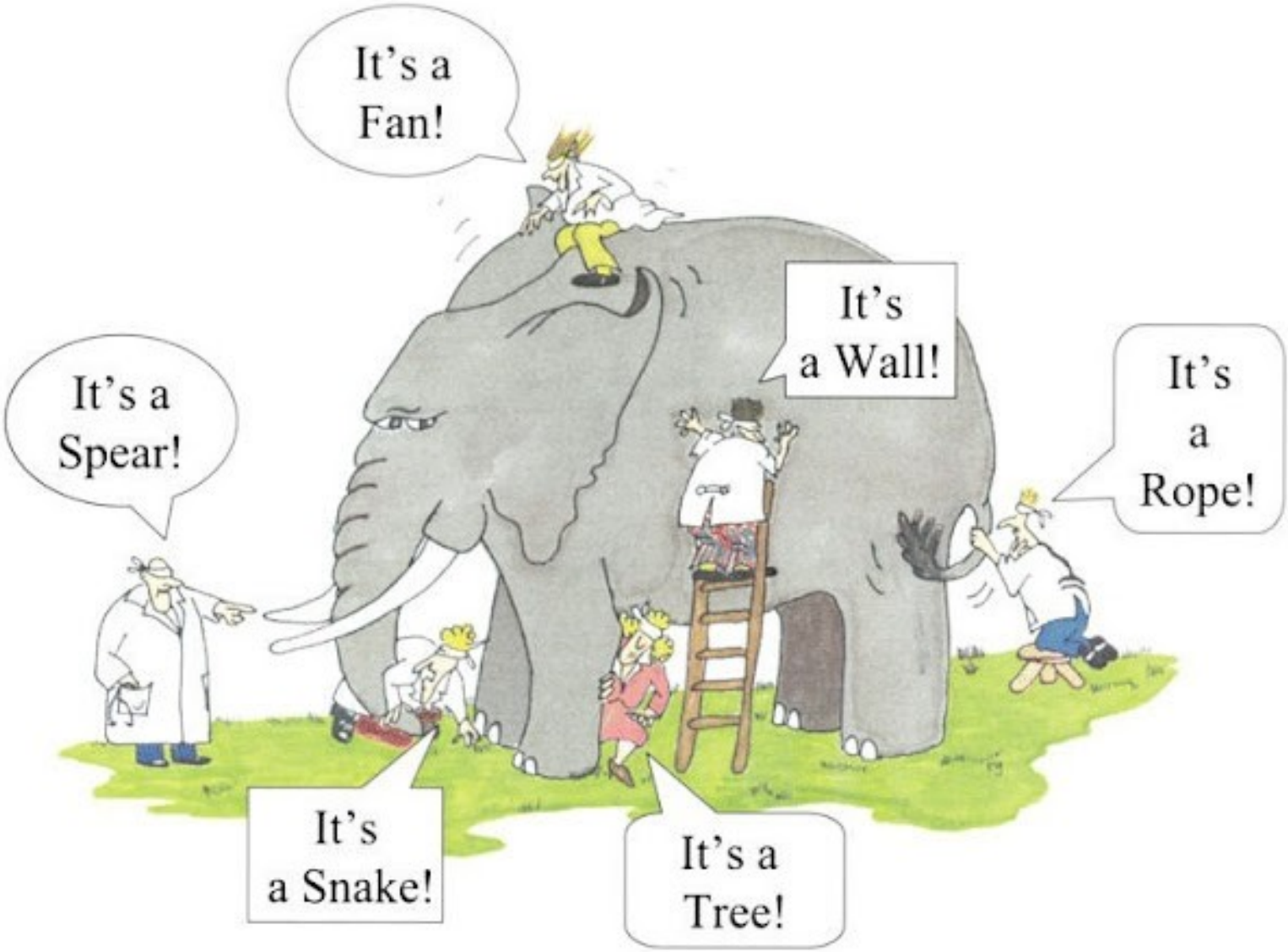
"The FBI assesses with medium confidence that as Smart Grid use continues to spread throughout the country, this type of fraud will also spread because of the ease of intrusion and the economic benefit to both the hacker and the electric customer," the agency said in its bulletin.

The feds estimate that the Puerto Rican utility's losses from the smart meter fraud could reach $400 million annually. The FBI didn't say which meter technology or utility was affected, but the only power company in Puerto Rico with anywhere near that volume of business is the publicly-owned Puerto Rican Electric Power Authority (PREPA). The company did not respond to requests for comment on this story. The hacks described by the FBI do not work remotely, and require miscreants to have physical access to the devices. They succeed because many smart meter devices deployed today do little to obfuscate the credentials needed to change their settings, said according to Tom Liston and Don Weber, analysts with InGuardians Inc., a security consultancy based in Washington, D.C. Liston and Weber have developed a prototype of a tool and software program that lets anyone access the memory of a vulnerable smart meter device and intercept the credentials used to administer it. Weber said the toolkit relies in part on a device called an optical probe, which can be made for about $150 in parts, or purchased off the Internet for roughly $300. "This is a well-known and common issue, one that we've warning people about for three years now, where some of these smart meter devices implement unencrypted memory," Weber said. "If you know where and how to look for it, you can gather the security code from the device, because it passes them unencrypted from one component of the device to another."

ECSEL JU

THE H SECURITY

Standards



ECSEL JU

Standards - IEC CEN-CENELEC ETSI

- Smart Grid Coordination Group
  - Smart Grid Report “Set of Standards”
  - Released version to SG-CG stakeholders for review
  - New Set of Standards planed to be published by the E of 2015

SGCG/M490/B_Smart Grid Report
Set of standards
Version 3.0
August 28th 2014

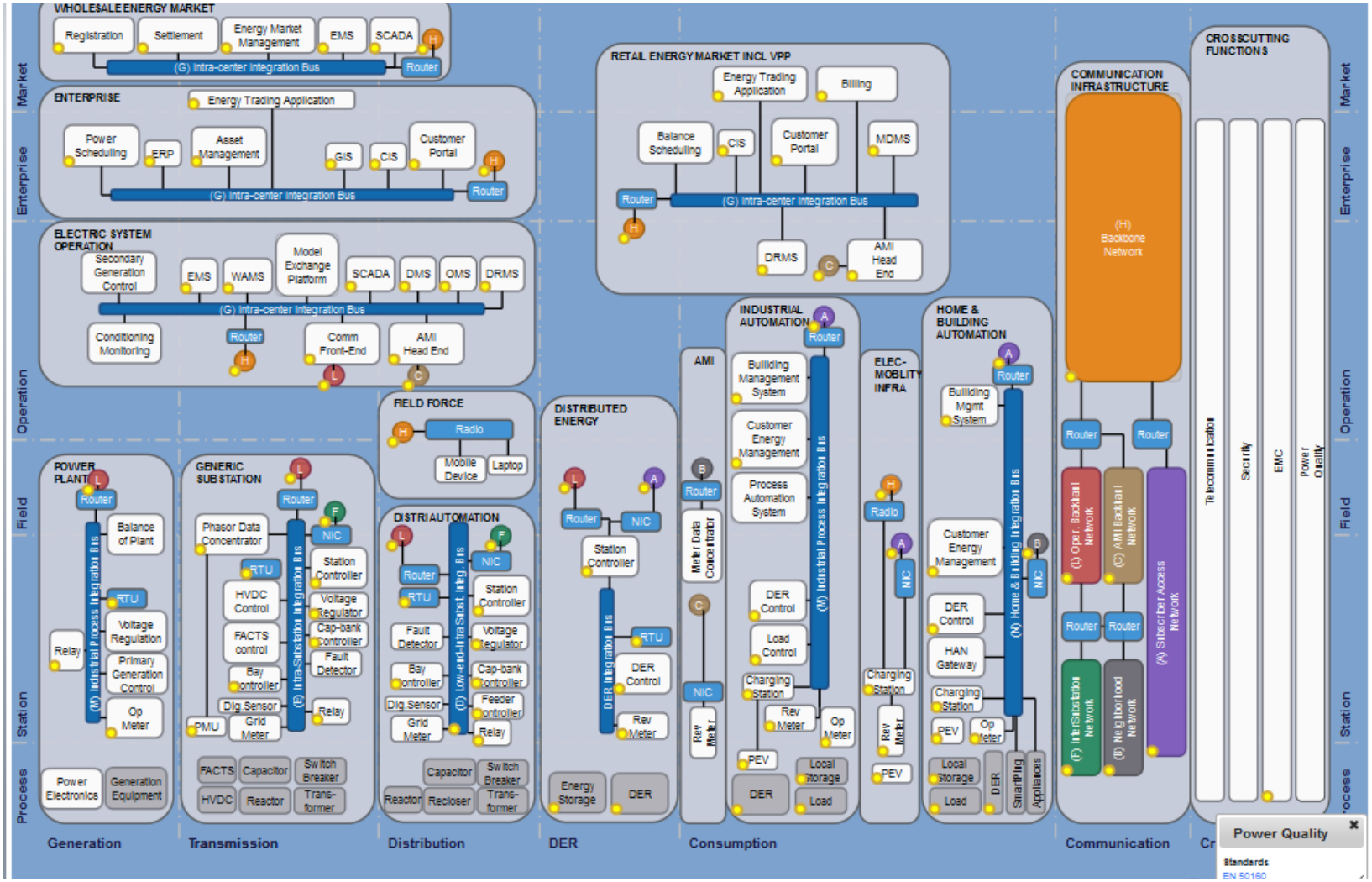
ECSEL JU

Feedback until Oct. 7. 2014

Standards - IEC CEN-CENELEC ETSI

http://smartgridstandardsmap.com/

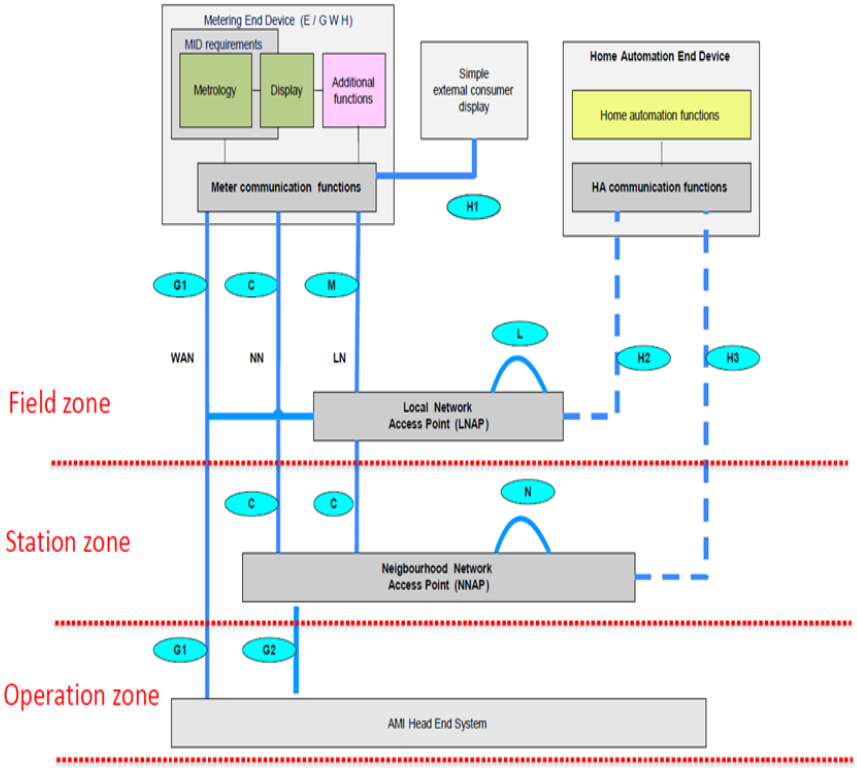
Covers the SGAM model

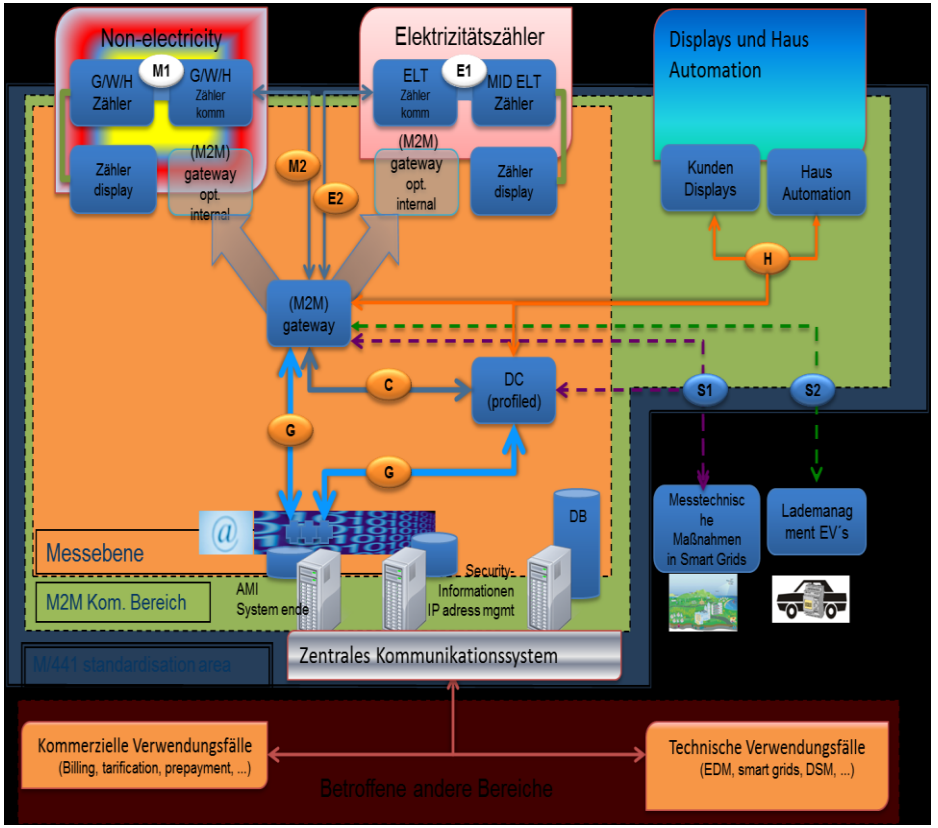


ECSEL JU

Standards - IEC CEN-CENELEC ETSI

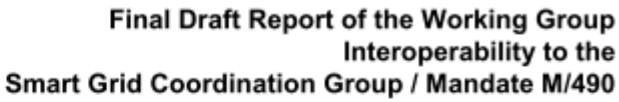
- "Set of Standards"
  - Reference Smart Metering architecture according to CLC TR 50572





Standards - IEC CEN-CENELEC ETSI

- Smart Grid Coordination Group
  - SGCG - Final Draft Report of the Working Group Interoperability to the Smart Grid Coordination Group
  - Survey: Highest Priority for Distribution Automation
    - Interoperability
    - Standardization



Final Draft Report of the Working Group Interoperability to the
Smart Grid Coordination Group / Mandate M/490

ECSEL JU

Feedback until Oct. 7. 2014

Standards - IEC CEN-CENELEC ETSI

- Smart Grid Coordination Group
  - Smart Grid Information Security

Smart Grid Coordination Group
Document for the M/490 Mandate
Smart Grid Information Security

Conclusion:
It should be noted, that cyber security is a continuous effort and cannot be handled in one shot only. Neither can be a 100 % security achieved.
Cyber security is a journey, not a destination.

Feedback until Oct. 7. 2014

Standards - IEC CEN-CENELEC ETSI

- Smart Grid Coordination Group
  - Report about Smart Charging of Electric Vehicles in relation to Smart Grid
    - This report is a result of work made by a working group under the CEN -CENELEC eMobility Coordination Group (EM-CG) and the CEN-CENELEC-ETSI Smart Grid Coordination Group (SG-CG), with the purpose of documenting different aspects of Electro Mobility Smart Charging.
  - Study Report on Electromagnetic Interference between Electrical Equipment/Systems in the Frequency Range below 150 kHz
    - Study Report on Electromagnetic Interference between Electrical Equipment/Systems in the Frequency Range below 150 kHz
    - Investigations in CENELEC SC 205A
    - Power Supplies as EMI Sources
    - Aging of Components is one of the Key Reasons for EMI

Standards - ITU-T

Smart Grid
Standardization Overview and Work Plan
April 2014 SG15 meeting
Contact persons for project updates:

Study Group 15 Counsellor Mr. Greg Jones International Telecommunication Union (ITU) Place des Nations 1211 Geneva 20 Switzerland Tel.: +41 22 730 5515 Fax: +41 22 730 5853 E-mail: greg.jones@itu.int	Study Group 15 Chairman Mr. Stephen J. Trowbridge Alcatel-Lucent 5280 Centennial Trail Boulder Colorado 80303-1262 USA Tel: +1 720 945 6885 E-mail: Steve.Trowbridge@alcatel-lucent.com	Question 15/15 Rapporteur Mr. Stefano Galli ASSIA, Inc. 333 Twin Dolphin Dr. Redwood City, CA 94065 USA Tel: +1 650-801-4120 Mobile: +1 917-532-4468 Email: sgalli@assia-inc.com

ECSEL JU

Standards - ITU-T

Items	SGs and aspects	
(1) M2M	SG13	Q3/13 USN, MOC QA/13 (currently Q3/13) Requirements for NGN evolution (NGN-e) and its capabilities including support of IoT QC/13 (currently Q5/13) Functional architecture for NGN evolution (NGN-e) including support of IoT Q12/13 Ubiquitous networking (object to object communication)
	SG15	Q1/15 IP home network and gateway
	SG16	Q25/16 USN applications and services
(2) Smart metering	SG15	Q15/15: PHY/DLL aspects of smart metering
(3) Vehicle communication	SG13	Q12/13 networked vehicle
	SG16	Q27/16 Vehicle gateway platform for telecommunication/ITS services /applications
(4) Access and home networking	SG9	Q5/9 Functional requirements for a universal integrated receiver or set-top box for the reception of advanced content distribution services Q9/9 The extension of network-based content distribution services over broadband in Home Networks
	SG13	Q12/13 Next generation home network
	SG15	Q1 IP home network and access network transport Q15/15: Smart Home (home networking related Smart Grid communications) Q18/15 Broadband in-premises networking
	SG16	Q21/16 home network services
(5) Energy saving network	SG13	QN/13 (split from Q21/13) Environmental and socio-economic sustainability in Future Networks and early realization of FN Q12/13 Evolution towards integrated multi-service networks and interworking
(6) Smart Grid Communications	SG15	Q15/15: various aspects related to Smart Grid Communications, from physical layer to transport of higher layer protocols
(7) Security	SG17	Q6/17 Security functional architecture for smart grid services using telecommunication network
(8) Climate change	SG5	Mitigation of climate change and improving energy efficiency

Standards - ITU-T

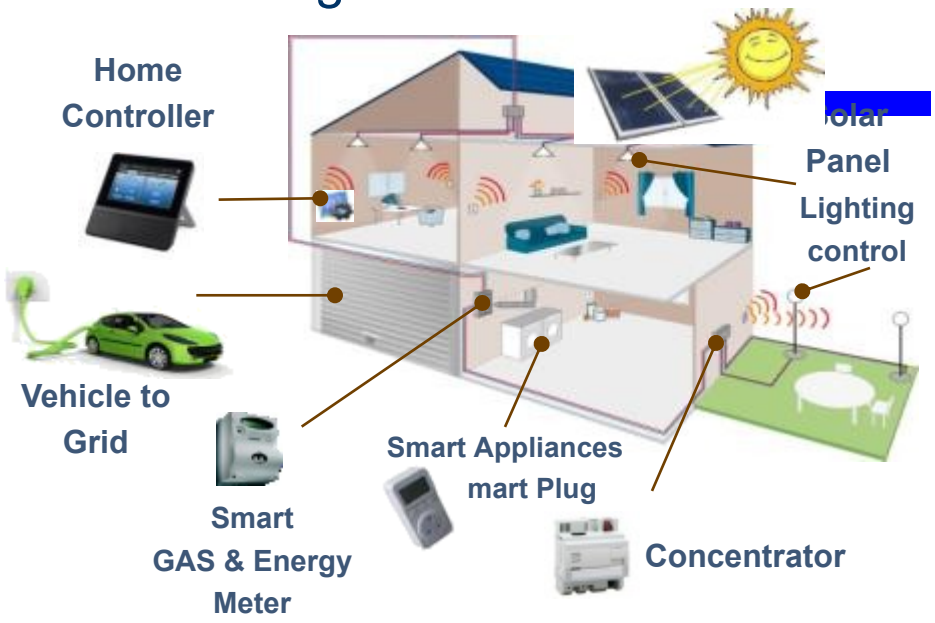
Q15/15 Recommendations related to Smart Grid Communications

Rec. No.	Title	Status	Date
G.9955 (2011)	Narrowband OFDM Power Line Communication Transceivers – Physical Layer Specification	Approved (To be deleted; superseded by G.9902, G.9903, G.9904)	12/2011
G.9956 (2011)	Narrowband OFDM Power Line Communication Transceivers – Data Link Layer Specification	Approved (To be deleted; superseded by G.9902, G.9903, G.9904)	11/2011
G.9901 (2014)	Narrow-band OFDM power line communication transceivers - Power spectral density specification	Approved	11/2012
G.9902 (2012)	Narrow-band OFDM power line communication transceivers for ITU-T G.hnem networks	Approved	10/2012
G.9903 (2014)	Narrow-band OFDM power line communication transceivers for G3-PLC networks	Approved	02/2014
G.9904 (2012)	Narrow-band OFDM power line communication transceivers for PRIME networks	Approved	10/2012
G.9905 (2013)	Centralized metric based source routing	Approved	08/2013
G.9959 (2012)	Short range narrowband digital radiocommunication transceivers – PHY & MAC layer specifications	Approved	02/2012
G.shp6	Smart Home profiles based on 6LoWPAN	Work in progress	

Standards - IEEE CSHBA

- IEEE-SA Industry Connections - CSHBA
  Convergence of Smart Home and Building Architectures

There are striking similarities among the communications network architectures of smart home and building environments as they relate to applications including electric vehicle, home or building energy management, infotainment, etc. However, a gap exists for interworking among these various domains.



Although today users are able to access many domains through their TVs, smart phones and tablets, an effort is needed to enable seamless user experience that spans multiple application domains.

ECSEL JU

Standard for an Architectural Framework for the Internet of Things (IoT)

IEEE P2413

Standards - IEEE P2413

- P2413 Purpose & Motivation
  - The Internet of Things (IoT) is a key enabler for many emerging and future “smart” applications and technology shifts in various technology markets. This ranges from the Connected Consumer to Smart Home & Buildings, E-Health, Smart Grids, Next Generation Manufacturing and Smart Cities. It is therefore predicted to become one of the most significant drivers of growth in these markets.
  - Most current standardization activities are confined to very specific verticals and stakeholder groups. They therefore represent islands of disjointed and often redundant development. The architectural framework defined in this standard will promote cross-domain interaction, aid system interoperability and functional compatibility, and further fuel the growth of the IoT market.

Standards - IEEE P2413 Scope

- This standard defines an architectural framework for the 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:
  - reference model that defines relationships among various IoT verticals (e.g., transportation, healthcare, etc.) and common architecture elements
  - blueprint for data abstraction and the quality "quadruple" trust that includes protection, security, privacy, and safety.”
- The architectural framework for IoT also provides a reference architecture that:
  - builds upon the reference model
  - defines basic architectural building blocks and their ability to be integrated into multi-tiered systems.
  - addresses how to document and, if desired, mitigate architecture divergence.

ECSEL JU

Standards - IEEE P2413 PAR

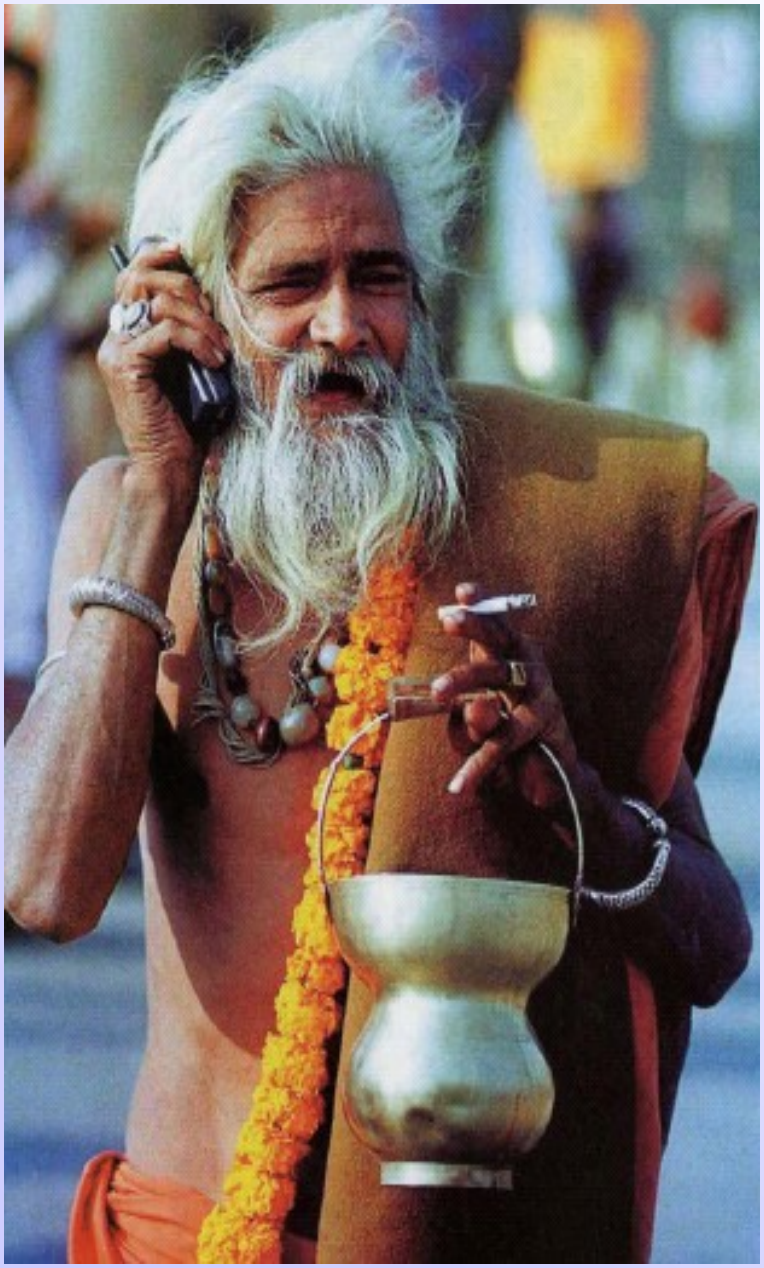
- 5.2 Scope: This standard defines an architectural framework for the Internet of Things (IoT), including descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains. The architectural framework for IoT provides a reference 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 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.
- 5.4 Purpose: The Internet of Things (IoT) is predicted to become one of the most significant drivers of growth in various technology markets. Most current standardization activities are confined to very specific verticals and represent islands of disjointed and often redundant development. The architectural framework defined in this standard will promote cross-domain interaction, aid system interoperability and functional compatibility, and further fuel the growth of the IoT market. The adoption of a unified approach to the development of IoT systems will reduce industry fragmentation and create a critical mass of multi-stakeholder activities around the world.
- 5.5 Need for the Project: This standard will help to reduce current fragmentation in the various IoT verticals. By addressing the need for an IoT architectural framework, IEEE will fulfill its mission to benefit humanity by increasing the interoperability and portability of IoT solutions to both the industry and the end consumer.

PAR: Project Authorization Request

ECSEL JU

Summary

- There are a lot of Activities:
  - IEC, CEN-CENELC, ETSI, NIST, ITU …
- There a lot of Standards but different Implementations
- Future Work:
  - Coexistence and Interoperability are still Issues
  - Certification of IoE Devices
  - Lack of standardized Data Models, Objects and according Standards
  - Standards for Security and Privacy by Design



Thank you for your attention…

We need to contact many TCs, SCs and industry groups to make an ecosystem around us to minimize unnecessary competition.

Greg Jones
Study Group 15 Counsellor
International Telecommunication Union

Backup

ECSEL JU

Introduction: Lantiq at a Glance

Key Facts

~800 employees
Broadband industry leader
100M+ chips shipped/year
Fabless

Markets Served

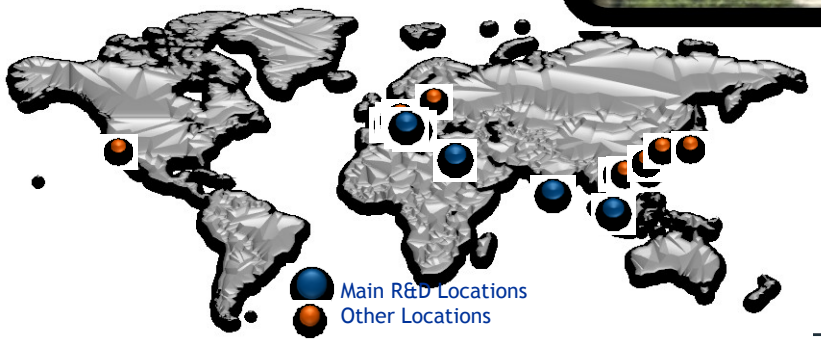
- Broadband Access Networ
- Voice Products
- Giga Home Gateways

Continuous Innovation

- 70% R&D employees
- Strong IP position: 2,000+ patents
- Premier customer base
- Very active in standards committees

Global Presence

Locations



ECSEL JU

Release/Patent P&P

- Release: The contributor acknowledges and accepts that this contribution is subject to the IEEE Copyright policies as stated in the IEEE-SA Standards Board Bylaws, section 7, http://http://standards.ieee.org/develop/policies/bylaws/sect6-7.html#7
- Patent Policy and Procedures: The contributor is familiar with the IEEE Patent Policy and Procedures <http://standards.ieee.org/guides/bylaws/sect6-7.html#6>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the IEEE of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the chair of the IEEE P2413 Working Group, Oleg Logvinov, <oleg.logvinov@st.com>, as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE P2413 Working Group. If you have questions, contact the IEEE Patent Committee Administrator at <patcom@ieee.org>.

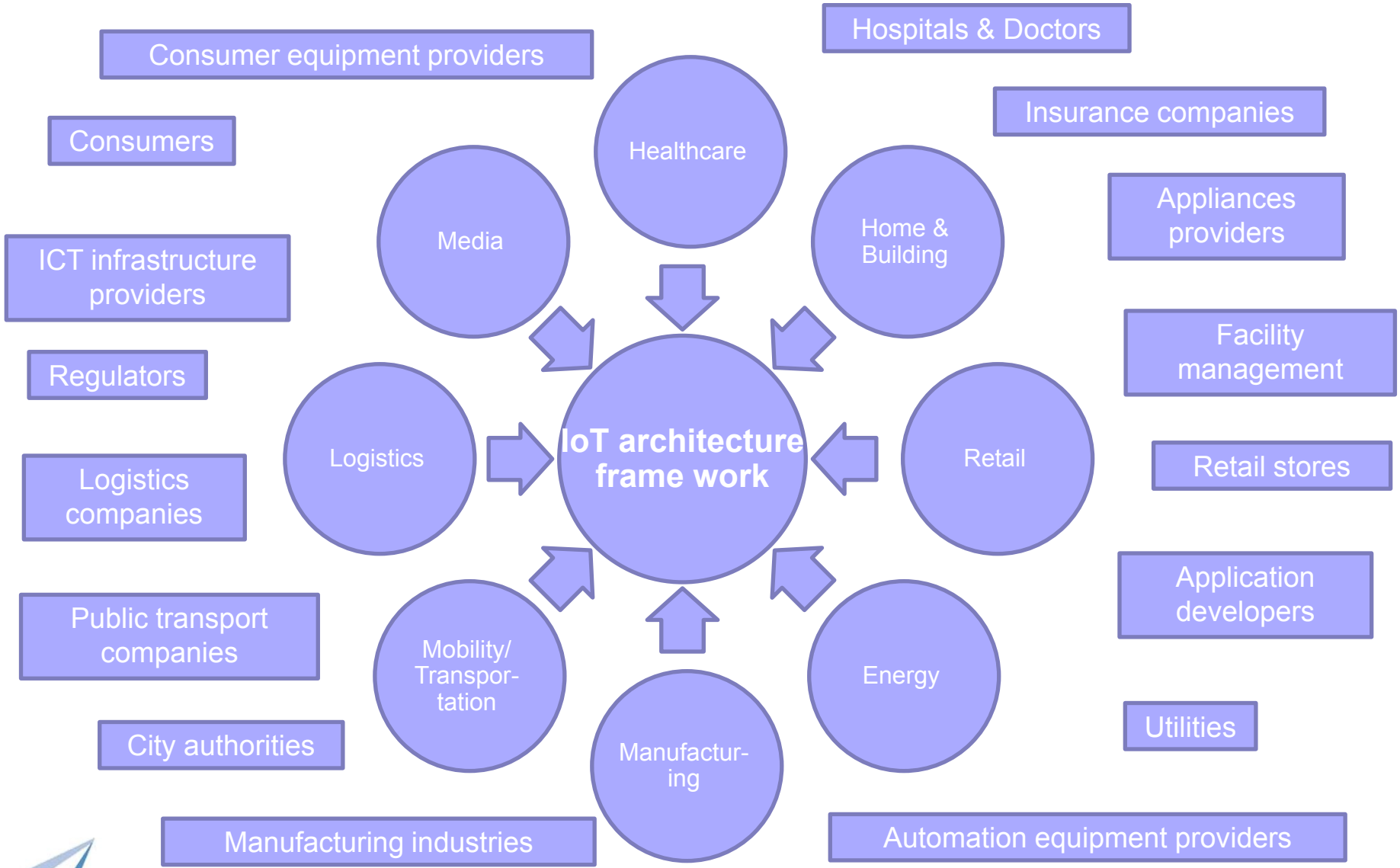
IEEE P2413

Architectural Framework for the Internet of Things (IoT)

Standard for an Architectural Framework for the Internet of Things (IoT) Introduction				
Date: 2014-07-10				
Author(s):				
Name	**Company**	**Address**	**Phone**	**email**
Oleg Logvinov	STMicroelectronics	220 Old New Brunswick Rd, Piscatway , NJ 08854, USA	+1 732 322 0155	Oleg.logvinov @st.com

ECSEL JU

IoT Markets & Stakeholders*



ECSEL JU

IEEE P2413 External interactions

- For a unified IoT architecture framework it is essential to interact with standardization activities for IoT-based vertical applications to
  - Cover the various applications, their requirements and specific IoT functionalities in the IoT architecture framework
  - Ensure that the framework can be referenced by these standardization activities as the base for their specific architecture definition
- Besides interactions with standardization activities within IEEE, P2413 will strive to establish liaisons with other standardization bodies like IEC (e.g. Smart Manufacturing, Smart Grid) and ISO (e.g. Intelligent Transportation Systems, e-Health) on IoT matters.

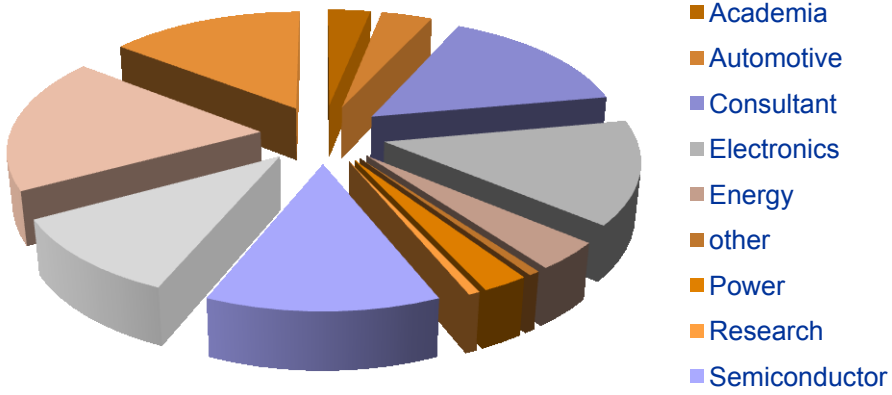
IEEE P2413 Goals

- Define an IoT architecture framework that covers the architectural needs of the various IoT application areas
- Promote cross-domain interaction by increasing system interoperability and functional exchangeability to further fuel the growth of the IoT-based application market
- Increase the transparency of system architectures to support system benchmarking, safety, and security assessments
- Reduce industry fragmentation and create a critical mass of multi-stakeholder activities around the world

ECSEL JU

IEEE Standards Association (IEEE-SA) Internet of Things (IoT) Workshop

- **18-19 September 2014**
  Computer History Museum
  in Mountain View, California, in the heart of Silicon Valley
- **Two-day workshop**
- **2013 Workshop: 227 Attendees**
- **A combination of panel sessions and keynote speeches, along with product showcases**
- **A dedicated session for**
  IEEE P2413



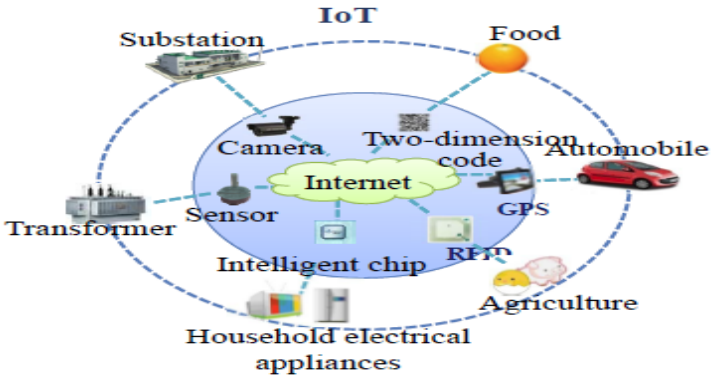
ECSEL JU

IoT Pervasiveness

IEEE STANDARDS ASSOCIATION IEEE

Concept of IoT

The basic idea of IoT is the pervasive presence around us of a variety of things or objects – like Radio-Frequency Identification tags, sensors, actuators, mobile phones, etc. –which, through information and communication network, are able to exchange information with each other and to be intelligently processed.

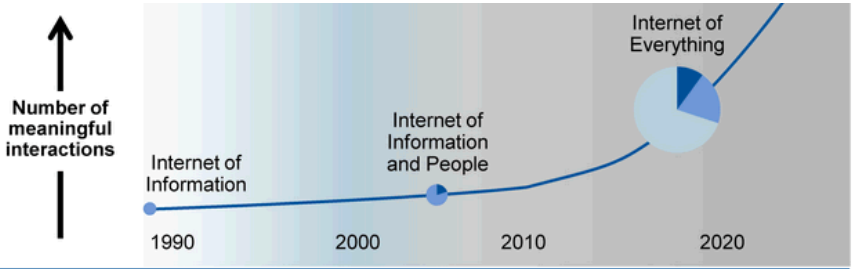


Three-tier architecture

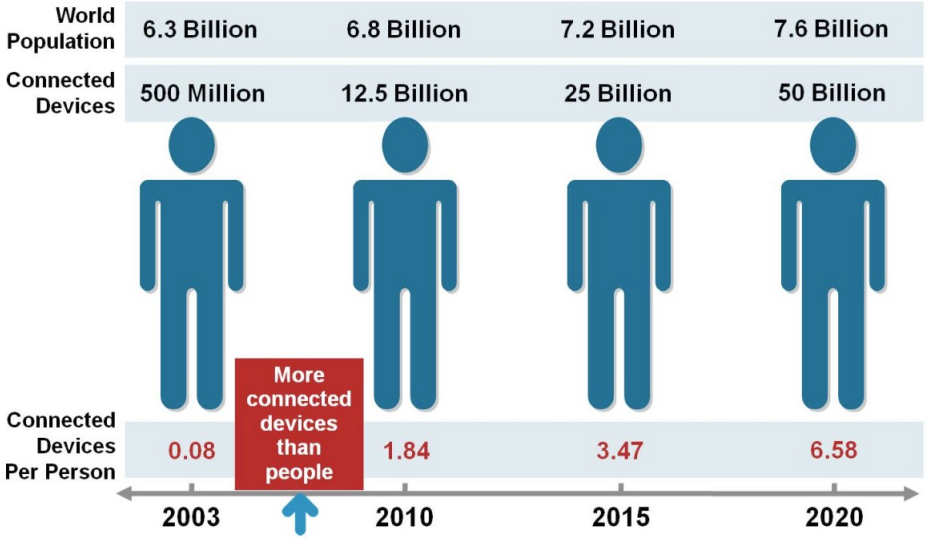
Application layer
Information storage , processing and visualization .

Network layer
Information transfer and routing control .

Sensing layer
Intelligence sensing, smart identification and information collection of the physical world.



Key milestones	> 50% of Internet connections are things	Things create more traffic than information and people
Number of permanently Internet-connected devices	> 15 billion	> 30 billion
Number of intermittently Internet-connected devices	> 50 billion	> 200 billion
Volume of traffic from things	Minority	Majority



ECSEL JU

Join us!

Join the IEEE P2413 Working Group
http://grouper.ieee.org/groups/2413/

For additional information, please contact:
Oleg Logvinov
P2413 Chair
oleg.logvinov@st.com
or
Brenda Mancuso
IEEE-SA Project Manager
blmancuso@ieee.org

ECSEL JU

Environments

- Security & Privacy
- (Cyber-Crime / war / Teror, acceptance and support of the residents'> NSA .....)

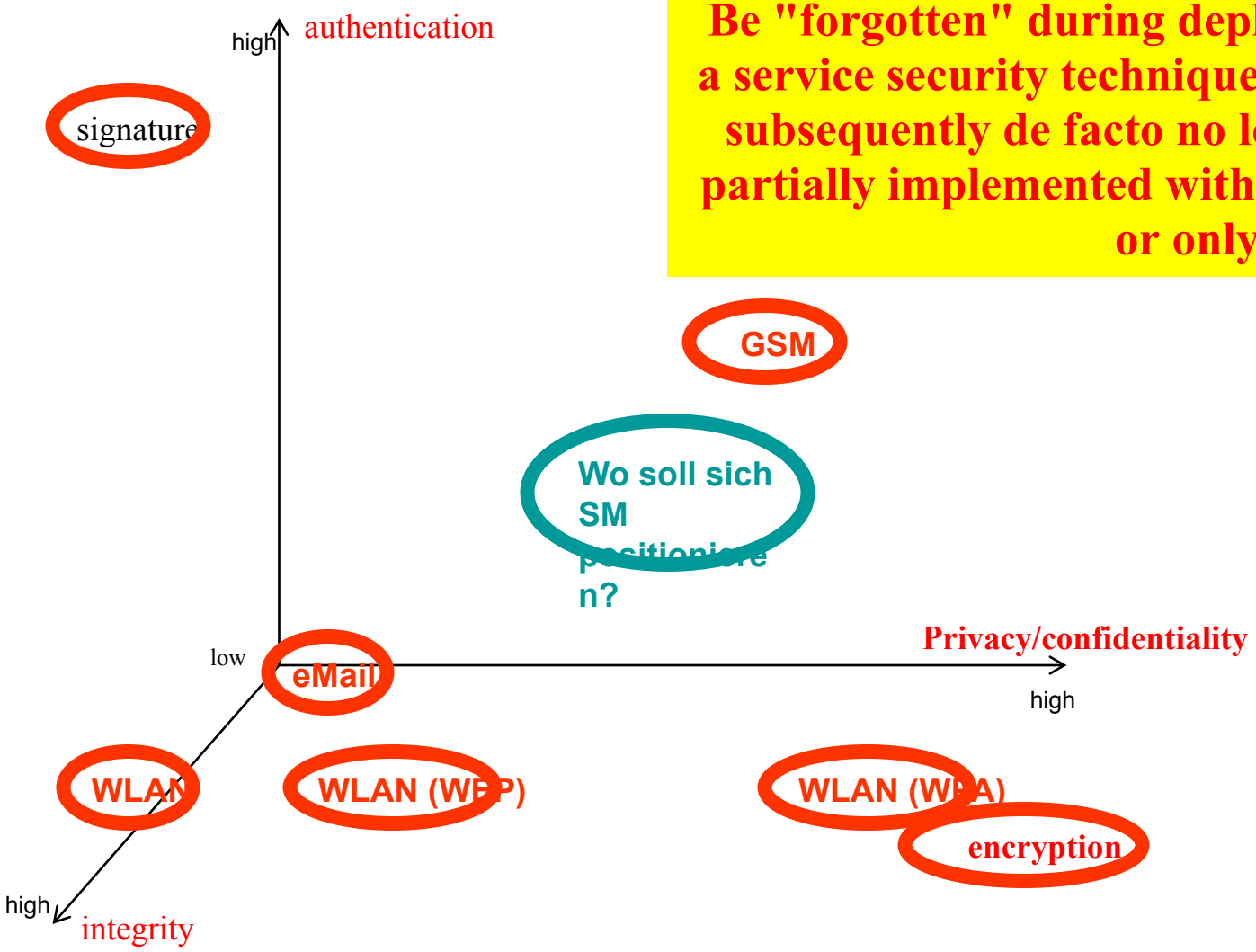
Smart City require a large number of sensors and actuators

- Minimum amount of energy required by Ultra Low Power Technologien->
- enables
- Basis for energy harvesting and battery operation over long periods of time> 10 years
- Economic installation (no wiring no permanent energy costs)

Smart City require a large number of sensors and actuators

- High data density on business processes and on all data transport routes.
- Especially big challange the "first" hop on the field level (communication Sensors Actuators) since there is only a limited number of parties available technologies (radio frequencies and economically possible cabling systems!)
- The co-existence of many different systems must be guaranteed from the outset by concepts both in terms of high number of data points and by Stepwise exchange through technology inovations. Example mobile GSM-GPRS-UMTS-LTE not disturb neither to physical nor logical level!

Safety consequences



Be "forgotten" during deployment of a service security techniques, they are subsequently de facto no longer only partially implemented with high costs or only uncertain

ECSEL JU

Common Criteria for Information Technology Security Evaluation

international standard ISO IEC

computer security

Common Criteria is a framework in which computer system users can specify their security
functional and assurance requirements (SFRs and SARs respectively) through the use of Protection Profiles (PPs), vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to
determine if they actually meet the claims. In other words, Common Criteria provides
assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

Common Criteria is used as the basis for a Government driven certification scheme and typically evaluations are conducted for the use of Federal Government agencies and critical infrastructure

http://www.commoncriteriaportal.org/

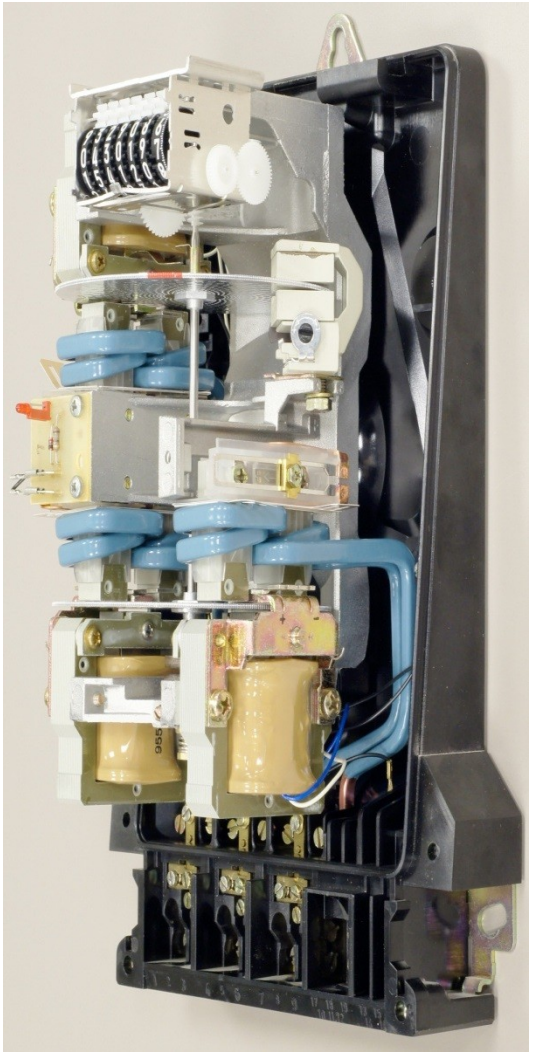
Contents

Source: http://www.commoncriteriaportal.org/

http://en.wikipedia.org/wiki/Common_Criteria

Consumption Ferraris counters

- 1-Phase (2 Wire):
  - Voltage Circuit 3.9 VA
  - Current Circuit 0.35 VA
  - **Total: 4.25 VA (37.23 kWh/y)**
- 3-Phase:
  - Voltage Circuit 6 VA
  - Current Circuit 3 x 0.5 VA = 1.5 VA
  - **Total: 7.5 VA**



ECSEL JU

Real-world electronic meters

- 1-Phase (2 Wire):
  - Voltage Circuit 0.3 W – 0.5 W
  - Current Circuit 0.01 W - 0.02 W
  - **Total:** **0.31 W – 0.52 W**
    (2.7 kWh/y – 4.5 kWh/

- 3-Phase:
  - Voltage Circuit 3 x 0.5 W = 1.5 W
  - Current Circuit 3 x 0.01 W = 0.03 W
  - **Total:** **1.53 W**
    (13.4 kWh/y)
- Data above was taken from the data sheets of actual meters in production

ECSEL JU

Summary

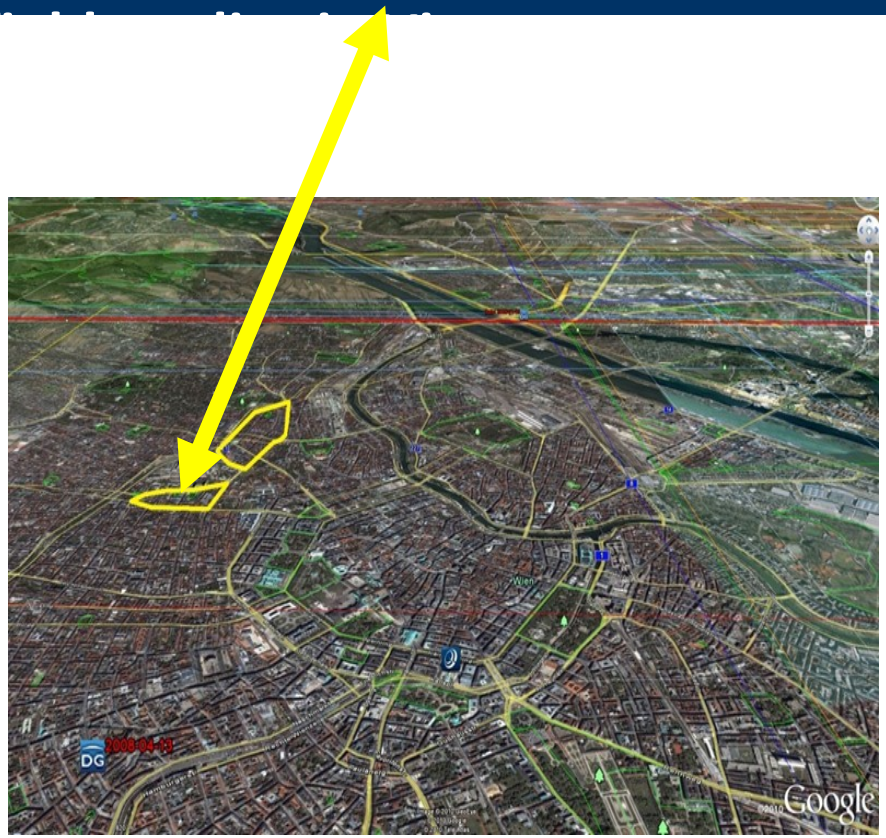
- The electronic electricity counter consumes less energy than the old fashioned Ferraris counter.
  - Meter itself consumes only 13.4 kWh/y against the previous 65.7 kWh/y
  - Its power consumption is easily outpaced by the consumption of the communication interfaces.
- The “smartness” of the meter increases the power consumption eventually to a point, where the new system consumes more energy than the old system.
  - A full featured smart meter might take about 8 kWh/y more
- Power consumption of a smart meter heavily depends on:
  - The amount of data transferred
  - The number of transmissions per day (96 ?)

Smart City‘s ensely populated areas Conditions ->Findings from

Up to 10.000 devices may, under favorable conditions, be inside listening distance.

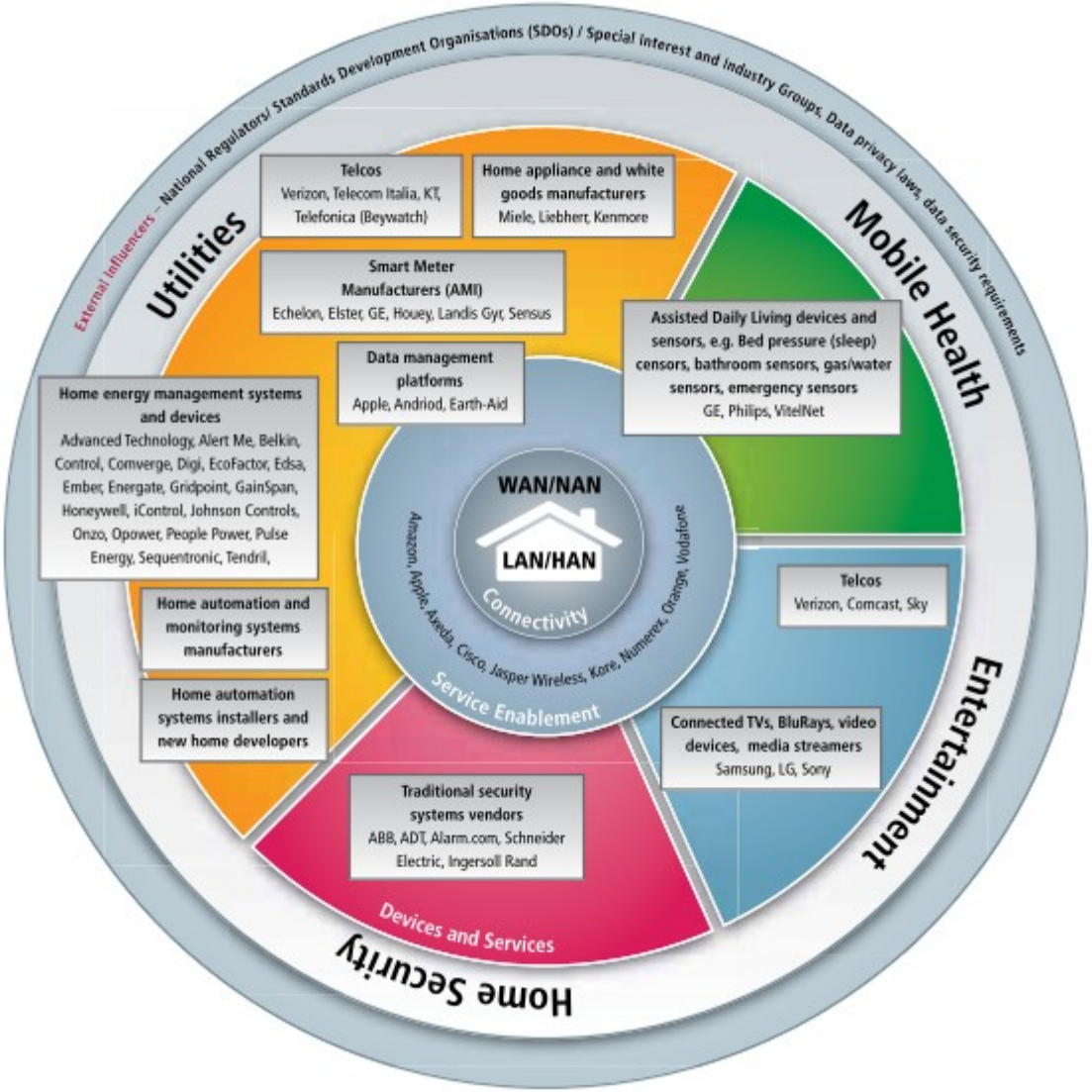
Proposal:

- Reduce transmission duration time by (Mesh networking ?)
- additional frequency band



ECSEL JU

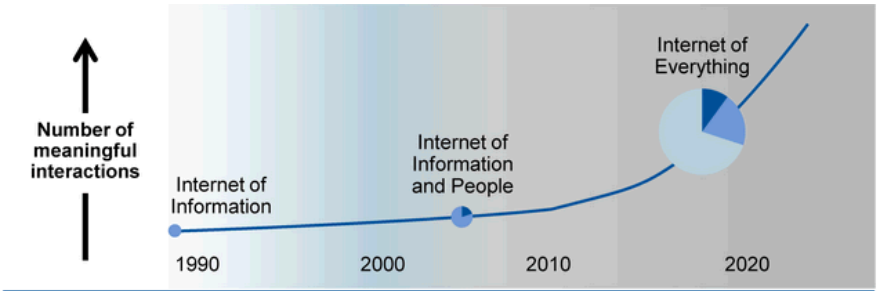
Communications Ecosystem



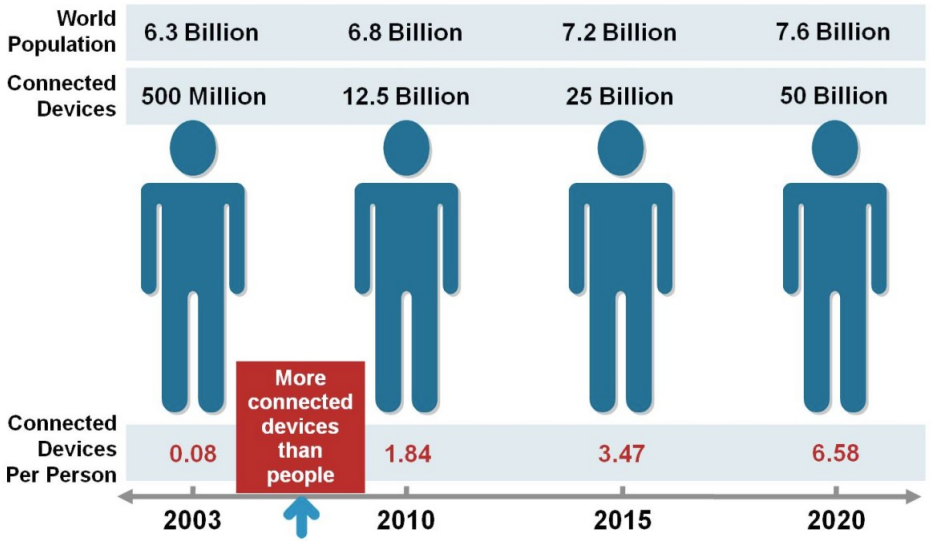
Source: GESMA "Vision of Smart Home"

Standards - IEEE P2413

- Standard for an Architectural Framework for the Internet of Things (IoT)



Key milestones	> 50% of Internet connections are things	Things create more traffic than information and people
Number of permanently Internet-connected devices	> 15 billion	> 30 billion
Number of intermittently Internet-connected devices	> 50 billion	> 200 billion
Volume of traffic from things	Minority	Majority



ECSEL JU